

# Appendices and Attachments

## Table of Contents\*

---

*\*Use PDF Bookmarks to navigate*

### Appendices

- |   |  |
|---|--|
| 1. CT Agency Regulation 19a-25                  | 12. HHS HIPPA Public Health Fact Sheet                                 |
| 2. CT Agency Regulation 19a-36                  | 13. CT OPM Network Security Policy and Procedures                      |
| 3. CDC Assurances of Confidentiality            | 14. CT OPM Policy on Security for Mobile Computing and Storage Devices |
| 4. Section Breach Mitigation Checklist          | 15. DAS/BITS Mobile Device Pledge                                      |
| 5. HSS Breach Notification Policy               | 16. DPH IT Mobile Device Incident Report                               |
| 6. DPH HR Security Protocols                    | 17. Section Sample Fax Cover Page Disclaimer                           |
| 7. HIPAA Access Letter                          | 18. NCHS Confidentiality Statute Section 308                           |
| 8. DPH Record Retention Schedule for HIV        | 19. DPH Data Sharing Agreement   |
| 9. DPH Record Retention Schedule for TB & STD   | 20. DPH Severance Policies   |
| 10. DPH IT eHARS Servers Disaster Recovery Plan | 21. 2023 Confidentiality Agreement                                     |
| 11. eHARS Disaster Recovery Plan Table          |  |

### Other Relevant Attachments

- |   |  |
|---|--|
| 1. DPH Confidentiality Policies and Regulations | 5. CDC Security and Confidentiality Validation |
| 2. DPH Confidentiality Pledge                   | 6. CDC Security Assessment Checklist           |
| 3. DAS/BITS IT Tech Policies                    | 7. CDC Site Visit Security Checklist           |
| 4. DPH DIS Field Activities                     |  |

**The DPH Legal Office has a breach reporting procedure that requires additional documentation. The Data Security Managers will provide the necessary reporting forms to Supervisors and staff involved in 1a breaches.**

### DPH Legal Department Documents

- |                                       |                       |
|---------------------------------------|-----------------------|
| Non-HIPAA Data Security Breach Policy | FOI Policy            |
| Data Breach Report                    | FOI Response Template |
| DPH Breach Resolution                 |                       |

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Agency*

**Department of Public Health**

*Subject*

**Disclosure of Health Data**

*Inclusive Sections*

**§§ 19a-25-1—19a-25-4**

---

CONTENTS

---

|                |  |
|----------------|--|
| Sec. 19a-25-1. | Definitions  |
| Sec. 19a-25-2. | Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality |
| Sec. 19a-25-3. | Disclosure of identifiable health data   |
| Sec. 19a-25-4. | Use of health data for enforcement purposes  |

**Disclosure of Health Data**

**Sec. 19a-25-1. Definitions**

As used in Sections 19a-25-1 through 19a-25-4, inclusive, of the Regulations of Connecticut State Agencies:

(1) “Aggregate health data” means health data that is obtained by combining like data in a manner that precludes the identification of the individual or organization supplying the data or described in the data.

(2) “Anonymous medical case history” means the description of an individual’s illness in a manner that precludes the identification of the individual or organization supplying the data or described in the data.

(3) “Commissioner” means the commissioner of the Department of Public Health.

(4) “Department” means the Department of Public Health.

(5) “Disclosure” or “disclose” means the communication of health data to any individual or organization outside the department.

(6) “Health data” means information, recorded in any form or medium, that relates to the health status of individuals, the determinants of health and health hazards, the availability of health resources and services, or the use and cost of such resources and services.

(7) “Identifiable health data” means any item, collection, or grouping of health data that makes the individual or organization supplying it, or described in it, identifiable.

(8) “Individual” means a natural person.

(9) “Local Director of Health” means the city, town, borough, or district Director of Health or any person legally authorized to act for the local director of health.

(10) “Medical or scientific research” means the performance of activities relating to health data, including, but not limited to:

(A) describing the group characteristics of individuals or organizations;

(B) characterizing the determinants of health and health hazards;

(C) analyzing the inter-relationships among the various characteristics of individuals or organizations;

(D) the preparation and publication of reports describing these matters; and

(E) other related functions as determined by the commissioner.

(11) “Organization” means any corporation, association, partnership, agency, department, unit, or other legally constituted institution or entity, or part thereof.

(12) “Studies of morbidity and mortality” means the collection, application, and maintenance of health data on:

(A) the extent, nature, and impact of illness and disability on the population of the state or any portion thereof;

(B) the determinants of health and health hazards, including but limited to,

(i) infectious agents of disease,

(ii) environmental toxins or hazards,

(iii) health resources, including the extent of available manpower and resources, or

(iv) the supply, cost, financing or utilization of health care services.

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-25-2

*Department of Public Health*

(C) diseases on the commissioner's list of reportable diseases and laboratory findings pursuant to section 19a-215 of the Connecticut General Statutes; or

(D) similar health or health related matters as determined by the commissioner.

(Adopted effective October 30, 1998)

**Sec. 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality**

(a) The department may, at the discretion of the commissioner, publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports:

(1) Are prepared for the purpose of medical and scientific research; and

(2) Do not include identifiable health data.

(b) No individual or organization with lawful access to such reports shall be compelled to testify with regard to such reports. Publication or release of such reports shall not subject said report or related information to subpoena or similar compulsory process in any civil or criminal, judicial, administrative or legislative proceeding.

(Adopted effective October 30, 1998)

**Sec. 19a-25-3. Disclosure of identifiable health data**

(a) The department shall not disclose identifiable health data unless:

(1) The disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to section 19a-215 of the Connecticut General Statutes;

(2) The disclosure is to health care providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control pursuant to section 19a-215 of the Connecticut General Statutes or for the purpose of reducing morbidity and mortality from any cause or condition, except that every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose;

(3) The disclosure is to an individual, organization, governmental entity in this or another state or to the federal government, provided the department determines that:

(A) Based upon a written application and such other information as required by the department to be submitted by the requesting individual, organization or governmental entity the data will be used solely for bona fide medical and scientific research;

(B) The disclosure of data to the requesting individual, organization or governmental entity is required for the medical or scientific research proposed;

(C) The requesting individual, organization, or governmental entity has entered into a written agreement satisfactory to the department agreeing to protect such data in accordance with the requirements of this section and not permit disclosure without prior approval of the department; and

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

---

*Department of Public Health*

*§19a-25-4*

(D) The requesting individual, organization or governmental entity, upon request of the department or after a specified date or event, returns or destroys all identifiable health data provided by the department and copies thereof in any form.

(4) The disclosure is to a governmental entity for the purpose of conducting an audit, evaluation, or investigation required by law of the department and such governmental entity agrees not to use such data for making any determination as to whom the health data relates.

(b) Any disclosure provided for in this section shall be made at the discretion of the department, provided the requirements for disclosure set forth in the applicable provisions of this section have been met. For disclosures under this section to governmental entities, the commissioner may waive the requirements of this section except for the requirements of subdivision (A) of subsection (3).

(c) Notwithstanding any other provisions of this section, no identifiable health data obtained in the course of activities undertaken or supported under this section shall be subject to subpoena or similar compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.

(Adopted effective October 30, 1998)

**Sec. 19a-25-4. Use of health data for enforcement purposes**

(a) Notwithstanding any provisions of sections 19a-25-1 to 19a-25-3, inclusive of the Regulations of State Agencies, the department may utilize, in any manner, health data including but not limited to aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law and said parties may not further disclose such data except to a tribunal, administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.

(Adopted effective October 30, 1998)

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

*Agency*

**Department of Public Health**

*Subject*

**Reportable Diseases and Laboratory Findings**

*Inclusive Sections*

**§§ 19a-36-A1—19a-36-A21**

CONTENTS

|                  |   |
|------------------|---|
| Sec. 19a-36-A1.  | Definitions   |
| Sec. 19a-36-A2.  | List of reportable diseases and laboratory findings                             |
| Sec. 19a-36-A3.  | Persons required to report reportable diseases and laboratory findings          |
| Sec. 19a-36-A4.  | Content of report and reporting of reportable diseases and laboratory findings  |
| Sec. 19a-36-A5.  | Confidentiality of data   |
| Sec. 19a-36-A6.  | Investigation and control of reportable disease and outbreaks by the department |
| Sec. 19a-36-A7.  | Diseases not enumerated   |
| Sec. 19a-36-A8.  | General measures for control of reportable diseases                             |
| Sec. 19a-36-A9.  | Control of diseases suspected of being reportable                               |
| Sec. 19a-36-A10. | Presumably exposed persons may be examined and controlled                       |
| Sec. 19a-36-A11. | Control of carriers of the infectious agent of communicable disease             |
| Sec. 19a-36-A12. | Enteric disease carriers  |
| Sec. 19a-36-A13. | Control of tuberculosis   |
| Sec. 19a-36-A14. | Control of refractory persons affected with tuberculosis                        |
| Sec. 19a-36-A15. | Control of venereal disease   |
| Sec. 19a-36-A16. | Control of refractory persons affected with venereal diseases                   |
| Sec. 19a-36-A17. | Observance of quarantine and instructions                                       |
| Sec. 19a-36-A18. | Control of quarantine area  |
| Sec. 19a-36-A19. | Duty of local director of health to quarantined persons in need                 |
| Sec. 19a-36-A20. | Preventing spread of disease by common carriers                                 |
| Sec. 19a-36-A21. | Food and food handlers restricted   |

**Reportable Diseases and Laboratory Findings**

**Sec. 19a-36-A1. Definitions**

As used in Sections 19a-36-A1 to 19a-36-A55:

(a) “Authorized agent” means an individual designated by a local director of health to act for him or her in the performance of any of his or her duties.

(b) “Carrier” means an infected person or animal who, without any apparent symptoms of communicable disease, harbors a specific infectious agent and may serve as a source of infection for humans. The state of harboring a specific infectious agent may occur in an individual with an infection that is inapparent throughout its course (asymptomatic carrier), or in an individual during the incubation period, convalescence, and post-convalescence of a clinically recognizable disease (incubatory carrier and convalescent carrier). The carrier state may be of short duration (transient carrier) or long duration (chronic carrier).

(c) “Case” means a person or animal who exhibits evidence of disease.

(d) “Cleaning” means the process of removal of organic matter conducive to growth or maintenance of infectivity of infectious agents by scrubbing and washing as with hot water and soap.

(e) “Commissioner” means the state commissioner of health services.

(f) “Communicable disease” means a disease or condition, the infectious agent of which may pass or be carried directly or indirectly, from the body of one person or animal to the body of another person or animal.

(g) “Communicable period” means any time period during which a specific infectious agent may be transferred directly or indirectly from an infected person or animal to another human or animal.

(h) “Contact” means a person or animal known to have had association with an infected person or animal in such a manner as to have been exposed to a particular communicable disease.

(i) “Contamination” means the presence of undesirable substance or material which may contain an infectious agent on external body surfaces (e.g., skin), articles of apparel, inanimate surfaces or in food or beverages.

(j) “Cultures” mean growths of an infectious agent propagated on selected living or artificial media.

(k) “Date of onset” means the day, month and year on which the case or suspected case experienced the first sign or symptoms of the disease.

(l) “Department” means the Connecticut Department of Health Services.

(m) “Disinfection” means a directly applied chemical or physical process by which the disease producing powers of infectious agents are destroyed. (1) “Concurrent disinfection” means the immediate disinfection and disposal of body discharges, and the immediate disinfection or destruction of all infected or presumably infected materials. (2) “Terminal disinfection” means the process of rendering the personal clothing and immediate physical environment of a patient free from the probability of conveying an infectious agent to others after removal of the patient or at a time when the patient is no longer a source of infection.

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A1

*Department of Public Health*

(n) “Epidemic” means the occurrence of cases of illness clearly in excess of normal expectancy over a specific time period in a community, geographic region, building or institution. The number of cases indicating an epidemic may vary according to the causative agent, size and type of population exposed, previous experience with the disease, and time and place of occurrence. An outbreak of disease is an epidemic.

(o) “Epidemiologic investigation” means an inquiry into the incidence, distribution and source of disease to determine its cause, means of prevention, and efficacy of control measures.

(p) “Foodborne outbreaks” means illness in two or more individuals acquired through the ingestion of common-source food or water contaminated with chemicals, infectious agents or their toxic products. Foodborne outbreaks include, but are not limited to, illness due to heavy metal intoxications, staphylococcal food poisoning, botulism, salmonellosis, shigellosis, *Clostridium perfringens* intoxication and hepatitis A.

(q) “Foodhandler” means a person who prepares, processes, or otherwise handles food or beverages for people other than members of his or her immediate household.

(r) “Health care facility” means any hospital, long term care facility, home health care agency, clinic or other institution licensed under Chapter 368v of the Connecticut General Statutes and also facilities operated and maintained by any state agency for the care or treatment of mentally ill persons or persons with mental retardation or substance abuse problems.

(s) “Health care provider” means a person who has direct or supervisory responsibility for the delivery of health care or medical services. This shall include but not be limited to: licensed physicians, nurse practitioners, physician assistants, nurses, dentists, medical examiners, and administrators, superintendents and managers of health care facilities.

(t) “Incubation period” means the time interval between exposure to a disease organism and the appearance of the first symptoms of the resulting disease.

(u) “Infection” means the entry and multiplication of an infectious agent in the body of a person or animal with or without clinical symptoms.

(v) “Infectious agent” means a microorganism capable of producing infection with or without disease.

(w) “Isolation” means the use of special precautions during the period of communicability to prevent transmission of an infectious agent. Such special precautions may include: physical separation of infected persons or animals from others, or precautions such as blood precautions that do not necessarily result in physical separation of individuals.

(x) “Laboratory” means any facility licensed, or approved by the department in accordance with section 19a-30 of the Connecticut General Statutes.

(y) “Local director of health” means and includes the city, town, borough or district director of health and any person legally authorized to act for the local director of health.

(z) “Medical information” means the recorded health information on an individual who has a reportable disease or who has symptoms of illness in the setting of an outbreak. This information includes details of a medical history, physical examination, any laboratory test,

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Department of Public Health*

*§19a-36-A2*

---

diagnosis, treatment, outcome and the description and sources of suspected causative agents for such disease or illness.

(aa) “Nosocomial infection” means infections that develop within a hospital or other health care facility or are produced by microorganisms acquired while in a hospital or health care facility.

(bb) “Outbreak.” See “epidemic.”

(cc) “Quarantine” means the formal limitation of freedom of movement of persons or animals exposed to, or suffering from a reportable disease for a period of time not longer than either the longest incubation period or the longest communicable period of the disease, in order to prevent spread of the infectious agent of that disease.

(dd) “Reportable disease” means a communicable disease, disease outbreak, or other condition of public health significance required to be reported to the department and local health directors.

(ee) “Reportable laboratory finding” means a laboratory result suggesting the presence of a communicable disease or other condition of public health significance required to be reported to the department and local health directors.

(ff) “State epidemiologist” means the person designated by the Commissioner as the person in charge of communicable disease control for the state.

(gg) “Surveillance” means the continuing scrutiny of all aspects of occurrence and spread of a disease relating to effective control of that disease, which may include but not be limited to the collection and evaluation of: morbidity and mortality reports; laboratory reports of significant findings; special reports of field investigations of epidemics and individual cases; data concerning the availability, use, and untoward side effects of the substances used in disease control, such as rabies vaccine; and information regarding immunity levels in segments of the population.

(hh) “Suspected case” means a person or animal suspected of having a particular disease in the temporary or permanent absence of definitive clinical or laboratory evidence.

(ii) “Other condition of public health significance” means a non-communicable disease caused by a common source or prevalent exposure such as pesticide poisoning, silicosis or lead poisoning.

(Effective October 25, 1989; Amended October 10, 2008)

**Sec. 19a-36-A2. List of reportable diseases and laboratory findings**

The commissioner shall issue a list of reportable diseases and laboratory findings within sixty days of the effective date of these regulations, on the next January 1, and annually thereafter. The list shall show it is the current list and shall specify its effective date. This list shall also include but not be limited to the reporting category of each disease, procedures for the reporting, and minimum investigation and control measures for each disease. Listed diseases are declared reportable diseases as of the effective date of approval by the commissioner.

(a) The commissioner in consultation with the state epidemiologist will annually review

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A3

*Department of Public Health*

the existing list and develop recommendations for deletions or additions to the list.

(b) The state epidemiologist or other commissioner designee shall convene and chair an advisory committee to review the recommendations for any changes to the list prior to preparing the final list for that year. This committee shall make recommendations to the commissioner regarding the contents of the list.

(c) The commissioner shall review the advisory committee's recommendations and make final deletions or additions to the list to take effect January 1 of the next year. He will furnish copies of the list before January 1 to the following:

- (1) physicians licensed by the department;
- (2) directors of clinical laboratories licensed, registered or approved by the department;
- (3) local directors of health in Connecticut;
- (4) health care facilities licensed under Chapter 368v of the Connecticut General Statutes.

(Effective October 25, 1989)

**Sec. 19a-36-A3. Persons required to report reportable diseases and laboratory findings**

**(a) Reportable Diseases.**

(1) Every health care provider who treats or examines any person who has or is suspected to have a reportable disease shall report to the local director of health or other health authority within whose jurisdiction the patient resides and to the department such information about the affected person as described in section 19a-36-A4 of these regulations.

(2) If the case or suspected case of reportable disease is in a health care facility, the person in charge of such facility shall ensure that reports are made to the local director of health and the department in the manner specified in section 19a-36-A4 of these regulations. The person in charge shall designate appropriate infection control or record-keeping personnel for this purpose.

(3) If the case or suspected case of reportable disease is not in a health care facility and if a health care provider is not in attendance or is not known to have made a report within the appropriate time specified in section 19a-36-A4, such report of reportable diseases shall be made to the local director of health or other health authority within whose jurisdiction the patient lives and the department in the manner specified in section 19a-36-A4 by:

(A) the administrator serving a public or private school or day care center attended by any person affected or apparently affected with such disease;

(B) the person in charge of any camp;

(C) the master or any other person in charge of any vessel lying within the jurisdiction of the state;

(D) the master or any other person in charge of any aircraft landing within the jurisdiction of the state;

(E) the owner or person in charge of any establishment producing, handling or processing dairy products, other food or non-alcoholic beverages for sale or distribution;

(F) morticians and funeral directors.

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Department of Public Health*

*§19a-36-A4*

---

(4) Each local director of health shall report or ensure reporting to the department within 24 hours of each case or suspected case of a Category I reportable disease and such additional information of which he has knowledge as described in section 19a-36-A4 of these regulations.

(b) **Reportable laboratory findings.**—The director of a laboratory that receives a primary specimen or sample which yields a reportable laboratory finding shall be responsible for reporting such findings within forty-eight (48) hours to the local director of health of the town in which the affected person normally resides, or, in the absence of such information, of the town from which the specimen originated, and to the department on forms provided by the department.

(1) When a laboratory identifies or presumptively identifies a significant isolate or other finding that requires confirmation by the laboratory as required in the annual list, the director must submit that isolate or specimen from which the finding was made to the department's laboratory division.

(2) Laboratory tests and confirmatory tests for certain reportable diseases as specially indicated in the annual list shall be exempted from any and all fees for the state laboratory services in accordance with Section 19a-26 of the Connecticut General Statutes.

(Effective October 25, 1989)

**Sec. 19a-36-A4. Content of report and reporting of reportable diseases and laboratory findings**

(a) **Reportable diseases.**

(1) Each report of a case or suspected case of reportable disease shall include the full name and address of the person reporting and of the physician attending; the diagnosed or suspected disease and date of onset; the full name, age, race/ethnicity, sex and occupation of the affected individual and other facts the department or local director of health requires for purposes of surveillance, control and prevention of reportable diseases. The reports shall be sent in envelopes marked "CONFIDENTIAL."

(2) Reports may be written or oral as required by the category of disease as follows:

(A) Category I: diseases of high priority because of need for timely public health action: reportable immediately by telephone on day of recognition or suspicion of disease; on weekdays to both, the local health director of the town in which the patient resides and the department, on weekends to the department. A completed disease report form provided by the department must also be mailed to both the local health director and the department within 12 hours.

(B) Category II: diseases of significant public health importance, usually requiring public health action: reportable by mail to the local director health and the department within 12 hours of recognition or suspicion on a form provided by the department.

(b) **Reportable laboratory findings.**

(1) Each report of reportable findings shall include the name, address, age, sex, and, if known, race/ethnicity of the person affected, the name and address of the attending

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A5

*Department of Public Health*

physician, the identity of the infectious agent or other reportable laboratory findings, and the method of identification.

(2) Reports shall be mailed to the local director of health of the town in which the patient resides and to the department within 48 hours of making the finding in envelopes marked "CONFIDENTIAL."

(Effective October 25, 1989)

**Sec. 19a-36-A5. Confidentiality of data**

All epidemiologic information which identifies an individual and which is gathered by the state or local health department in connection with the investigation of reported cases or suspected cases of disease or during the investigation of outbreaks of disease shall be kept in compliance with current confidentiality statutes.

(Effective October 25, 1989)

**Sec. 19a-36-A6. Investigation and control of reportable disease and outbreaks by the department**

(a) The department, in cooperation with the local director of health, in the investigation and control of reportable disease shall make or cause to be made such investigation as it deems necessary and shall secure all such data as may assist it in establishing adequate control measures.

(b) In order to investigate and control any apparent outbreak or unusual occurrence of reportable disease, the department shall institute such special disease surveillance, follow-up reports and control measures as it deems necessary.

(c) Individual medical information pertaining to cases of reportable disease, persons affected by outbreaks of disease or significant increases in the rate of nonsocomial infection shall be provided when requested to an investigator who presents official identification of the department or the local department of health. Such an investigator may be an employee of the State or local health department.

(Effective October 25, 1989)

**Sec. 19a-36-A7. Diseases not enumerated**

Diseases not specifically listed pursuant to section 19a-36-A2 and presenting a special problem shall be reported and controlled in accordance with special instructions of the state department of health or, in the absence of such instructions, in accordance with orders and directions of the local director of health.

(Effective October 25, 1989)

**Sec. 19a-36-A8. General measures for control of reportable diseases**

The local director of health, in instituting measures for the control of reportable diseases:  
**Investigation**

(a) shall make, or cause to be made, such investigations as he may deem necessary and

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Department of Public Health*

*§19a-36-A8*

---

shall secure all such data as may assist him in establishing adequate control measures;

**Isolation and orders**

(b) shall establish and maintain quarantine, isolation or such other measures for control as are required by statute, the public health code or special instructions of the state department of health, and, when possible, shall issue his instructions and orders in writing or on printed forms;

**Removal**

(c) shall have the authority to set up proper isolation or quarantine of an affected person or persons, carrier or contact, when, in his opinion or in the opinion of the state commissioner of health, this is not or cannot be effectively maintained on the premises occupied by such person or persons by methods designated in this part; to remove or require the removal of such person or persons to a hospital or other proper place designated by him; or to employ such guards or officers as may be necessary to maintain effective isolation or quarantine;

**Instruction**

(d) shall provide, by himself or his authorized agent, for the specific instruction of cases, contacts, their attendants and all other persons affected, in the proper methods for the prevention of the spread of the disease and shall supply such information and literature as may be required by law or by the instructions of the state department of health;

**Enforcement**

(e) shall make, at intervals during the period of communicability, inquiry or investigation to satisfy himself that the measures instituted by him for the protection of others are being properly observed;

**Laboratory tests**

(f) shall, when the control or release of a case, contact or carrier of a reportable disease is dependent upon laboratory findings, require the specimens upon which such findings are based to be examined by the laboratory division of the state department of health or by a laboratory specifically approved for that purpose by the state department of health and shall, by himself or his authorized agent, secure and submit release cultures or specimens for examination; in cases of enteric diseases all release specimens shall be taken at least one week after specific therapy has been discontinued;

**Schools—Isolation**

(g) shall, in the event of an outbreak of a communicable disease in any public, private, parochial or church school, make a prompt and thorough investigation; control such an outbreak by individual examination of pupils, teachers and other persons associated with the outbreak; employ such other means as he deems necessary to determine the source of infection or to provide for the segregation of infected persons; in the event of an outbreak of a communicable disease in any school, require school physicians and school nurses to conform to the orders, regulations and restrictions issued by him;

**Schools—Readmission**

(h) shall, in the case of any school child who has been excluded from school for having

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A9

*Department of Public Health*

been a case, contact or carrier of a communicable disease, by himself or his authorized agent, issue a permit for such child to re-enter school when in his opinion such child is no longer infectious;

**Unusual disease**

(i) shall, when an unusual or rare disease occurs in any part of the state or when any disease becomes so prevalent as to endanger the state as a whole, contact the state department of health for assistance, and shall cooperate with the representatives of the state department of health acting under the direction of the state commissioner of health;

**Other measures**

(j) shall introduce such other measures as he may deem advisable.

(Effective October 25, 1989)

**Sec. 19a-36-A9. Control of diseases suspected of being reportable**

The local director of health, on receiving a report of a disease suspected of being reportable, shall confer with the physician or other person making such report, make further examination or investigation as he deems necessary and advise, recommend or establish such procedures as he may deem necessary to protect the public health until the character of the disease is definitely determined.

(Effective October 25, 1989)

**Sec. 19a-36-A10. Presumably exposed persons may be examined and controlled**

The local director of health, when he has reasonable grounds to believe that a person or persons may have been exposed to a communicable disease, may control such persons as known contacts and may make such examinations and adopt such measures as he deems necessary and proper for the protection of the public health and the prevention of the spread of disease.

(1) The conviction of any person for any offense involving sexual promiscuity or illicit sex relations shall constitute reasonable grounds for the local director of health to believe that that person may have been exposed to a communicable disease and shall justify the examination and such other measures of control of that individual as are deemed necessary and proper by the state department of health for the protection of public health and the prevention of spreading of disease.

(2) The warden or other person in charge of any prison or jail in the state shall notify the prison or jail physician, in writing, within twenty-four hours upon the receipt of a prisoner who may have been exposed to a communicable disease and of every prisoner who has been convicted of any offense involving sexual promiscuity or illicit sex relations. A routine medical examination shall be made on every prisoner whose conviction involves sexual promiscuity or illicit sex relations. Such routine medical examination shall include the taking of a blood specimen for serological test for syphilis and the taking of three smears for gonococci taken not less than twenty-four hours apart and, if the prisoner is found to be infected, treatment shall be instituted as necessary. The tests referred to above shall be

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Department of Public Health*

*§19a-36-A12*

---

performed in the bureau of laboratories of the state department of health or in a laboratory specifically approved for these purposes by the state department of health, and they shall be performed in a manner that meets the approval of the state department of health. Upon the expiration of a sentence, any person having syphilis or gonococcal infection, whether in an infectious or non-infectious stage, and in need of further followup treatment shall be reported to the state department of health by the attending physician, who shall give the name, sex, age and marital status and a record of the treatment given while such person was imprisoned.

(Effective October 25, 1989)

**Sec. 19a-36-A11. Control of carriers of the infectious agent of communicable disease**

Carriers, whether transient, convalescent or chronic, of the infectious agent of any communicable disease shall be maintained under observation until repeated laboratory examinations of appropriate specimens show the absence of the infectious agent. Examination of all such specimens shall be in conformity with subsection (f) of section 19a-36-A8.

(a) Any local director of health or physician who discovers any carrier of an infectious agent shall report the fact to the state department of health giving the full name, age, sex, occupation and address of such carrier. The state department of health shall, upon receipt of such report, notify the local director of health of the town, city or borough wherein the carrier resides. The local director of health concerned shall then communicate the fact to the carrier himself, or his guardian, giving specific instructions regarding the precautions necessary to protect others from infection.

(b) Any privy or latrine used by an enteric disease carrier shall be so constructed as to exclude flies and to meet the approval of the local director of health. The disinfection and disposal of its contents shall be in accordance with instructions given by the local director of health.

(c) A carrier of an infectious agent shall not engage in any occupation involving the handling of any food or beverage intended for the use of others.

(d) Enteric disease carriers shall not work on any public water supply or watershed.

(e) A carrier who changes his residence shall notify the local director of health of the town, city or borough in which he has been residing of the date of his departure, his destination and his new address. The local director of health shall immediately forward this information to the state department of health.

(f) The local director of health shall visit each carrier within his jurisdiction at least once every three months and shall render quarterly reports concerning each such carrier to the state department of health upon forms prescribed for the purpose.

(Effective October 25, 1989)

**Sec. 19a-36-A12. Enteric disease carriers**

(a) A chronic carrier of enteric disease shall be defined as a person who persists in

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A13

*Department of Public Health*

excreting enteric pathogenic organisms for twelve months or more after onset of illness or probable date of infection or one who, though he may never have been known to have the disease, has been shown to harbor the infectious agent in his body.

(b) All specimens for the release of enteric carriers from supervision shall be collected at least ten days after the cessation of any antibiotic therapy or any therapy directed at the disease.

(c) All specimens for the release of enteric carriers from supervision shall be examined in conformity with subsection (f) of section 19a-36-A8.

(d) Chronic carriers of the organisms causing typhoid fever and paratyphoid fever shall not be released from supervision until six successive specimens of urine and six successive specimens of feces, the last two of which shall be validated by collection of the specimen in a hospital or otherwise under direct supervision, have been found negative. Specimens for such examination shall be so collected that a time interval of not less than one month shall elapse between successive specimens of urine and between successive specimens of feces. The final two specimens of feces to be examined may be validated by the giving of lycopodium or a negative bile culture may be substituted for such validation.

(e) A chronic carrier of enteric disease excreting the organism in discharges other than the feces or urine shall not be released from supervision until negative cultures as outlined by the state department of health for the specific case have been obtained.

(Effective October 25, 1989)

**Sec. 19a-36-A13. Control of tuberculosis**

(a) When a licensed physician or hospital superintendent has reported a case of tuberculosis and has agreed to assume the responsibility for the proper instruction of the patient and the taking of measures necessary for the protection of others, the local director of health need not take action other than that prescribed by sections 19a-262 to 19a-264, inclusive, of the general statutes.

(b) When such patient, while in an infectious state, neglects or refuses to follow the prescribed instructions or discontinues treatment, the physician or superintendent shall immediately notify the local director of health.

(c) When a physician or hospital superintendent has declined to assume such responsibility, the local director of health shall supply the affected person with printed instructions and take such other action as may be necessary and proper for the protection of the public health.

(Effective October 25, 1989)

**Sec. 19a-36-A14. Control of refractory persons affected with tuberculosis**

When it comes to the attention of a local director of health that a person is affected with tuberculosis and is a menace to the public health or is likely to jeopardize the health of any person or persons in or on the premises occupied or frequented by the affected person, he shall immediately investigate and shall take proper measures to prevent the spread of such

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

---

*Department of Public Health*

*§19a-36-A17*

---

disease for the protection of the public health and, if necessary, may cause the removal of such person to an isolation hospital or other proper place, there to be received and kept until he is no longer a menace to the public health.

(Effective October 25, 1989)

**Sec. 19a-36-A15. Control of venereal disease**

(a) When a licensed physician or hospital superintendent has reported a case of gonorrhea or syphilis and has agreed in writing to assume the responsibility for the proper instruction of the patient, the local director of health shall supply such physician or hospital superintendent with printed instructions for such patient.

(b) When such patient, while in an infectious state, neglects or refuses to follow the prescribed instructions or discontinues treatment, the physician or superintendent shall immediately notify the local director of health.

(c) In investigating cases or suspected cases of the above-mentioned diseases, the local director of health shall treat all information as confidential, but such course shall not preclude the making of reports to the state department of health.

(Effective October 25, 1989)

**Sec. 19a-36-A16. Control of refractory persons affected with venereal diseases**

When it comes to the attention of a local director of health that a person is affected with or presumably affected with gonorrhea or syphilis in any form and is likely to jeopardize the health of any person or persons in or on the premises occupied or frequented by the affected person, the local director of health shall immediately investigate and shall take proper measures to prevent the spread of such disease for the protection of the public health, and he shall direct such person to report regularly for treatment to a licensed physician or to a public clinic, there to be treated until such person is free from infectious discharges. If such person, in the opinion of the local director of health, is a menace to the public health, the local director of health shall order the removal of such person to an isolation hospital or other proper place, there to be received and kept until he no longer is a menace to the public health; or the local director of health shall adopt such other measures as he may deem necessary to protect the public health.

(Effective October 25, 1989)

**Sec. 19a-36-A17. Observance of quarantine and instructions**

Every person who is affected with a communicable disease, who is a carrier or who is suspected of having come in contact, directly or indirectly, with a case of communicable disease shall strictly observe and comply with all orders, quarantine regulations and restrictions given or imposed by the local health authority or the state commissioner of health in conformity with law.

(Effective October 25, 1989)

*Regulations of Connecticut State Agencies*

TITLE 19a. Public Health and Well-Being

§19a-36-A18

*Department of Public Health*

**Sec. 19a-36-A18. Control of quarantine area**

No person other than the attending physicians and authorized attendants shall enter or leave, and no one except the local director of health or his representative shall permit any other person to enter or leave, any room, apartment or premises quarantined for a communicable disease, nor shall any person needlessly expose a child or other person to a communicable disease. No person shall remove any article from a quarantined area without permission of the local director of health. The local director of health shall report immediately to the state commissioner of health, by telegraph or telephone, the name, address, probable destination and route of departure of any person who was under control for a reportable disease and who has left his jurisdiction without his consent.

(Effective October 25, 1989)

**Sec. 19a-36-A19. Duty of local director of health to quarantined persons in need**

When a person under quarantine is, in the opinion of the local director of health, unable to obtain medical care, food or other actual necessities, the local director of health shall report his findings to the proper town, city or borough authority. If such town, city or borough authority fails to supply at once the needed care, the local director of health shall supply such quarantined person with medical attention, food or other actual necessities, and the expense incurred in performing such duty shall constitute a legal expense of the local director of health and shall be paid according to state statute.

(Effective October 25, 1989)

**Sec. 19a-36-A20. Preventing spread of disease by common carriers**

In the event of the epidemic prevalence of a communicable disease, when a written declaration to that effect has been made by the state commissioner of health, any person, firm or corporation operating any common carrier within the state, or in the waters thereof, shall comply strictly with any order issued by the state commissioner of health for the purpose of preventing the introduction into the state, or the transmission from one point to another within the state, of any person or persons, animals, insects or materials likely to convey the disease.

(Effective October 25, 1989)

**Sec. 19a-36-A21. Food and food handlers restricted**

When a case of any of the reportable diseases listed pursuant to section 19a-36-A2 occurs on the premises where milk or food is produced, kept, handled or sold, the local director of health shall institute such measures as he deems necessary to prevent the spread of such disease and to protect such foods from being contaminated; and he shall require all uninfected persons who reside in an apartment or dwelling where any such disease exists, and who handle milk or food elsewhere, to remain away from such abode as long as the disease is present.

(Effective October 25, 1989)

---

## Assurances of Confidentiality

---

### Assurance of Confidentiality

#### Purpose

An Assurance of Confidentiality is a formal confidentiality protection authorized under Section 308(d) of the Public Health Service Act. It is used for projects conducted by CDC staff or contractors that involve the collection or maintenance of sensitive identifiable or potentially identifiable information. This protection allows CDC programs to assure individuals and institutions involved in research or non-research projects that those conducting the project will protect the confidentiality of the data collected. The legislation states that no identifiable information may be used for any purpose other than the purpose for which it was supplied unless such institution or individual has consented to that disclosure.

#### Statutory Authority

Under section 308(d) of the Public Health Service Act surveys conducted by the National Center for Health Statistics (NCHS) as part of their authorizing legislation are automatically protected by an Assurance of Confidentiality. In addition, Assurances of Confidentiality may be issued to projects conducted by all other CDC components, after formal application to and approval by the CDC Confidentiality Review Group has been obtained.

Information about institutions and/or individuals of research or non-research projects that involve the collection or maintenance of sensitive identifiable or potentially identifiable information and for which an Assurance of Confidentiality has been approved is protected. At CDC, the 308(d) assurance has most often been used to protect sensitive identifiable data for non-research projects, but has also been used for research studies collecting sensitive identifiable data.


#### Extent and Limitations of Coverage

Protected information includes identifiable or potentially identifiable information on institutions or individuals who are the subjects of research or non-research studies with an approved Assurance of Confidentiality.

Disclosures can be made without individual authorization only for purposes stated at the time of data collection or specifically consented to thereafter by each of the parties who were provided the promise of confidentiality.

*Assurances of Confidentiality do not take the place of good data security or clear policies and procedures for data protection, which are essential to the protection of participants' privacy. Investigators should take appropriate steps to safeguard data and findings. Unauthorized individuals must not access the data or learn the identity of participants.*

#### Assurances of Confidentiality Contact

Phone: 404-639-4642 

Email: [cdccoc@cdc.gov](mailto:cdccoc@cdc.gov) (<mailto:cdccoc@cdc.gov>).

Page last reviewed: October 11, 2017

Page last updated: April 10, 2015

Content source: Office of the Associate Director for Science

**Actions to Be Taken Immediately upon Identification of an Incident****1. Notification Process**

- ☐ Notify privacy and security officers
- ☐ Initiate security incident report form
- ☐ Record name and contact information of reporter
- ☐ Gather description of event
- ☐ Identify location of event

**2. Investigation Steps**

- ☐ Establish security incident response team (e.g., security officer, privacy officer, risk manager, administration, and others as needed) and identify team leader (e.g., privacy or security officer)
- ☐ Identify and take immediate action to stop the source (e.g., hacking) or entity responsible (e.g., work force member, vendor)
- ☐ Identify system, application, or electronic PHI compromised and then immediately begin identification process of those patients whose information was compromised and what data elements were included (e.g., name, age, date of birth, Social Security number, diagnosis)
- ☐ Determine need to notify key internal stakeholders not represented on the team:
  - HIM department (if necessary to sequester records)
  - Billing and patient accounts department (if necessary to suspend billing process)
  - Human resources department (if a work force member is suspected)
  - Vendor relations or purchasing leadership
  - Others as necessary
- ☐ Identify the source or suspects involved in event:
  - If the source is identified as a vendor or business associate, determine if business associate agreement has been established (collect as evidence)
  - If the source is identified as a work force member, establish existence of criminal background check, privacy and security education and training, etc. Coordinate with human resources to determine appropriate sanctions.
  - If the source is external, work with law enforcement agency to determine appropriate actions
- ☐ Carry out IT forensic investigation to gather evidence and determine course of events as well as identify electronic PHI compromised
- ☐ Identify and sequester pertinent medical records, files, and other documents (paper and electronic)
- ☐ Determine need for external notification or involvement (see individual sections following):
  - Legal counsel (identify all communications as “Privileged and Confidential Attorney-Client Communication/Work Product”)
  - IT forensics support
  - Law enforcement agency (local and federal)
  - Media
  - Victims

- ☐ Determine need to contact other additional external stakeholders:
  - Corporate office
  - Licensing or accrediting agencies
  - Centers for Medicare and Medicaid Services, Office for Civil Rights (self-reporting is not required by regulation, it is an organizational decision)
  - Business associates or partners

**Other Actions as Applicable**

1. Contact Law Enforcement Officials
  - ☐ Verify event constitutes a crime and is reportable
  - ☐ Determine appropriate law enforcement agency and contact
  - ☐ In cooperation with local law enforcement officials, determine the need to involve other external law enforcement agencies (e.g., FTC, FBI, Social Security Administration, Inspector General)
  - ☐ Obtain name of law enforcement contact to provide upon victim request
2. Collection of Evidence
  - ☐ Security incidence response form
  - ☐ IT forensic evidence (e.g., reports, logs, audits)
  - ☐ Records of communications (e.g., phone logs, e-mail, letters)
  - ☐ Law enforcement agency and police reports
  - ☐ Legal counsel guidance
3. Notification of Victims
  - ☐ Determine need to notify victims. Consider:
    - Likelihood of harm (e.g., stolen laptop protected by password or encryption, PHI limited to first names and dates only)
    - Recipient of information, if known (e.g., if recipient is known covered entity, there is less risk than if PHI was disclosed to other individuals)
    - Regulatory reporting and disclosure requirements (review state regulations)
    - Type of incident (e.g., targeted theft of data or incidental as part of crime of opportunity such as laptop left unaccompanied in airport waiting area)
    - Actions of other organizations if involved in event (e.g., information system of vendor hacked containing multiple healthcare clients)
    - Historical responses by others involved in similar events
  - ☐ Prepare a communication plan to cover oral and written communications to victims as well as information to assist them with personal needs (FTC guidance) and organizational contact person for questions and concerns (privacy officer)
  - ☐ Provide information regarding law enforcement contacts
  - ☐ Consider provision of credit monitoring services (e.g., fees paid by organization? If so, how long?)

# Data Breach Investigation and Mitigation Checklist

## Actions to Be Taken Immediately upon Identification of an Incident

4. Communication with Media
    - ☐ Determine need to proactively contact media or prepare press release in response to inquiries. Consider:
      - Likelihood of media awareness or investigation
      - Scope of event (e.g., number of individuals impacted, type of information disclosed, threat of harm to victims)
      - Potential for harm to individuals (e.g., patients, business associates, clients, others)
      - Organizational preventive safeguards and practices
      - Mitigation efforts
      - Preparation of talking points for public affairs department outlining organizations privacy and security safeguards
      - Limitations of disclosure as advised by legal counsel or law enforcement
  5. Other Organizational Processes to Be Considered
    - ☐ Determine how best to account for disclosures of PHI (HIPAA requirement):
      - Update each health record (paper or electronic) with disclosure information
      - Provide list of patients to privacy officer in response to accounting of disclosure requests (may be preferred for large numbers of disclosures)
    - ☐ If event is result of a business associate's failure to safeguard PHI, consider need to terminate relationship (refer to business associate agreement)
- ☐ Determine:
    - How well did the work force members respond to event?
    - Were documented procedures followed? Were they adequate?
    - What information was needed sooner?
    - Were there any steps or actions that might have inhibited recovery?
    - What could work force members do differently the next time an incident occurs?
    - What corrective actions can prevent similar events in the future?
    - What additional resources are needed to detect, analyze, and mitigate future incidents?
    - Can missing electronic PHI be recreated to provide continuity of care?
    - What external resources and contacts proved helpful?
    - Other conclusions or recommendations
2. Follow-Up
    - ☐ Security incident response form completed and supporting documentation made part of form or filed as attachments (consider restricting access to the form)
    - ☐ Policy and process review completed and all necessary changes made based on shortcomings identified through managing event
    - ☐ Training, education, and awareness activities carried out (balancing need for awareness with disclosure of event)
    - ☐ Event documented as educational case study (de-identified) for internal use

## Follow-Up Activities, Identifying Opportunities for Improvement

1. Evaluation of Security Incident Response (Document on Form)
  - ☐ Identify actions:
    - Identification measures (incident verified, assessed, options evaluated)
    - Evidence collected
    - Eradication measures
    - Recovery measures
3. Other
  - ☐ Consider the offer of a reward for return of lost or stolen equipment ❖

## Health Information Privacy

---

### Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

### Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

There are three exceptions to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted

by the Privacy Rule. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

## Unsecured Protected Health Information and Guidance

Covered entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

This guidance was first issued in April 2009 with a request for public comment. The guidance was reissued after consideration of public comment received and specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, the guidance also applies to unsecured personal health record identifiable health information under the FTC regulations. Covered entities and business associates, as well as entities regulated by the FTC regulations, that secure information as specified by the guidance are relieved from providing notifications following the breach of such information.

[View the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.](#)

## Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

### Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).

With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

### Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

### Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

### Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

## Administrative Requirements and Burden of Proof

Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured protected health information did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required: (1) its risk assessment demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure; or (2) the application of any other exceptions to the definition of “breach.”

Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

## Instructions for Covered Entities to Submit Breach Notifications to the Secretary

[Submit a Breach Notification to the Secretary.](#)

## View Breaches Affecting 500 or More Individuals

Breaches of Unsecured Protected Health Information affecting 500 or more individuals. [View a list of these breaches.](#)

**STATE OF CONNECTICUT  
DEPARTMENT OF PUBLIC HEALTH**

**PROCEDURE MANUAL  
HUMAN RESOURCES**

|                               |                       |
|-------------------------------|-----------------------|
| <b>Name of Procedure:</b>     | Security Protocols    |
| <b>Procedure Number:</b>      | HR 13-001             |
| <b>Prepared By:</b>           | Administration Branch |
| <b>Date Prepared:</b>         | 3/5/2013              |
| <b>Date Revised:</b>          |                       |
| <b>Forms and Attachments:</b> |                       |

**Introduction:**

It is The Department of Public Health's policy to maintain a safe and secure work environment for its employees. All DPH employees are required to comply with the safety procedures outlined below:

**Procedures:**

1. Employees must visibly display a State issued photo ID badge at all times when present at the 410-470 Capital Avenue complex.
2. If a state photo ID badge is unavailable upon entering the complex, employees must produce a valid ID and sign- in at the security desk to obtain a visitor's pass. This pass must be worn throughout the day while in the complex.
3. If a State ID badge is lost, employees must contact Human Resources to arrange for a replacement ID badge.
4. Security doors are to be completely closed after entering and leaving the building complex.
5. When expecting visitors, email [capavesecurity@rmbradley.com](mailto:capavesecurity@rmbradley.com) with the date, time and location of the meeting as well as the first and last names of visitors in advance of the scheduled meeting.
6. Employees are responsible for escorting visitors from the floor security door to the work area and escort the visitors back to the floor security door when the visit is complete.
7. Any suspicious activity must be reported to a security officer immediately by calling 1-860-418-6075.

# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

Deidre S. Gifford, MD, MPH  
Acting Commissioner



Ned Lamont  
Governor  
Susan Bysiewicz  
Lt. Governor

To: Health Care Provider or Medical Records Department Staff

From: Ellen Blaschinski, RS, MBA *Ellen Blaschinski*  
Public Health Branch Chief  
Preparedness/Local Health/HIV/STD/ TB/HIV/Viral Hepatitis Branch

Date: June 16, 2020

Re: Access to medical records and/or patient information

**Heather Linardos, Epidemiologist 4** is authorized to review patient medical records or have access to patient information on behalf of the Connecticut Department of Public Health (DPH).

Covered entities may release personally identifiable health information to the Department and its agents without an authorization, consent, release, or opportunity to object by the patient under both state and Federal (HIPAA) law, as follows:

Pursuant to *Conn. Gen. Stat.* §19a-215 and the Regulations of State Agencies §§19a-36-A4 and 19a-36-A6, the requested information is required to be provided to the Department of Public Health and its agents.

Please note that *Conn. Gen. Stat.* §52-146o(b)(1) authorizes the release of these records without the patient's consent.

Additionally, the Department of Public Health is a health oversight agency as defined by §164.501 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA also authorizes providers to release personally identifiable health information to the Department without authorization, consent, release, or opportunity to object by the patient, as information (i) required by law to be disclosed (HIPAA Privacy Regulation, 42 CFR §164.512(a)), (ii) as part of the Department's public health activities (HIPAA Privacy Regulation, 42 CFR §164.512(b)), and (iii) as part of the Department's public health oversight activities (HIPAA Privacy Regulation, 42 CFR §164.512(d)).

Please note: the definition of "health oversight agency" (§164.501 of HIPAA Privacy Regulations) includes entities "acting under a grant of authority from or contract with such public agency." Thus, covered entities are authorized to release personally identifiable health information under the authorities cited above, to the Department's contractors who are acting as the Department's agents.

Providers may also rely upon the Department and its agents that the requested information is what is minimally necessary to achieve the purpose of the disclosure (42 CFR §164.514(d)(3)(iii)(A) of the HIPAA Privacy Regulations).

The medical records department or provider office may wish to retain a copy of this letter for future medical record requests.

If you have questions or wish to confirm the information in this letter, please call or email me at the contact information below.

Thank you very much for your cooperation.

(860) 509-7900  
ellen.blaschinski@ct.gov

Phone: (860) 509-7900 • Fax: (860) 509-8237  
Telecommunications Relay Service 7-1-1  
410 Capitol Avenue, P.O. Box 340308  
Hartford, Connecticut 06134-0308  
www.ct.gov/dph  
Affirmative Action/Equal Opportunity Employer



**RECORDS RETENTION SCHEDULE**  
**DEPARTMENT OF PUBLIC HEALTH**

Form RC-050 (Revised 02/2012)



STATE OF CONNECTICUT  
 Connecticut State Library  
 Office of the Public Records Administrator  
 231 Capitol Avenue, Hartford, CT 06106  
[www.cslib.org/publicrecords](http://www.cslib.org/publicrecords)

**RECORDS RETENTION**  
**SCHEDULE #**
12-2-2

**AGENCY:**  
 Department of Public Health (DPH)

**AGENCY ADDRESS:**  
 410 Capitol Avenue, Hartford, CT 06106

This schedule is: ☐ NEW  
☒ REVISED  
 Superseded schedule number(s):  
 00-4-2 (page 1 only)

**DIVISION, UNIT, OR FUNCTION:**  
 Public Health Initiatives Branch – AIDS and Chronic Diseases Section

**RMLO (type or print):**  
 Lisa Kessler

**JOB TITLE OF RMLO (type or print):**  
 Staff Attorney

**APPROVED (Signature of State Archivist):**

**DATE SIGNED:**

4/5/2012

**APPROVED (Signature of RMLO):**

**DATE SIGNED:**

3/30/12

**APPROVED (Signature of Public Records Administrator):**

**EFFECTIVE DATE OF SCHEDULE:**

4/9/2012

General Statutes of Connecticut (CGS) §19a-2a thru §19a-215

Public Health Code (Conn. Agencies Regs.) §19a-36-A3 thru §19a-36-A4 (reportable diseases only)

Acronyms used on this schedule:

- Department of Public Health (DPH)
- Centers for Disease Control and Prevention (CDC)
- Human immunodeficiency virus (HIV)

Acquired immunodeficiency syndrome (AIDS)

| Series # | Records Series Title | Description | Retention | Disposition | Notes |
|----------|----------------------|-------------|-----------|-------------|-------|
|----------|----------------------|-------------|-----------|-------------|-------|

**A. HIV/AIDS Surveillance Program**

|     |  |  |                                   |   |  |
|-----|--|--|-----------------------------------|---|--|
| 01. | <b>HIV/AIDS Confidential Case Report Forms</b>         | This series documents the report of cases of HIV infection by faculties or providers to DPH. Including but not limited to: Adult HIV/AIDS Confidential Case Report (Form OMB No. 0920-0009) [also known as "AIDS Case Report"] and Pediatric HIV/AIDS Confidential Case Report Form (Form CDC 50.42B). | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |
| 02. | <b>Laboratory Report of Significant Findings Forms</b> | This series documents the report of cases of reportable diseases by laboratories to DPH. Including but not limited to: Laboratory Report of Significant Findings, Diseases Relating to Public Health (Form OL-15C).  | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |

**RECORDS RETENTION SCHEDULE**  
**DEPARTMENT OF PUBLIC HEALTH**

Form RC-050 (Revised 02/2012)



STATE OF CONNECTICUT  
Connecticut State Library  
Office of the Public Records Administrator  
231 Capitol Avenue, Hartford, CT 06106  
[www.cslib.org/publicrecords](http://www.cslib.org/publicrecords)

**RECORDS RETENTION**  
**SCHEDULE #**  
12-2-2

| Series #                         | Records Series Title                                      | Description   | Retention                         | Disposition                                 | Notes  |
|----------------------------------|---|---|-----------------------------------|---|--|
| 03.                              | <b>Physician Case Report Forms</b>                        | This series documents the report of cases of reportable diseases by physicians to DPH. Including but not limited to: Reportable Disease Confidential Case Report (Form PD-23).  | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |
| <b>B. HIV Prevention Program</b> |   |   |                                   |   |  |
| 04.                              | <b>HIV Test Forms (OMB No. 0920-0696)</b>                 | This series documents demographic information on clients who receive an HIV test. This information is subsequently entered into XPems, a CDC reporting system.  | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |
| 05.                              | <b>HIV Counseling and Testing Data Forms</b>              | This series documents information included in quarterly reports from HIV Prevention contractors and provides more HIV testing information than what is captured in XPems.   | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |
| 06.                              | <b>HIV Counseling and Testing Site Profile Records</b>    | This series documents site specific demographic profiles of HIV counseling and testing sites and is updated in quarterly and monthly reports from HIV Prevention contractors and used to update site information in XPems.          | 2 years from date records created | Destroy after receipt of signed Form RC-108 |  |
| 07.                              | <b>HIV Counselor Certificate Training Program Records</b> | This series documents the training and certification of HIV Prevention Counselors by DPH. Including but not limited to: waivers; applications; performance appraisals; records of certificate actions; and recertification actions. | 3 years from date records created | Destroy after receipt of signed Form RC-108 | HIV Prevention Counselor Certificates expire at the end of each fiscal year (June 30 <sup>th</sup> ) and are automatically renewed if the holder has attended the required number of continuing education workshops. |
| 08.                              | <b>AIDS Educator Certificate Training Program Records</b> | This series documents the training and certification of AIDS Educators by DPH. Including but not limited to: records of certificate actions and recertification actions.  | 3 years from date records created | Destroy after receipt of signed Form RC-108 |  |

# RECORDS RETENTION SCHEDULE DEPARTMENT OF PUBLIC HEALTH

Form RC-050 (Revised 02/2012)




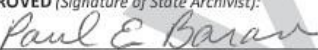
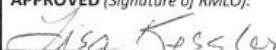

STATE OF CONNECTICUT  
Connecticut State Library  
Office of the Public Records Administrator  
231 Capitol Avenue, Hartford, CT 06106  
[www.cslib.org/publicrecords](http://www.cslib.org/publicrecords)


## RECORDS RETENTION SCHEDULE #

12-2-2

1. **SCOPE:** This schedule lists records unique to the Department of Public Health (DPH) and is used in conjunction with the General Records Retention Schedules and other relevant Records Retention Schedules.
2. **AUTHORITY:** The Office of the Public Records Administrator issues this Records Retention Schedule under the authority granted by §11-8 and §11-8a of the *General Statutes of Connecticut* (CGS).
3. **RETENTION PERIODS:** Retention periods listed on this schedule are based on the records' administrative, fiscal, legal, and historical values, as well as statutory or regulatory requirements. In most instances the established period sets the minimum retention requirement. However, some records have maximum retention periods set by Federal or State statutes or regulations. Please note that any statute or regulation listed in brackets in the "Retention" column indicates the legal citation for that retention requirement. If a records series states, "Permanent/Archival," the agency should request approval to transfer the records to the State Archives or an approved archival repository once the records are inactive. If a records series states, "May contain historical value," the agency should contact the State Archives for archival appraisal before requesting disposition of the records. Not all such records will be determined to be archival; conversely, some records without this statement might have archival value. See General Letter #2009-1 for guidelines on transferring records to the State Archives.
4. **FORMAT:** Retention periods listed on this schedule apply to the official record copy, whether in paper, electronic, or other format. If records are maintained only in an electronic system, the records custodian must be able to retrieve and interpret the content for the retention period.
5. **DISPOSITION AUTHORIZATION:** This schedule is used concurrently with the *Records Disposition Authorization* (Form RC-108), which is used to request permission to destroy or transfer records that have met their retention period. The agency Records Management Liaison Officer (RMLO), the State Archivist, and the Public Records Administrator must sign the authorization form *prior* to destruction or transfer of public records. The Office of the Public Records Administrator cannot grant continuing approval to destroy records on an ongoing basis. No records may be destroyed if there are pending or active Freedom of Information Act (FOIA) requests; litigations; investigations; audits; or other cases, claims, or actions. Note that if there is a destruction hold placed on records, the retention period does not change and once the hold is lifted, the records may be destroyed after receipt of the signed Form RC-108.
6. **DISPOSITION DUE TO REFORMATTING:** Records custodians may request permission to dispose of original records that have been scanned provided the retention period is 10 years or less and the agency has submitted a *Certificate of Compliance* in accordance with the State Library's *Standards for the Use of Imaging Technology for Storage, Retrieval, and Disposition of Public Records*. With certain exceptions, custodians may request permission to dispose of original records that have been microfilmed provided the agency has submitted a *Certificate of Compliance* in accordance with the State Library's *Required Minimum Microfilming Standards for Public Records*.
7. **AUDIT REQUIREMENTS:** Under the Single Audit Act (31 USC 7501) audit requirements apply to Federal, State, and Local programs. The retention requirement, "\_\_\_ years, or until audited, whichever is later," requires further explanation. In most instances "audit" refers to the general agency audit conducted by the State Auditors of Public Accounts or the general town or municipal audit conducted by an outside auditing agency, unless otherwise noted. The specific record itself may or may not have been examined as part of the audit process. The requirement of "until audited" is fulfilled when the official audit report is issued. The auditors may recommend that certain records be corrected. Such records, even when they meet retention requirements, must be retained during the period that any review is pending.
8. **FOIA DISCLOSURE:** This retention schedule governs the retention of public records – not the disclosure of public records. Refer to CGS §1-200 et seq. or contact the Office of Governmental Accountability, Freedom of Information Commission (FOIC), regarding the disclosure of public records.
9. **ESSENTIAL RECORDS:** Records designated as "Essential" are those records necessary to respond to an emergency; to reestablish normal operations after any such emergency; to protect the rights and interests of the agency; and to protect the rights and interests of individuals for whom it has responsibility.
10. **OBSOLETE RECORDS:** Records designated as "OBSOLETE" or "SERIES CLOSED" are no longer created or received in the normal course of business. Records custodians should request approval for the appropriate disposition of any records so designated as soon as the retention period has passed.
11. **RECORDS CREATION REQUIREMENT:** Nothing on this schedule mandates the creation of a record or records series if the agency does not already create or receive it in the normal course of business. However, agencies should be aware of any additional recordkeeping requirements established by state or federal statute or regulation.


(First page of the retention schedule for HIV surveillance related forms.)

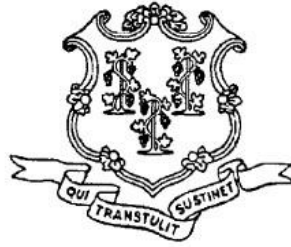
| <b>RECORDS RETENTION SCHEDULE</b><br><b>Department of Public Health - Infectious Disease Unit</b><br>Form RC-050 (Revised 02/2012) |   |  STATE OF CONNECTICUT<br>Connecticut State Library<br>Office of the Public Records Administrator<br>231 Capitol Avenue, Hartford, CT 06106<br><a href="http://www.cslib.org/publicrecords">www.cslib.org/publicrecords</a> |   | <b>RECORDS RETENTION SCHEDULE #</b><br><u>13-1-2</u>  |   |
|--|---|--|---|---|---|
| <b>AGENCY:</b><br>Department of Public Health (DPH)  |   | <b>AGENCY ADDRESS:</b><br>410 Capitol Avenue, Hartford, CT 06106   |   | This schedule is: <input type="checkbox"/> ORIGINAL<br><input checked="" type="checkbox"/> REVISED<br><b>Superseded schedule number(s):</b><br>#00-4-2, Epidemiology (p. 2), STD (p. 3), and Pulmonary (p. 4) |   |
| <b>DIVISION, UNIT, OR FUNCTION:</b><br>Infectious Disease Unit   |   | <b>RELEVANT STATUTES &amp; REGULATIONS AND ACRONYMS USED ON THIS SCHEDULE:</b><br>Connecticut General Statutes §19a-2a thru 19a-215; Public Health Code §9a-36-A3 thru 19a-36-A4   |   |   |   |
| <b>RMLO (type or print):</b><br>Lisa Kessler   | <b>JOB TITLE OF RMLO (type or print):</b><br>Staff Attorney | <b>APPROVED (Signature of State Archivist):</b><br>   |   | <b>DATE SIGNED:</b><br>9/26/2013  |   |
| <b>APPROVED (Signature of RMLO):</b><br>          | <b>DATE SIGNED:</b><br>9/23/13                              | <b>APPROVED (Signature of Public Records Administrator):</b><br>   |   | <b>EFFECTIVE DATE OF SCHEDULE:</b><br>9/27/2013   |   |
| Series #   | Records Series Title  | Description  | Retention   | Disposition   | Notes   |
| <b>A. INFECTIOUS DISEASE SECTION (Administration)</b>  |   |  |   |   |   |
| 01.  | <b>Annual Disease Reports</b>                               | This series documents infectious disease statistics from 1895 to present. Data are arranged by town and disease and by year. The report includes, but is not limited to: Epidemiology, Sexually Transmitted Diseases [STD] and Tuberculosis.   | Permanent   | Retain in agency or transfer to State Archives  |   |
| 02.  | <b>Annual Disease Summary</b>                               | This series summarizes infectious disease statistics by disease and by year from 1895 to present. This report is inclusive, but not limited to: Epidemiology, Sexually Transmitted Diseases [STD] and Tuberculosis.  | Permanent   | Retain in agency or transfer to State Archives  |   |
| <b>B. EPIDEMIOLOGY AND EMERGING INFECTIONS PROGRAM</b>   |   |  |   |   |   |
| 03.  | <b>Reportable Disease and Outbreak Investigation Files</b>  | This series documents the investigation of reportable diseases and outbreaks pursuant to Conn. Agencies Regs. §19a-36-A6. Including but not limited to: written reports, surveys including prevalence studies, background materials, questionnaires, databases and previous studies.                         | 10 years from the date DPH is informed of an outbreak | Destroy after receipt of signed Form RC-108   | The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak. |

| <b>RECORDS RETENTION SCHEDULE</b><br><b>Department of Public Health - Infectious Disease Unit</b><br>Form RC-050 (Revised 02/2012) |   |   |  | STATE OF CONNECTICUT<br>Connecticut State Library<br>Office of the Public Records Administrator<br>231 Capitol Avenue, Hartford, CT 06106<br><a href="http://www.cslib.org/publicrecords">www.cslib.org/publicrecords</a> | <b>RECORDS RETENTION SCHEDULE #</b><br><u>13-1-2</u>  |
|--|---|---|--|---|---|
| Series #   | Records Series Title  | Description   | Retention  | Disposition   | Notes   |
| 04.  | <b>Reportable Disease Forms</b>   | This series documents diseases reported by persons or laboratories required to report or where laboratory evidence suggests a Reportable Disease found on the current Reportable Diseases List pursuant to CGS §19a-2a. Including but not limited to: Reportable Disease Confidential Case Report Form (PD-23) and Laboratory Report of Significant findings form (OL-15C) and DPH summaries. | 3 years from date reported   | Destroy after receipt of signed Form RC-108   |   |
| 05.  | <b>Reportable Disease and Outbreak Investigation Files – Supporting Documentation</b> | This series documents the investigation of reportable diseases and outbreaks pursuant to Connecticut Agencies Regs. Sections 19a-36-A6. Including, but not limited to supporting documentation including surveys, background materials, questionnaires, databases and previous studies.   | 1 year from the date DPH is informed of an outbreak                                | Destroy after receipt of signed Form RC-108   | The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak. |
| 06.  | <b>Reportable Disease Special Research Projects</b>                                   | This series documents special research projects (i.e. Lyme disease, emerging infections), either federally or outside funded, including, but not limited to Yale Emerging Infections Program. Including, but not limited to surveys, background materials, questionnaires, databases and previous studies.  | 3 years after DPH notification of outbreak   | Destroy after receipt of signed Form RC-108   |   |
| <b>C. HEALTHCARE ASSOCIATED INFECTIONS (HAI) PROGRAM</b>   |   |   |  |   |   |
| 07.  | <b>Healthcare Associated Infections (HAI) Reportable Disease Validation Records</b>   | This series documents data collected during chart audits of health facility patients who may be eligible to be reported to DPH as a case of healthcare associated infection. These records are distinct from standard reportable disease forms. They are used to determine the accuracy and completeness of healthcare facility reporting of publicly reportable HAIs                         | 3 years  | Destroy after receipt of signed Form RC-108   |   |

|  |  |   |  |
|--|--|---|--|
| <b>RECORDS RETENTION SCHEDULE</b><br><b>Department of Public Health - Infectious Disease Unit</b><br>Form RC-050 (Revised 02/2012) |  | STATE OF CONNECTICUT<br>Connecticut State Library<br>Office of the Public Records Administrator<br>231 Capitol Avenue, Hartford, CT 06106<br><a href="http://www.cslib.org/publicrecords">www.cslib.org/publicrecords</a> | <b>RECORDS RETENTION SCHEDULE #</b><br><u>13-1-2</u> |
|--|--|---|--|

| Series #   | Records Series Title                            | Description  | Retention | Disposition                                    | Notes   |
|--|---|--|-----------|--|---|
| 08.  | Annual Public Health Reports to the Legislature | This series documents legislatively mandated annual reports to the chairs of the Public Health Committee summarizing data on publicly reportable HAIs in healthcare facilities in Connecticut.   | Permanent | Retain in agency                               | These reports are also posted to the DPH website pursuant to CGS § 19a-490a.<br><br>The agency also retains the records of Advisory Committee on Healthcare Associated Infections established by CGS § 19a-490n. See S1 for retention requirements. |
| <b>D. SEXUALLY TRANSMITTED DISEASE (STD) PROGRAM</b> |   |  |           |  |   |
| 09.  | STD Case Reporting Forms                        | This series documents sexually transmitted diseases reported by persons or laboratories required to report or where laboratory evidence suggests an STD. Includes but is not limited to STD Case Report (STD-23) and Laboratory Report of Significant Findings (OL-15C) that are specific for STDs.  | 3 years   | Destroy after receipt of signed Form RC-108    |   |
| 10.  | STD Epidemiological Records                     | This series documents reports to the federal Center for Disease Control [CDC] of individual cases of STDs including Syphilis. Includes but is not limited to field and interview records used to gather information on individual patients.  | 3 years   | Destroy after receipt of signed Form RC-108    |   |
| 11.  | Syphilis Case Reports, Monthly                  | [Obsolete] This series documents internal program monthly and annual summaries of syphilis cases reported in the state, 2000 - 2010.   | 3 years   | Destroy after receipt of signed Form RC-108    |   |
| 12.  | STD Summary Morbidity Reports                   | [Obsolete] This series documents summaries of STD cases diagnosed in the state as well as quarterly and annual reports made to CDC. This includes but is not limited to STD Quarterly/Annual Morbidity Report, Annual Report, Civilian Cases of Primary, Secondary and Early Latent Syphilis and Gonorrhea and Quarterly Epidemiological Activity for Venereal Disease Report. | Permanent | Retain in agency or transfer to State Archives |   |

| <b>RECORDS RETENTION SCHEDULE</b><br><b>Department of Public Health - Infectious Disease Unit</b><br>Form RC-050 (Revised 02/2012) |  |  STATE OF CONNECTICUT<br>Connecticut State Library<br>Office of the Public Records Administrator<br>231 Capitol Avenue, Hartford, CT 06106<br><a href="http://www.cslib.org/publicrecords">www.cslib.org/publicrecords</a>        |  | <b>RECORDS RETENTION SCHEDULE #</b><br><u>13-1-2</u> |  |
|--|--|---|--|--|--|
| Series #   | Records Series Title   | Description   | Retention  | Disposition  | Notes  |
| <b>E. TUBERCULOSIS (TB) CONTROL PROGRAM</b>  |  |   |  |  |  |
| 13.  | <b>Patient Files, Active TB (Numerical)</b>                    | This series documents information for patients diagnosed with tuberculosis disease. This includes but is not limited to physician and laboratory report forms, clinical information, contact investigation forms and master index card with medication information.   | 10 years onsite; 60 years offsite  | Destroy after receipt of signed Form RC-108          | *It is necessary to retain TB patient records for up to 70 years because persons who have latent TB infection or TB disease have a life-time risk of developing active TB or recurrent TB. |
| 14.  | <b>Patient Files, Latent TB (Alphabetical)</b>                 | This series documents information for patients diagnosed with latent tuberculosis infection. This includes but is not limited to physician and laboratory report forms, clinical information, contact investigation forms and master index cards with medication information.                                       | 10 years onsite; 60 years offsite  | Destroy after receipt of signed Form RC-108          | *It is necessary to retain TB patient records for up to 70 years because persons who have latent TB infection or TB disease have a life-time risk of developing active TB or recurrent TB. |
| 15.  | <b>Patient Files, Active TB – Master Index Cards</b>           | [Obsolete] This series documents a variety of finding aids for access to files of patients with diagnosed tuberculosis disease.   | 10 years onsite; 60 years offsite  | Destroy after receipt of signed Form RC-108          | The master card indexes end in 2013 when the last file index was computerized.   |
| 16.  | <b>Verified TB Cases Reports</b>                               | This series documents reports to the federal Center for Disease Control [CDC] of individual tuberculosis cases.   | 3 years  | Destroy after receipt of signed Form RC-108          |  |
| 17.  | <b>Federal Grant / Programmatic Materials</b>                  | This series documents federal program and grant management. This includes but is not limited to grant and program activity reports made to CDC.   | 3 years from the date of the last expenditure report submitted for the funding period [45 CFR 92.42] | Destroy after receipt of signed Form RC-108          |  |
| 18.  | <b>Refugee Health Assessment Records</b>                       | This series documents medical follow-up for persons entering Connecticut as refugees. This includes but is not limited to health care provider forms and test results.  | 10 years   | Destroy after receipt of signed Form RC-108          |  |
| 19.  | <b>Refugee Arrival Forms/Class A/B Immigrant Arrival Forms</b> | This series documents information received informing the state of refugees and immigrants arriving in Connecticut with overseas TB classifications that require medical and public health follow-up. This includes but is not limited to notification forms and support documents from CDC and other organizations. | 3 years  | Destroy after receipt of signed Form RC-108          |  |



# **State of Connecticut Department of Public Health (DPH)**



## **IT Disaster Recovery Plan For e-HARS MS Servers**

## **Table of Contents**

|  |  |
|--|--|
| Information Technology Statement of Intent.....        |  |
| 1 Plan Overview.....                                   |  |
| 1.1 Major goals of this plan.....                      |  |
| 2 Backup procedures.....                               |  |
| 2.1 Needed to restore data at alternate locations..... |  |
| 3 Impact assessment.....                               |  |
| 3.1 Extent of outage assessment form.....              |  |
| 4 Maximum Tolerable Outage (MTO) Defined.....          |  |
| 5 Restoration order - highest in importance.....       |  |
| 6 Plan invocation.....                                 |  |
| 6.1 Notification.....                                  |  |
| 7 Contact with Employees.....                          |  |
| 8 Monitor progress.....                                |  |
| 9 Legal actions.....                                   |  |
| 10 DRP exercises.....                                  |  |
| 11 Disaster recovery activity report.....              |  |
| 12 Disaster Recovery Flow Chart.....                   |  |
| 13 Internal Notification calling Tree Flow Chart.....  |  |
| 14 Internal Notification Contact.....                  |  |
| 15 External contacts calling tree Flow Chart.....      |  |
| 16 External Contacts.....                              |  |
| 17 Disaster Recovery plan for <eHARS Staging>.....     |  |
| 18 Disaster Recovery plan for <eHARS Production>.....  |  |
| 19 Disaster Recovery plan for <SQL eHARS DB>.....      |  |

## **Information Technology Statement of Intent**

This document delineates DPH's policies and procedures for technology disaster recovery, as well as the process-level plans for recovering any or all of the following servers; **e-HARS** MS Servers. This document summarizes DPH's recommended procedures, to ensure these specific system's uptime, data integrity and availability, and business continuity. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

### **1 Plan Overview**

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

If an alternate site is utilized to restore server/system functionality, then all of the same security standards that were implemented at the primary location to protect the site, servers & data will be implemented at the new location.

#### **1.1 Major goals of this plan**

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

### **2 Backup Procedures**

DPH's backup strategy

- Incremental backups will be taken every Monday through Thursday using ARCserve,
- Full backups will be taken every Friday using ARCserve
- Monthly backups will be taken at the end of every month using ARCserve
- Yearly backups will be taken once a year at the end of every December using ARCserve
- Every week tapes will be sent to William B. Meyer's for offsite storage.
- A session password is utilized to encrypt and decrypt the data that is stored on the backup tapes.

- Test restores are done once a month to make sure backup procedures are functioning properly and data is able to be restored from the tapes.
- Per recommendations from Dell, tapes are only used a total of 75 times and then discarded, this is to ensure media integrity.

## 2.1 Needed to restore data at alternate location

- Replacement Servers
- Tape Library with LTO-5 drive
- The same version of ARCserve.
- The original session password that was utilized to encrypt the tapes.
- Follow the same restore procedure utilized at the primary site.

### \*\*\*Note\*\*\*

A copy of the session password that is utilized for encryption and decryption of data is stored within a password protected file on a secure network drive (Only Network Administrators have access to the folder). If needed, there is also a hard copy of the password information saved in the IT DPT's safe.

## 3 Impact assessment

Using the following steps, the disaster recovery team will determine the seriousness of the incident and to what extent the business is impacted:

1. Define the extent of the outage
2. Determine the possible effects to internal and external users
3. Make a decision based on the results from Step 2 to mitigate the outage

### 3.1 Extent of outage assessment form

| Server Affected | Description Of Problem | Extent Of Damage |
|-----------------|------------------------|------------------|
|                 |                        |                  |
|                 |                        |                  |
|                 |                        |                  |
|                 |                        |                  |
|                 |                        |                  |
|                 |                        |                  |
|                 |                        |                  |

## 4 Maximum Tolerable Outage (MTO)

The maximum length of time the specific server function can be unavailable without causing unacceptable consequences.

The attached chart indicates the Maximum Tolerable Outage (MTO) time per server. The standard fix processes will be utilized if the server\servers can be restored to normal

functionality within these time frames. The supervisor responsible for managing the outage will decide whether or not the situation warrants declaring a disaster when the server/servers cannot be restored within the Maximum Tolerable Outage (MTO) time frame.

| <b>Application Name</b> | <b>Application Server Name</b> | <b>Database Server Name</b> | <b>Maximum tolerable Outage (MTO)</b> |
|-------------------------|--------------------------------|-----------------------------|---------------------------------------|
| EHars                   | DPH-AP036 Staging              | DPH-SQL018 Staging          | 12-24 hrs                             |
| EHars                   | DPH-AP037 Production           | DPH-SQL017 Production       | 12-24 hrs                             |
| EHars                   | DPH-SQL009 DB                  |                             | 12-24 hrs                             |
|                         |                                |                             |                                       |
|                         |                                |                             |                                       |
|                         |                                |                             |                                       |
|                         |                                |                             |                                       |

## 5 Restoration order

In a multi-server failure, the attached chart indicates what servers are considered the most critical and should be restored to full functionality first. If multiple systems with the same priority rating are down, the supervisor responsible for managing the outage will decide the order of system restoration.

| <b>Server Name</b> | <b>Application</b> | <b>1 indicates the highest in importance, the most business critical.</b> |
|--------------------|--------------------|---|
| DPH-AP036          | EHARS Staging      | 1   |
| DPH-AP037          | EHARS Production   | 1   |
| DPH-SQL009         | EHARS DB           | 1   |
|                    |                    |   |
|                    |                    |   |

## 6 Plan invocation

There are many potential disruptive threats which can occur at any time and affect the normal business process. DPH has considered a wide range of potential threats and each potential emergency situation has been examined.

Potential threats that could cause the **e-HARS** servers to fail

- Corrupted File System due to system crash
- File system damaged to automatic volume repair utilities
- File system corruption due partition/volume resizing utilities
- Corrupt volume management settings
- Server hardware upgrades (Storage Controller Firmware, BIOS, RAID Firmware)
- Expanding Storage Array capacity by adding larger drives to controller
- Failed Array Controller
- Failed drive on Storage Array
- Storage Array failure but drives are working
- Failed boot drive
- Migration to new Storage Array system
- Mechanical failure brought about by manufacturing fault
- Bad RAM, network adapter, or other hardware on the server
- Extremes of temperature (too hot or too cold)
- Faulty system software, software incompatibilities, driver conflicts
- Server OS upgrades (Service Packs, Patches to OS)
- Migration to different OS
- Power problems while server is in use (surges, failures, brownouts, etc.)
- Natural disasters: Floods, Tornados, Hurricanes, Earthquakes, and Blizzards
- Flooding from broken water pipes

### 6.1 Notification

The person discovering the incident will Respond immediately and utilize the Notification Calling Tree to alert the appropriate personnel.

The primary contact on the calling tree will ensure that the appropriate personnel are notified and allocate responsibilities and activities as required. The Disaster Recovery Team (DRT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the performance of the **e-HARS MS** systems.

## **7 Contact with Employees**

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's backup to relay information on the disaster.

## **8 Monitor progress**

The supervisor responsible for managing the outage will continuously monitor the disaster recovery operations progress.

The key objectives:

- Identifying problems
- Making adjustments to the recovery operations as needed.
- Assessing whether the Disaster Recovery process is being implemented as planned
- Ensuring that the restoration schedule is being met
- Shutting down the disaster recovery operation once functionality has been returned to normal

## **9 Legal Actions**

The DPH's legal department will review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

## **10 DRP Exercises**

Disaster recovery plan exercises are an essential part of the DPH's development process. These exercising will ensure that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

The key objectives:

- Test the recovery processes and procedures.
- Familiarize staff with the recovery process and documentation.
- Verify the effectiveness of the recovery documentation.
- Establish if the recovery objectives are achievable.

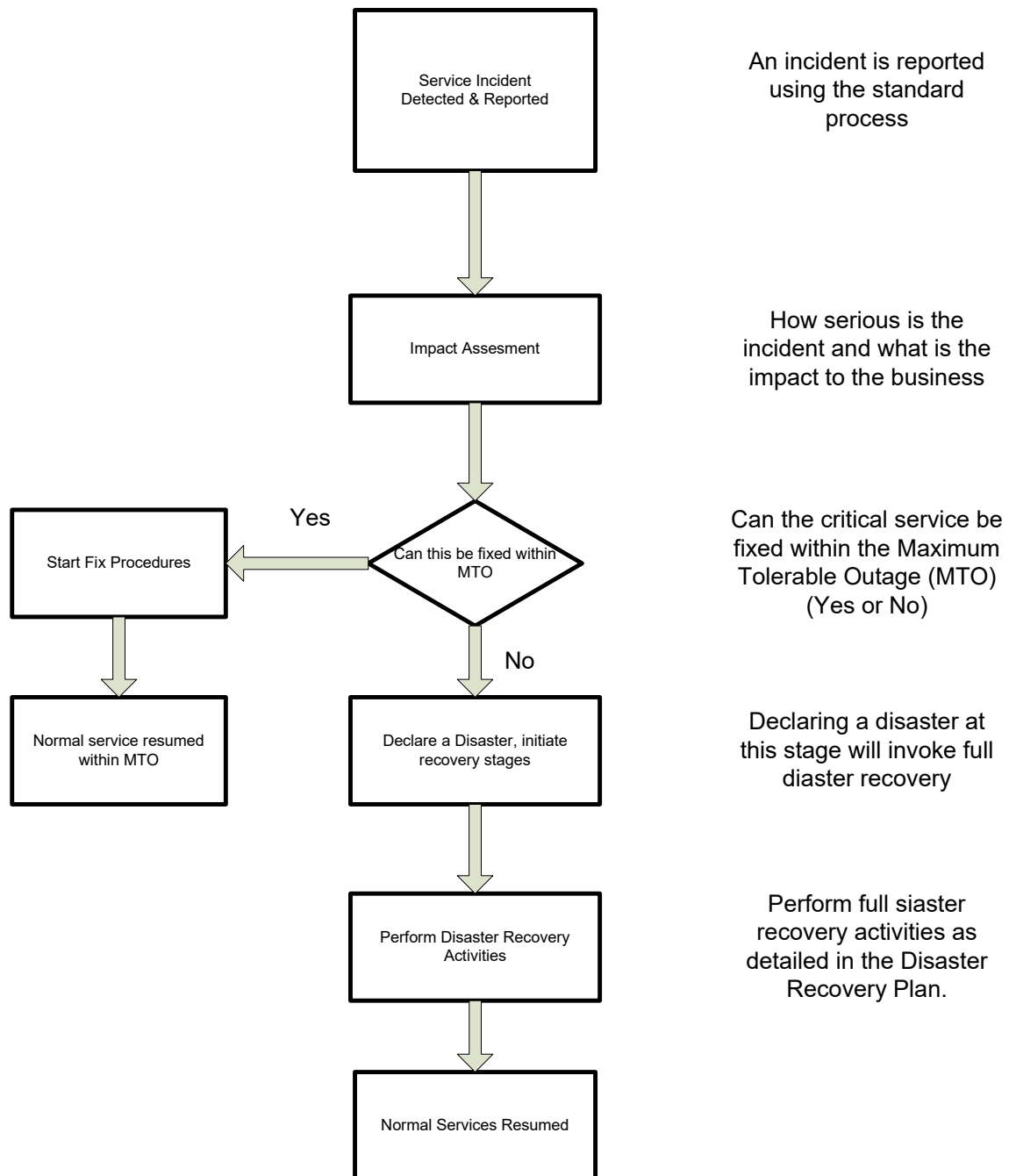
## **11 Disaster Recovery Activity Report**

On completion of the disaster recovery response the DRT leader will prepare a report on the activities undertaken.

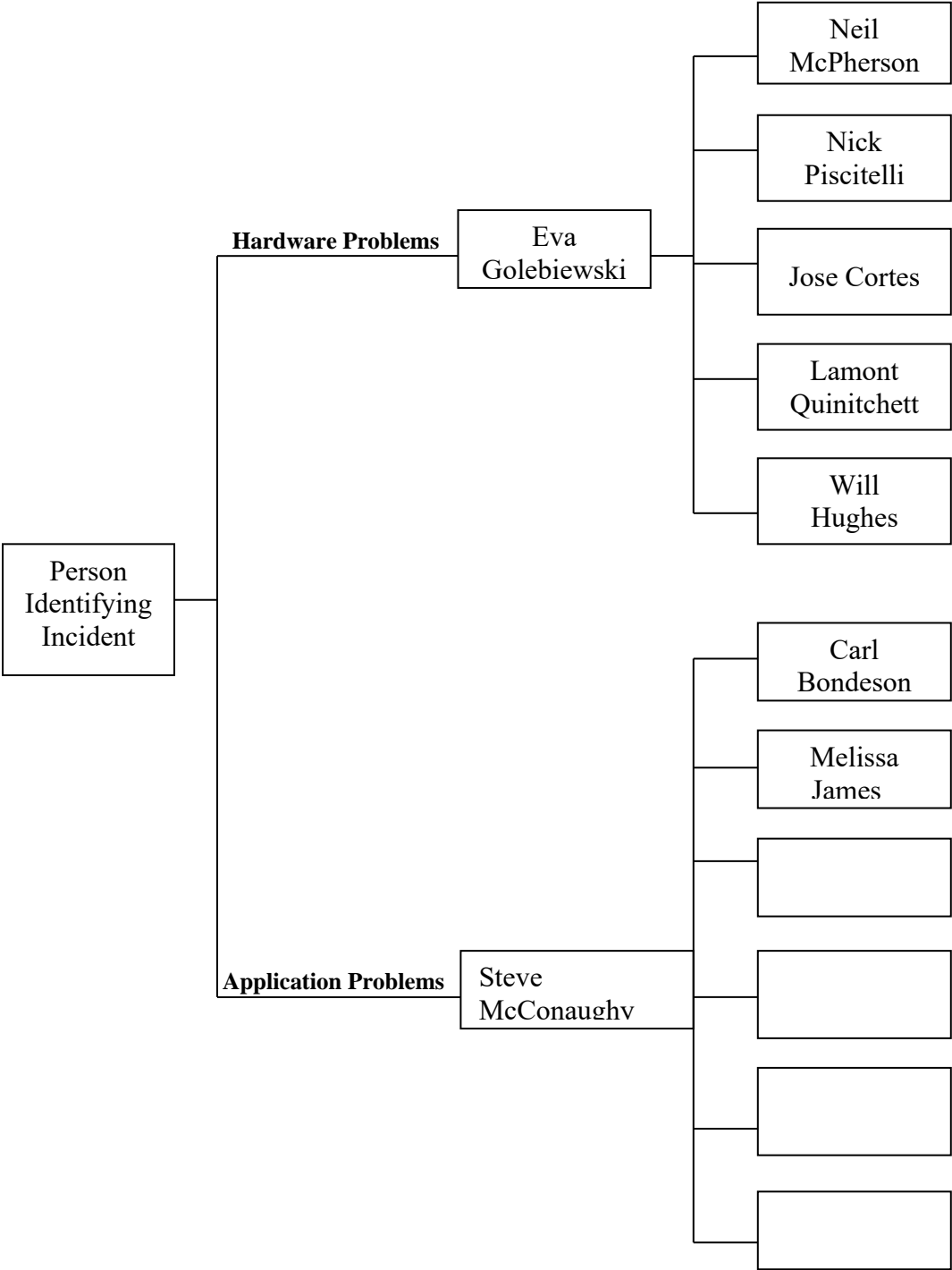
The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the Disaster Recovery Team (DRT)
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Lessons learned

## Disaster Recovery Flow Chart



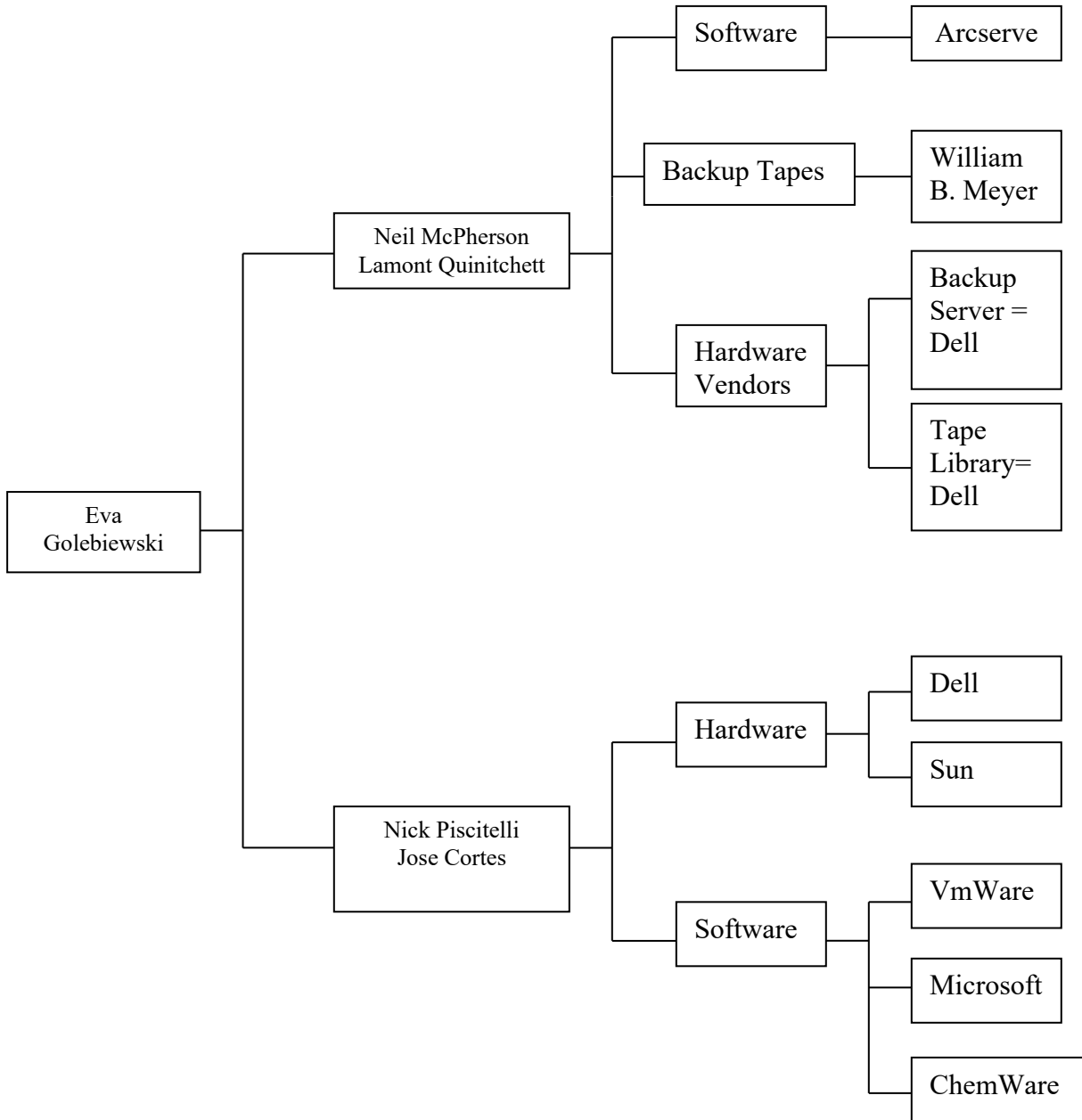
Internal Notification Calling Tree Flow Chart



## Internal Notification Contact Info

| Name, Title             | Contact Option | Contact Number                    |
|-------------------------|----------------|-----------------------------------|
| <b>Eva Golebiewski</b>  | Work           | <b>860-509-7430</b>               |
|                         | Mobile         | <b>860-680-6964</b>               |
|                         | Email Address  | <b>Eva.Golebiewski@ct.gov</b>     |
| <b>Nick Piscitelli</b>  | Work           | <b>860-509-8145</b>               |
|                         | Mobile         | <b>203-499-8019</b>               |
|                         | Email Address  | <b>Nicholas.Piscitelli@ct.gov</b> |
| <b>Jose Cortes</b>      | Work           | <b>860-509-7681</b>               |
|                         | Mobile         |                                   |
|                         | Email Address  | <b>Jose.Cortes@ct.gov</b>         |
| <b>Neil McPherson</b>   | Work           | <b>860-509-7254</b>               |
|                         | Mobile         | <b>203-675-4616</b>               |
|                         | Email Address  | <b>Neil.McPherson@ct.gov</b>      |
| <b>Will Hughes</b>      | Work           | <b>860-509-7679</b>               |
|                         | Mobile         |                                   |
|                         | Email Address  | <b>William.Hughes@ct.gov</b>      |
| <b>Steve McConaughy</b> | Work           | <b>860-509-7273</b>               |
|                         | Mobile         |                                   |
|                         | Email Address  | <b>Stephen.McConaughy@ct.gov</b>  |
|                         | Work           |                                   |
|                         | Mobile         |                                   |
|                         | Email Address  |                                   |
| <b>Carl Bondeson</b>    | Work           | <b>860-509-7434</b>               |
|                         | Mobile         |                                   |
|                         | Email Address  | <b>Carl.Bondeson@ct.gov</b>       |
|                         | Work           |                                   |
|                         | Mobile         |                                   |
|                         | Email Address  |                                   |
|                         | Work           |                                   |
|                         | Mobile         |                                   |
|                         | Email Address  |                                   |

## External Contacts Calling Tree Flow Chart



## External Contacts

| <b>Name, Title</b>                  | <b>Contact Option</b> | <b>Contact Number</b>               |
|-------------------------------------|-----------------------|-------------------------------------|
| William B. Meyer                    | Phone                 | <b>(855) 291-8301</b>               |
|                                     |                       |                                     |
| Dell                                | Phone                 | <b>1-800-981-3355</b>               |
|                                     |                       |                                     |
| Oracle support<br>(For Sun Systems) | Phone                 | <b>1.800.223.1711</b>               |
|                                     | On-Line               | <b>support.oracle.com</b>           |
|                                     |                       |                                     |
| VmWare                              | Phone                 | <b>877-486-9273 or 650-475-5345</b> |
|                                     |                       |                                     |
| Microsoft                           | Phone                 | <b>1-800-642-7676</b>               |
|                                     |                       |                                     |
| Arcserve                            | Phone                 | <b>1-800-225-5224</b>               |
|                                     |                       |                                     |
|                                     |                       |                                     |

# Disaster Recovery Plans

## Disaster Recovery Plan for <e-Hars Server >

|   |  |
|---|--|
| <b>SYSTEM</b>                               | <b>DPH-AP036</b>   |
| <b>OVERVIEW</b>                             |  |
| <b>PRODUCTION SERVER</b>                    | Location: <b>3<sup>rd</sup> floor data center, Location 13-160</b><br>Server Model: <b>Virtual</b><br>Operating System: <b>2008 R2 Standard SP1 64-bit</b><br>CPUs: <b>Intel Xeon X5660 @ 2.80GHz (2)</b><br>Memory: <b>4 GB</b><br>Total Disk: <b>50 GB</b><br>DNS Entry: <b>DPH-AP009</b><br>IP Address:               |
| <b>APPLICATIONS</b>                         | EHARS Staging  |
| <b>ASSOCIATED SERVERS</b>                   | DPH-AP037, DPH-SQL009  |
| <b>KEY CONTACTS</b>                         |  |
| Hardware Vendor                             | Dell   |
| System Owners                               | Eva Golebiewski  |
| <i>Business Unit</i>                        | <i>Epidemiology</i>  |
| Application Owners                          | Stephen McConaughy   |
| <b>BACKUP STRATEGY FOR SYSTEM ONE</b>       |  |
| Daily                                       | Utilizing ARCserve, incremental backups every Monday - Thursday  |
| Weekly                                      | Utilizing ARCserve, full backups every Friday  |
| <b>DISASTER RECOVERY PROCEDURE</b>          |  |
| <u>Scenario 1</u><br><br>Total Loss of Data | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Identify latest backup (Tapes)</li> <li>• Restore missing information from the backup tapes</li> <li>• Validate and return to service</li> </ul>  |
| <u>Scenario 2</u><br><br>Total Loss of HW   | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Initiate hardware procurement</li> <li>• OS install/Backup agent install</li> <li>• Restore missing information from the backup tapes to the new server</li> <li>• Perform system test, Validate and return to service</li> </ul> |

## 18 Disaster Recovery Plan for <e-Hars Server >

|   |  |
|---|--|
| <b>SYSTEM</b>                               | <b>DPH-AP037</b>   |
| <b>OVERVIEW</b>                             |  |
| <b>PRODUCTION SERVER</b>                    | Location: <b>3<sup>rd</sup> floor data center, Location 13-160</b><br>Server Model: <b>Virtual</b><br>Operating System: <b>2008 R2 Standard SP1 64-bit</b><br>CPUs: <b>Intel Xeon X5550 @ 2.67GHz (2)</b><br>Memory: <b>4 GB</b><br>Total Disk: <b>50 GB</b><br>DNS Entry: <b>DPH-AP010</b><br>IP Address:               |
| <b>APPLICATIONS</b>                         | EHARS Production   |
| <b>ASSOCIATED SERVERS</b>                   | DPH-AP036, DPH-SQL009  |
| <b>KEY CONTACTS</b>                         |  |
| Hardware Vendor                             | Dell   |
| System Owners                               | Eva Golebiewski  |
| <i>Business Unit</i>                        | <i>Epidemiology</i>  |
| Application Owners                          | Stephen McConaughy   |
| <b>BACKUP STRATEGY FOR SYSTEM ONE</b>       |  |
| Daily                                       | Utilizing ARCserve, incremental backups every Monday - Thursday  |
| Weekly                                      | Utilizing ARCserve, full backups every Friday  |
| <b>DISASTER RECOVERY PROCEDURE</b>          |  |
| <u>Scenario 1</u><br><br>Total Loss of Data | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Identify latest backup (Tapes)</li> <li>• Restore missing information from the backup tapes</li> <li>• Validate and return to service</li> </ul>  |
| <u>Scenario 2</u><br><br>Total Loss of HW   | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Initiate hardware procurement</li> <li>• OS install/Backup agent install</li> <li>• Restore missing information from the backup tapes to the new server</li> <li>• Perform system test, Validate and return to service</li> </ul> |

## 19 Disaster Recovery Plan for <SQL Server >

|   |  |
|---|--|
| <b>SYSTEM</b>                               | <b>DPH-SQL009</b>  |
| <b>OVERVIEW</b>                             |  |
| <b>PRODUCTION SERVER</b>                    | Location: <b>3<sup>rd</sup> floor data center, Location 13-160</b><br>Server Model: <b>Virtual</b><br>Operating System: <b>2008 R2 Standard</b><br>CPUs: <b>Intel Xeon X5660 @ 2.8 GHZ (2)</b><br>Memory: <b>12 GB</b><br>Total Disk: <b>1.03TB</b><br>DNS Entry: <b>DPH-AP010</b><br>IP Address:                        |
| <b>APPLICATIONS</b>                         | SQL DB/EHARS   |
| <b>ASSOCIATED SERVERS</b>                   |  |
| <b>KEY CONTACTS</b>                         |  |
| Hardware Vendor                             | Dell   |
| System Owners                               | Eva Golebiewski  |
| <i>Business Unit</i>                        | <i>Epidemiology</i>  |
| Application Owners                          | Stephen McConaughy   |
| <b>BACKUP STRATEGY FOR SYSTEM ONE</b>       |  |
| Daily                                       | Utilizing ARCserve, incremental backups every Monday - Thursday  |
| Weekly                                      | Utilizing ARCserve, full backups every Friday  |
| <b>DISASTER RECOVERY PROCEDURE</b>          |  |
| <u>Scenario 1</u><br><br>Total Loss of Data | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Identify latest backup (Tapes)</li> <li>• Restore missing information from the backup tapes</li> <li>• Validate and return to service</li> </ul>  |
| <u>Scenario 2</u><br><br>Total Loss of HW   | <ul style="list-style-type: none"> <li>• Determine the extent of the outage</li> <li>• Initiate hardware procurement</li> <li>• OS install/Backup agent install</li> <li>• Restore missing information from the backup tapes to the new server</li> <li>• Perform system test, Validate and return to service</li> </ul> |

**eHARS-HARMS-HANK Disaster Recovery Plan Roles**

| <b>Name</b>         | <b>Role/Title</b>                               | <b>Phone number</b> |
|---------------------|---|---------------------|
| Delores Greenlee    | Section Chief                                   | (860) 509-7924      |
| Heather Linardos    | Primary Lead – HIV Surveillance Pgm Coordinator | (860) 509-7907      |
| Eva Golebieski      | DPH IT Primary Lead                             | (860) 509-7430      |
| Nicholas Piscitelli | DPH IT Secondary Lead                           | (860) 509-8145      |

| <b>Name of person making changes</b> | <b>Role/Title of person making changes</b>          | <b>Date of change</b> | <b>Version #</b> | <b>Notes</b>     |
|--------------------------------------|---|-----------------------|------------------|------------------|
| Heather Linardos                     | Primary Lead – HIV Surveillance Program Coordinator | 12/2017               | 1.2              | New DSM assigned |
|                                      |   |                       |                  |                  |
|                                      |   |                       |                  |                  |

## Permitted Uses and Disclosures: Exchange for Public Health Activities

*45 Code of Federal Regulations (CFR) 164.512(b)(1)*

The [Health Insurance Portability and Accountability Act \(HIPAA\)](#) governs how [Covered Entities \(CEs\)](#) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization. The Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR) previously issued fact sheets describing how this works when sharing PHI for [treatment](#) and for [health care operations](#). This fact sheet explains, through hypothetical scenarios, how these rules work for disclosures of PHI for public health activities to **public health agencies that are authorized by state or federal law to collect the information they seek**. It also gives a few examples of sharing PHI in support of other important public health policies. While HIPAA requires that the information disclosed is the [minimum](#) information necessary for the purpose, it permits the discloser to reasonably rely on a public health authority's request as to what information is necessary for the public health activities.

**Other laws may apply. This fact sheet discusses only HIPAA.**

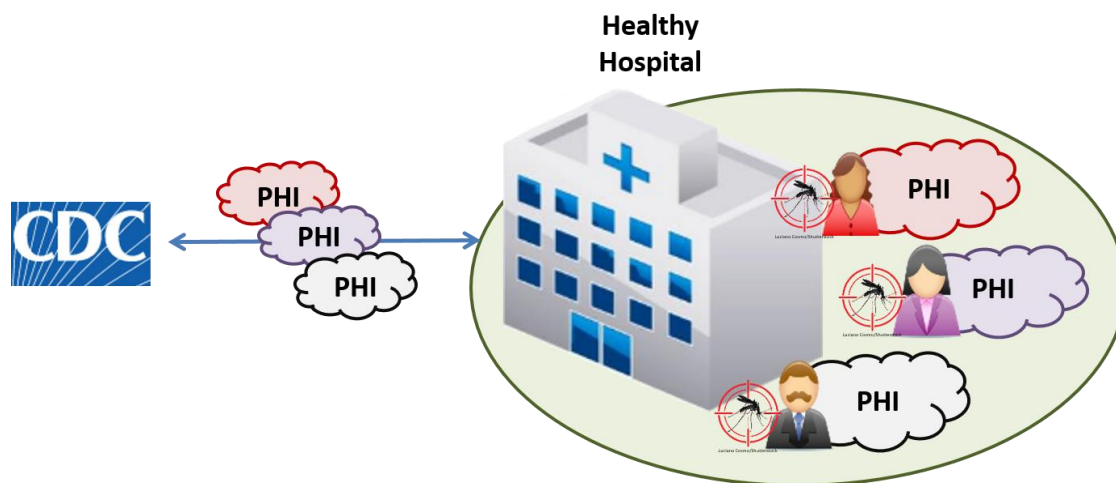
Depending upon the nature and manner of a disclosure, other requirements of the HIPAA [Privacy](#) and [Security](#) Rules may be applicable. For example, if a [Business Associate \(BA\)](#) discloses PHI for public health activities on behalf of a CE, the BA must be authorized to do so in the [BA Agreement \(BAA\)](#) it has with the CE. For any of the scenarios below in which electronic PHI is disclosed, the discloser must meet the HIPAA Security Rule requirements. All the scenarios apply to all types of CEs, whether they use health information technology (health IT) certified by ONC or other forms of electronic transmission.

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 1: Exchange for Reporting of Disease

Healthy Hospital is located in the City of Sunshine, which has had a recent increase in the number of confirmed cases of the Zika virus.

The U.S. Centers for Disease Control and Prevention (CDC), acting in its capacity as a public health authority and authorized by law to collect disease surveillance information, requests that Healthy Hospital report PHI on an ongoing basis for all prior and prospective cases of patients exposed to the Zika virus, whether suspected or confirmed. Healthy Hospital may use health IT certified by the ONC Health IT Certification program (“certified health IT”) to disclose PHI to the CDC in response to the request and may reasonably rely on CDC’s request as to the PHI needed. Healthy Hospital must meet the requirements of the HIPAA Security Rule if providing electronic PHI to CDC. The CDC’s ability to collect this type of information extends to all public health information within the scope of CDC’s public health authority.

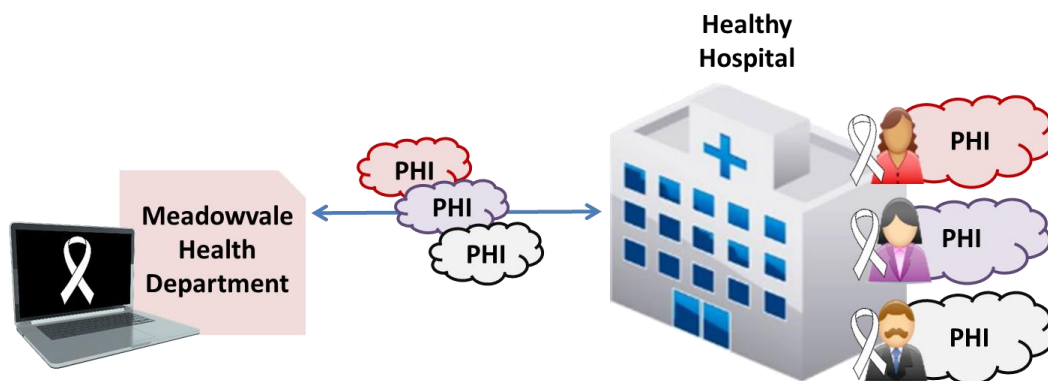


*Figure 1: Reporting of Disease Scenario*

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 2: Exchange for Conduct of Public Health Surveillance

Healthy Hospital is located in the State of Meadowvale. The Meadowvale Health Department maintains the state central cancer registry, and State law authorizes the Department to collect data on cancer occurrence (including the type, extent, and location of the cancer) and the type of initial treatment. Under [45 CFR 164.512\(b\)\(1\)\(i\)](#), Healthy Hospital may use certified health IT to disclose electronic PHI to the Meadowvale Health Department's central cancer registry. In deciding how much and what information to supply to Meadowvale Department of Health, HIPAA permits Healthy Hospital to reasonably rely on the Meadowvale Department of Health's statement of what information is necessary for the public health activities. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

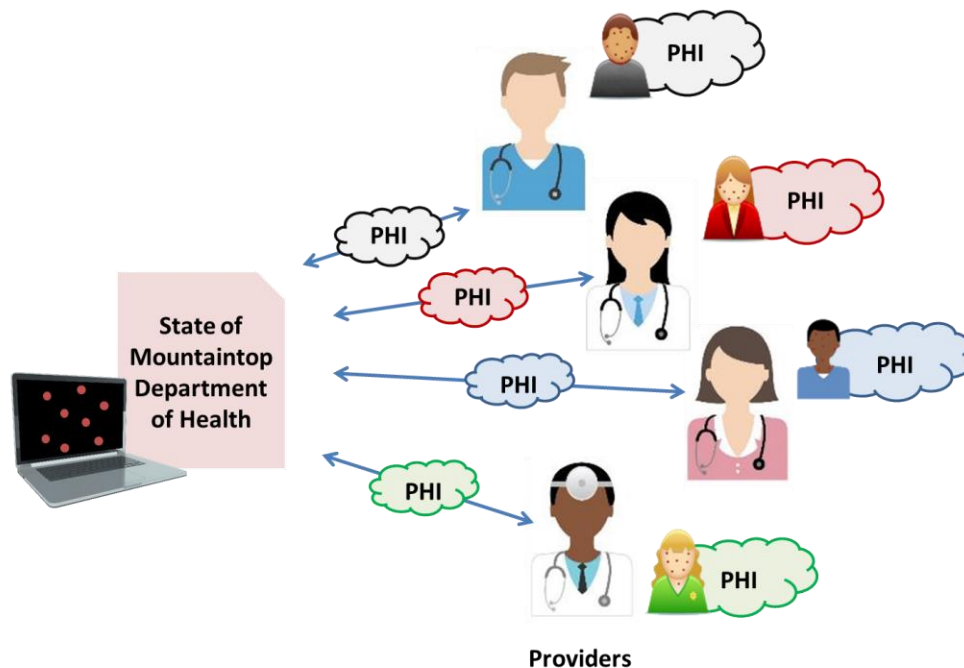


**Figure 2: Public Health Surveillance Scenario**

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 3: Exchange for Public Health Investigations

The State of Mountaintop Department of Health investigates the source of a recent measles outbreak in a local school, and State law authorizes the Department to access medical records to complete the investigations. The Mountaintop Department of Public Health asks all health providers in the state to report confirmed diagnoses of measles, including patient identity, demographic information, and positive test results. Under [45 CFR 164.512\(b\)\(1\)\(i\)](#), providers within the State of Mountaintop may use certified health IT to disclose PHI to the Department of Health. While providers may only disclose the minimum necessary for the purpose of the public health investigation, they may reasonably rely on representations from the Department of Health about what PHI is necessary to conduct the investigation. Disclosure of electronic PHI requires HIPAA Security Rule compliance.



**Figure 3: Public Health Investigations Scenario**

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 4/5: Exchange for Public Health Interventions

When Urban City's water supply is found to be contaminated with lead in State Prarieland, the Prarieland Health Department implements a lead poisoning intervention program and needs lead exposure test results of children who might have been exposed. Because of the known long-term neurological effects of lead poisoning in children, Prarieland's Health Department is authorized by law to obtain the test results of each tested child and to track those children's health and development over time. The Department contracts with a local health information exchange (HIE) to collect, on the Health Department's behalf from local providers, PHI about the tested children. Under [45 CFR 164.512\(b\)\(1\)\(i\)](#), providers may disclose the PHI to the Prarieland Health Department using certified health IT. While providers must only disclose the minimum necessary for the purpose of the public health intervention, they can reasonably rely on representations from the Prarieland Department of Health that the requested PHI is the minimum needed to implement the program. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

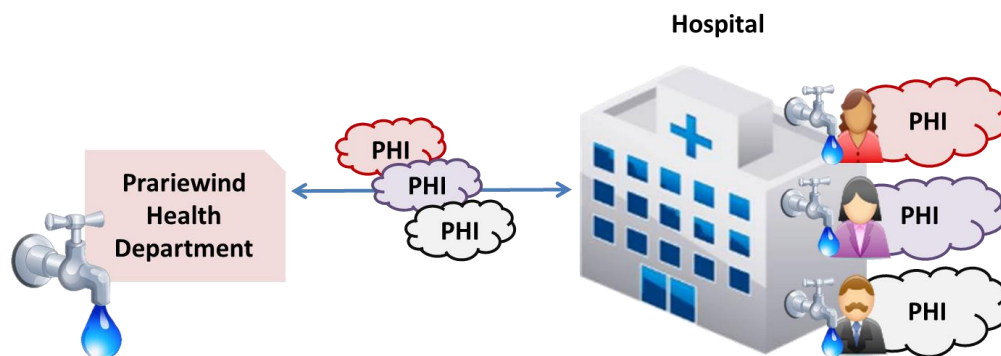
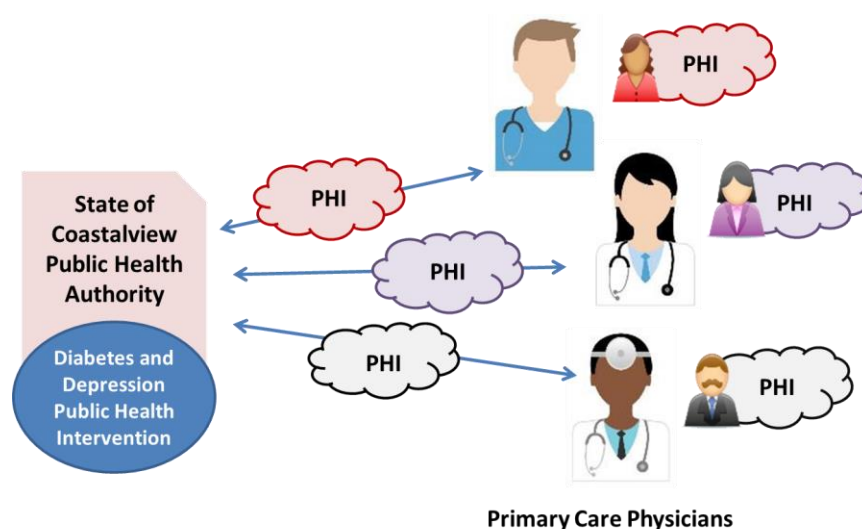


Figure 4: Public Health Interventions Scenario 1

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

For another example, the State of Coastalview Public Health Authority is responsible under state law for implementing a CMS State Innovation Model (SIM) program in their state. Coastalview was awarded a SIM grant to conduct a public health intervention measuring of outcomes for patients that have both diabetes and depression and whose primary care provider (PCP) coordinate their patients' care.

Coastalview requests that PCPs within the state disclose PHI to the state's Public Health Authority to assist in the evaluation of care coordination outcomes. Under [45 CFR 164.512\(b\)\(1\)\(i\)](#), PCPs within Coastalview's jurisdiction may disclose PHI to the Coastalview Public Health Authority using certified health IT. While PCPs must only disclose the minimum necessary for the purpose of the public health intervention, they may reasonably rely on representations from the Public Health Authority that the requested PHI is the minimum needed. Disclosure of electronic PHI requires HIPAA Security Rule compliance.



**Figure 5: Public Health Interventions Scenario 2**

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 6: Exchange Subject to Food and Drug Administration (FDA) Jurisdiction

Medical devices are subject to the jurisdiction of the [U.S. Food and Drug Administration \(FDA\)](#). A device manufacturer announces a Class I Medical Device Recall for HeartWare2.0. Dr. Johnson implanted HeartWare 2.0 in 35 patients prior to the recall. Dr. Johnson employs certified health IT to identify patients with HeartWare 2.0. She may disclose PHI, such as patient contact information and other health information about the affected patients, to the FDA under [45 CFR 164.512\(b\)\(1\)\(iii\)\(c\)](#). Dr. Johnson must disclose only the information she thinks is necessary to support the recall, but she may seek the manufacturer's input, if she wants, in making that decision.

Disclosure of electronic PHI requires HIPAA Security Rule compliance.

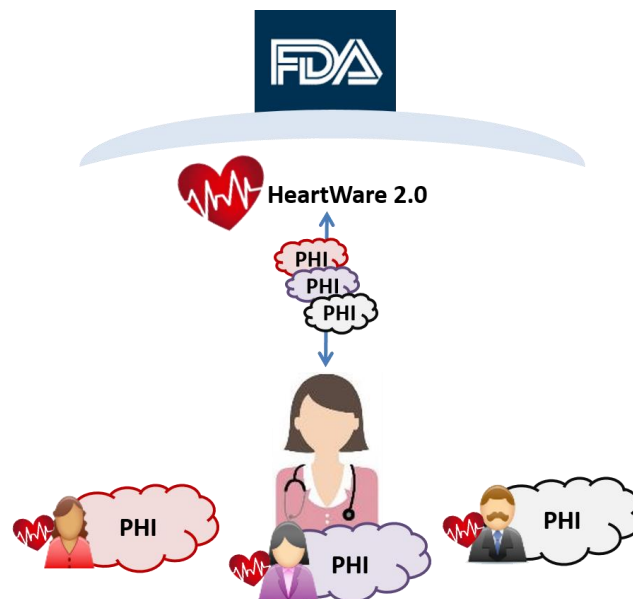


Figure 6: FDA Jurisdiction Scenario

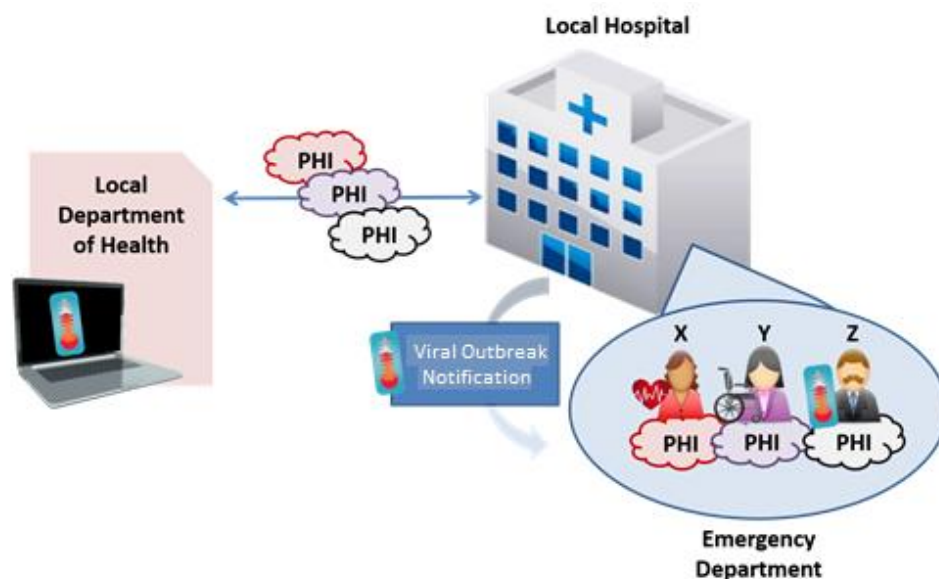
*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 7: Exchange for Persons Exposed to Communicable Disease and for Related Public Health Investigation

Patient Y went to the Emergency Department at Local Hospital due to a severe laceration to the leg. While in the waiting area, Patient Y sits next to Patient Z. It is later confirmed that Patient Z has an airborne, communicable virus. Patient Y and other patients in the waiting area were potentially exposed.

Local law permits providers to notify individuals that may have been exposed to a communicable disease. Local Hospital may use PHI and certified health IT to identify patients who were in the waiting area and potentially exposed to the virus. Local Hospital may send notices to the exposed patients about their exposure based on 45 CFR 164.512(b)(1)(iv). Local Hospital must only use and disclose the minimum necessary PHI for the purpose of the notification of exposure to the communicable disease.

Local Department of Health, in conjunction with Local Hospital, is conducting an investigation into outbreaks of the virus. Local Department of Health is authorized by law to collect disease information and access medical records to conduct investigations and implement disease control measures and asks Local Hospital to provide the PHI of patients exposed to the virus. Local Hospital may use certified health IT to disclose this PHI to the Department of Health based on 45 CFR 164.512(b)(1)(i). While Local Hospital must only disclose the minimum necessary for the purpose of the public health investigation, it may reasonably rely on the Local Department of Health's representations about what is the minimum information needed to conduct the investigation. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

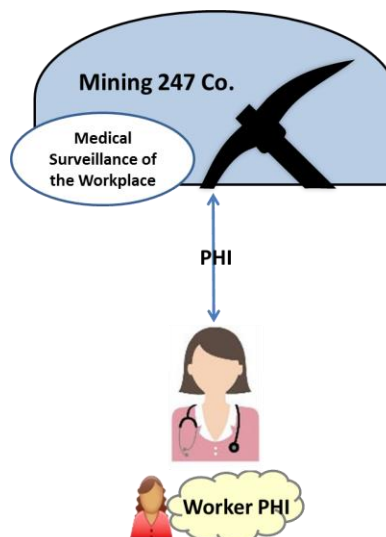


**Figure 7: Exchange for Persons Exposed to Communicable Disease and for Related Public Health Investigations Scenario**

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

## Scenario 8: Exchange in Support of Medical Surveillance of the Workplace

Worker Bee is employed by Mining 247 Company. By federal law, Mining 247 is required to monitor the safety of working conditions, also known as medical surveillance of the workplace. At the request of Mining 247 Company, Dr. Hopeful provides health care evaluation services to Worker Bee so the company can evaluate work-related illness and injuries and conduct medical surveillance. Mining 247 Company needs this information to comply with the Mine Safety and Health Administration (MSHA) and state laws. Under [45 CFR 164.512\(b\)\(1\)\(v\)](#), Dr. Hopeful may disclose Worker Bee's workplace medical surveillance-related PHI to Mining 247 Company. Dr. Hopeful must provide Worker Bee with written notice that the information will be disclosed to his or her employer at the time the health care evaluation is provided (or the notice may be prominently posted at the worksite if that is where the service is provided). Dr. Hopeful must only disclose the minimum necessary PHI that consists of findings concerning the workplace surveillance. Dr. Hopeful discloses the information to Mining 247. As she disclosed the information electronically, the HIPAA Security Rule applies to her disclosure.



**Figure 8: Exchange in Support of Medical Surveillance of the Workplace Scenario**

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

---

## Scenario 9: Using Certified Electronic Health Record Technology

Providers who need to share PHI with agencies or organizations for public health activities may use certified health IT to send the information to the requesting agency or organization. Disclosure of electronic PHI by certified health IT or other electronic means requires HIPAA Security Rule compliance by the provider.

---

### Additional Resources

- [Office for Civil Rights HIPAA Regulations Website](#)
- [ONC Guide to Privacy & Security of Electronic Health Information \(2015\)\[PDF-1.26MB\]](#)

*The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.*

[CT.gov Home](#) [\(/\)](#) [Office of Policy and Management](#) [\(/OPM\)](#) Network Security Policy and Procedures

## Network Security Policy and Procedures

**Version:** 2.2

**Date Issued (revised):** December 9, 2019

**Date Effective:** immediately

**Supersedes:** Version 2.1

**Reason for Change:** Eliminated all references to the Department of Information Technology (DOIT).

### Purpose

The Office of Policy and Management (OPM) has established this policy and reporting requirements, and associated standards to assure that critical information is protected and data flow is not interrupted by unauthorized access.

### Policy Statements

The following policy statements are abstracted from the official State of Connecticut Network Security Policy.

1. All information traveling over state computer networks that has not been specifically identified as the property of other parties will be treated as though it is a state asset. If there is no primary agency designated to administer this information, the Department of Administrative Services, Bureau of Enterprise Systems and Technology (DAS-BEST) will become the steward of this data until another agency is designated. It is the policy of the State to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.
2. In addition, it is the policy of the State to protect information belonging to third parties--that has been entrusted to the State in confidence--in the same manner as private sector trade secrets as well as in accordance with applicable contracts.
3. All computers permanently or intermittently connected to State of Connecticut networks, and all DAS-BEST computers that intermittently or continuously connect to an internal or external network must employ password-based access controls. All users must be positively identified prior to being able to use any multi-user computer or communications system resources.
4. The computer and communications system privileges of all users, systems, and independently operating programs (such as "agents") must be restricted based on the need-to-know.
5. Participation in external networks as a provider of services that external parties rely on is expressly prohibited unless the Agency System Administrator has identified, in writing, the security risk involved and submitted those risks to DAS-BEST and the Chief Information Officer (CIO) has expressly accepted these and other risks associated with the proposal.
6. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to DAS-BEST.
7. Each agency that has existing dial-up lines/modems today must submit a request for consideration of approval to DAS-BEST.
8. Wireless communications, or other broadcast technologies, must not be used for data transmission containing State "confidential" or "restricted" data unless the connection is encrypted and has an acceptable level user authentication.
9. Third party vendors must NOT be given dial-up privileges to State computers and/or networks unless the involved system administrator determines that they have a bone fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).
10. All users wishing to use the State internal networks, or multi-user systems that are connected to the State internal networks, must sign a compliance statement prior to being issued a user-ID.
11. Confidential or restricted data in unencrypted format is prohibited on State mobile computing and storage devices. Please see the State Policy on mobile computing and storage devices for additional guidance and requirements.

### Agency Planning and Reporting Responsibilities

#### Planning

1. Each State agency will develop it's own network security policy. The agency security policy will address:
  - a. System Access Control which includes how to choose passwords, how to set-up passwords and log-in/log-off procedures,
  - b. System Privileges; limiting system access, process for granting system privileges and the process for revoking system privileges and Establishment of Access Paths;
  - c. Computer Network Changes; conditions for participation in external networks, policy for initiating sessions via dial-up lines, establishing wireless communications and discussion of computer viruses, worms, and Trojan horses.
2. Each agency, must determine what agency information is confidential or restricted
3. The agency network security policy will be incorporated in the agency's Information Technology plan and architecture document.

#### Reporting

1. Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to DAS-BEST.
2. Any agency that has its own Internet connection today or will have in the future, must submit the following information to DAS-BEST:
  - a. Name of the Internet Provider and line speed of the circuit
  - b. Model and type of Firewall hardware and software.
  - c. Port numbers that are opened in the Firewall.

## **Compliance**

1. Each agency must submit it's own Network Security Policy to DAS-BEST for review and approval.
2. Each State Agency must have a designated information security liaison. The name, telephone number and email address of the individual or individuals must be sent to DAS-BEST. This information must come from the Commissioner or IT Manager level.

Any modification in existing Network/Systems configurations, that is in contrast to the Statewide Security policy must be submitted for approval to DAS-BEST.

## **Scope**

This policy applies to the following entities: any State of Connecticut agency, institution, office, department, commission, council or instrumentality that utilizes State owned and maintained data networks in the conduct of its business.

## **Definitions**

### **State Agency**

For the purposes of this policy, the term State Agency refers to any State of Connecticut agency, institution, office, department, commission, council or instrumentality.

### **Compliant**

For the purposes of this policy, an agency's network security policy will be considered compliant when it meets the criteria defined in, and/or performs as described in, the State Network Security Policy.



## Policy on Security for Mobile Computing and Storage Devices

**Version:** 1.1

**Date Issued (revised):** December 9, 2019

**Date Effective:** immediately

**Supersedes:** Version 1.0 September 10, 2007

**Reason for Change:** Eliminated all references to the Department of Information Technology (DOIT).

### Purpose

The Office of Policy and Management (OPM) has established this policy on the secure implementation and deployment of mobile computing and storage devices within State government for the protection of State data that may be stored on those devices.

This policy refers to and enhances State of Connecticut Network Security Policy and Procedures. The Policies should be read together to ensure a full understanding of State Policy.

### Scope

This policy covers all State of Connecticut Executive Branch agencies and employees whether permanent or non-permanent, full or part-time, and all consultants or contracted individuals retained by an Executive Branch Agency with access to State data (herein referred to as "users").

This policy does not apply to the Judicial or Legislative Branches of government, or State institutions of higher education. However, these branches and institutions may consider adopting any or all parts of this policy.

This policy covers mobile computing devices and mobile storage devices (herein referred to as "mobile devices").

### Authority

In accordance with Conn.Gen. Stat. §4d-8(a), the Office of Policy and Management is responsible for [developing and implementing policies pertaining to information and telecommunication systems for State Agencies](#).

## Policy Statements

1. No confidential or restricted State data shall reside on any mobile devices except as set forth in paragraph 2. Agencies are required to utilize secure remote data access methods, as approved by the Department of Administrative Services, Bureau of Enterprise Systems and Technology (DAS-BEST), in support of mobile users.
2. In the event utilization of secure remote access methods are not possible, the Agency must adhere to the following restrictions and requirements:
  - a. The Agency Head must authorize and certify in writing, in advance, that the storing of restricted and confidential State data on the mobile device is necessary to conduct Agency business operations;
  - b. The Agency Head or their designee must determine and certify in writing that reasonable alternative means to provide the user with secure access to that State data do not exist;
  - c. The Agency Head or their designee must assess the sensitivity of the data to reside on a secure mobile device and determine that the business need necessitating storage on the mobile device outweigh(s) the associated risk(s) of loss or compromise; and
  - d. The Agency Head or their designee must authorize, in writing, the storage of specific State data on a secure mobile device and the acceptance of all associated risk(s).
3. State data that an Agency Head has authorized to be stored on a secure mobile device shall be:
  - a. the minimum data necessary to perform the business function necessitating storage on the mobile device;
  - b. stored only for the time needed to perform the business function;
  - c. encrypted using methods authorized by DAS-BEST;
  - d. protected from any and all forms of unauthorized access and disclosure; and
  - e. stored only on secure mobile devices in accordance with OPM policies and DAS-BEST standards and guidelines.
4. Any State data placed on a mobile device shall be documented, tracked, and audited by the authorizing Agency. The information tracked shall include the identification of the individual authorizing storage of the data on the mobile device, the authorized user of the

mobile device, the asset tag of the mobile device, information about the stored data, and the final disposition of that data.

5. Agencies will configure mobile devices to allow only the minimum features, functions, and services needed to carry out Agency business requirements.

6. Agencies will ensure that mobile computing devices are configured with approved and properly updated software-based security mechanisms including anti-virus, anti-spyware, firewalls, and intrusion detection. Users shall not bypass or disable these security mechanisms under any circumstances.

7. Users in the possession of State owned mobile devices during transport or use in public places, meeting rooms and other unprotected areas must not leave these devices unattended at any time, and must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft.

8. Agencies shall establish and document reporting, mitigation and remediation procedures for lost or stolen mobile devices containing State data and for State data that is compromised through accidental or non-authorized access or disclosure.

9. In the event that a mobile device containing State data is lost, stolen, or misplaced, and/or the user has determined unauthorized access has occurred, the user must immediately notify his or her Agency of the incident. The affected Agency must immediately notify the DAS-BEST helpdesk of the incident in order to initiate effective and timely response and remediation.

10. Agencies shall develop and implement a formal, documented security awareness and training program sufficient to ensure compliance with this policy.

11. Agencies must obtain a signed, formal acknowledgement from users indicating that they have understood, and agreed to abide by the rules of this policy.

12. Agencies and users shall adhere to this security policy and associated procedures; failure to do so may result in sanctions.

## Definitions

### Confidential or Restricted State Data

Confidential or restricted State data includes but is not limited to;

Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual;

Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

In accordance with the State of Connecticut Network Security Policies and Procedures, each Agency is responsible for the assessment and categorization of their data as Confidential or Restricted in accordance with the definitions set forth in this policy.

### Mobile Computing Devices

The term "mobile computing devices" refers to portable or mobile computing and telecommunications devices that can execute programs. This definition includes, but is not limited to, notebooks, palmtops, PDAs, iPods, BlackBerry devices, and cell phones with internet browsing capability.

### Mobile Storage Devices

The term "mobile storage devices" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

### Secure Mobile Devices

A mobile device that has a sufficient level, as defined by this policy and DAS-BEST standards, of access control, protection from malware and strong encryption capabilities to ensure the protection and privacy of State data that may be stored on the mobile device.

State of CT-Department of Public Health  
 Information Technology  
 Phone: 860-509-7777  
 Email: [Helpdesk.DPH@ct.gov](mailto:Helpdesk.DPH@ct.gov)  
 410 Capitol Avenue, 3<sup>rd</sup> Floor, MS #13DPR  
 Hartford, CT 06134

I, Click here to enter text., pledge that I will not store any “Confidential or Restricted State Data”<sup>1</sup> or “Protected Health Information”<sup>2</sup> on any mobile computing device, including but not limited to portable devices such as laptops, thumb drives, flash drives, PDAs, portable memory devices or any other type of electronic storage or storage media equipment **without proper authorization forms signed by the CT DPH Commissioner or his designee** and that if using a DPH provided and password-protected device, I will delete protected health information (and empty it from the computer’s recycle bin) promptly when it is no longer needed to fulfill my job responsibilities.

I also pledge that I will adhere to the State of Connecticut “Acceptable Use of State Systems Policy” that includes but is not limited to “Connecting personally owned hardware”<sup>3</sup> to the network or computing devices.

I further pledge that **I will not** reveal my passwords, security ids /codes / keys or like information to any other person. I understand that Laws pertaining to confidentiality of patient/client records also apply to information stored electronically and I understand that violation of patient confidentiality is potential grounds for civil suit and substantial fines. Additionally, I understand that violation of this pledge may be grounds for disciplinary action, potentially including termination of employment.

My signature confirms that I have received, agree to, and will adhere to policies as detailed in the “Policy on Security for Mobile Computing and Storage Devices” and the State of Connecticut “Acceptable Use of State Systems Policy”.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

---

<sup>1</sup> **Confidential or restricted State data** includes but is not limited to:

- a) Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual’s identity, violate the individual’s right to privacy or otherwise harm the individual.
- b) Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

<sup>2</sup> **Protected Health Information (PHI) data** includes but is not limited to:

- a) Health information that could reveal the identity of a person.
- b) Under HIPAA, PHI identifiers include Name, Street Address, City, County, Precinct, Zip Code, Dates (except year) that directly relate to a person (including , Social Security number, birth date, admission date, Medical record number, Health plan beneficiary number, discharge date, date of death, and all ages over),
- c) Telephone numbers, Fax numbers, E-mail addresses, Account number, Certificate/license number, Vehicle identifiers and serial numbers, including license plate numbers, Device identifiers and serial numbers, Web Universal Resource Locator (URL), Internet Protocol (IP) address number, Biometric identifiers (for example, finger or voice prints), Full face photographs or similar images, Any unique identifying number, characteristic or code.

<sup>3</sup> **State of Connecticut Acceptable Use of State Systems Policy** includes, but is not limited to, Item 5 of the section titled “Examples of Unacceptable Use of State Systems” which prohibits connecting personally owned hardware.



## **Mobile Device Incident Reporting Guidelines**

As soon as you are aware an incident has occurred you must notify:

**CTDPH IT Security Officer:**                      **Nicholas Piscitelli**                      **860-509-8145**

**CTDPH IT Technical  
Infrastructure Supervisor:**

**Eva Golebiewski**                      **860-509-7430**

**IF YOU ARE UNABLE TO REACH ONE OF THE ABOVE PERSONNEL  
AND REPORT THE INCIDENT TO A LIVE PERSON; CONTACT:**

**CTDPH HELPDESK:**                      **860-509-7777**

*IF THE INCIDENT OCCURS OVER THE WEEKEND AND/OR*  
***YOU ARE UNABLE TO REACH THE CTDPH HELPDESK WITHIN 60 MINUTES,***  
***IT IS IMPERATIVE YOU IMMEDIATELY CALL THE DOIT HELP DESK 860-622-2300 - OPTION 9***  
***TO BEGIN INCIDENT RESPONSE, ASSESSMENT AND REMEDIATION ACTIVITIES.***

Provide the following information when making a report:

- **YOUR NAME.**
  - **PHONE NUMBER WHERE YOU MAY BE REACHED.**
  - **Position within the agency, and the name of your facility.**
  - **DATE AND TIME THE INCIDENT OCCURRED.**
  - **AS DETAILED DESCRIPTION OF THE INCIDENT AS POSSIBLE.**
  - **Names and contacts information of witnesses, if any.**
  - **Attach a copy of the police report from the police station where the loss was reported if Available; otherwise provide the name of the police station, officer's names, and report number.**
  - **A copy of the associated Mobile Data Control Form to include:**
    - Serial number of device(s) lost or affected by the incident
    - Asset tag number of device(s) lost or affected by the incident
    - Description of the device(s) involved
    - Identification and description of potentially compromised data
- Note: If you do not have this form, (the original is kept on record at your facility); provide as much information as possible and the names on this form and that of your facilities IT staff.*

If the device is still in your possession, but you believe data has been stolen from it,  
do not use the device again until it is cleared for use by the response team assigned to the incident.

**DEFINITIONS OF: "CONFIDENTIAL OR RESTRICTED STATE DATA", "MOBILE COMPUTING DEVICES", "MOBILE STORAGE DEVICES", "SECURE MOBILE DEVICES" as defined by the STATE OF CT APPEAR ON THE NEXT PAGE.**

## **DEFINITIONS:**

### **Confidential or Restricted State Data**

includes but is not limited to;

Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual;

Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

In accordance with the State of Connecticut Network Security Policies and Procedures, each Agency is responsible for the assessment and categorization of their data as Confidential or Restricted in accordance with the definitions set forth in this policy.

### **Mobile Computing Devices**

The term "mobile computing devices" refers to portable or mobile computing and telecommunications devices that can execute programs. This definition includes, but is not limited to, notebooks, palmtops, PDAs, iPods®, BlackBerry® devices, and cell phones with internet browsing capability.

### **Mobile Storage Devices**

The term "mobile storage devices" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

### **Secure Mobile Devices**

A mobile device that has a sufficient level, as defined by this policy and DOIT standards, of access control, protection from malware and strong encryption capabilities to ensure the protection and privacy of State data that may be stored on the mobile device.

## **Sample Confidentiality Disclaimer for Fax Cover Pages**

The documents accompanying this fax transmission contain health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

\* Based on "Facsimile Transmission of Health Information"

[http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_031811.hcsp?dDocName=bok1\\_031811](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031811.hcsp?dDocName=bok1_031811)

**Section 308(d) of the Public Health Service Act (42 U.S.C. 242m)**

NCHS Confidentiality Statute--No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under section 304, 306, or 307 may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose and in the case of information obtained in the course of health statistical or epidemiological activities under section 304 or 306, such information may not be published or released in other form if the particular establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented (as determined under regulations of the Secretary) to its publication or release in other form.

## Connecticut Department of Public Health Data Sharing Request Form (Program 1) and (Program 2)

*This form shall be used for data sharing request within the Connecticut Department of Public Health for the purpose of public health practice. Please review DPH Protocol for Data Sharing before completing this form.*

**Date:**

**Person Requesting Data**

Name/Title/Phone:

Program/Section/Branch:

**Program Responsible for Data**

Name/Title/Phone:

Branch /Section/Program:

Section Chief/Phone:

**Purpose of Proposed Data Sharing**

*Please describe the project/study/analysis you wish to pursue through use of the requested data and how it will be used to meet your project goals.*

**Name and Year(s) of Dataset Requested:**

**Subset of Data Requested (e.g. all, disease/diagnosis, age ranges, essential variables):**

*All data sharing will be limited to CT Occurrences unless otherwise approved here.*

Records:

Variables:

**Proposed Time Frame for use of Data (or if ongoing):**

**Names of persons who will have access to requested data:**

**Please check off how the data will be stored and the confidentiality of the data maintained**

☐ CD/Disk (password protected)

☐ Hard drive (work computer)

☒ Network

☐ Encrypted laptop

**Requestor Assurances**

The requestor agrees to the following terms and conditions of this data sharing request (please initial each statement).

1. **(If Applicable)** I am requesting identifiable data or will be linking requested data to identifiable data. \_\_\_\_\_
  - a. I have used the protocol checklist to reasonably assure that my project is public health practice. \_\_\_\_\_

2. The data will not be used for any purpose other than that specified in this request. \_\_\_\_\_
3. The data will not be released in whole or part, to anyone not involved in this data sharing agreement, including others within DPH. \_\_\_\_\_
4. Data, statistics, or information derived from the requested data that can directly or indirectly identify an individual will not be published or released in any form. \_\_\_\_\_
5. The data requestor agrees to establish appropriate safeguards to protect the confidentiality of the data and prevent unauthorized access. \_\_\_\_\_
6. The data requestor understands that disciplinary action may be taken in the event of intentional disclosure of confidential data. \_\_\_\_\_
7. **(Not applicable if ongoing data sharing)** The data requestor agrees to destroy/delete the data upon termination of the project. \_\_\_\_\_

---

**I have read and understand the DPH Protocol for Data Sharing. I have also reviewed this request form and affirm that the statements here are true and correct.**

Person Requesting Data

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Section Chief: \_\_\_\_\_ Date: \_\_\_\_\_

---

**I have read and understand the DPH Protocol for Data Sharing and agree that the purposed project/study is public health practice and not research. I have also reviewed this request form and agree to provide the data requested for the specified time period.**

Program Responsible for Data

Section Chief: \_\_\_\_\_


Date: \_\_\_\_\_



# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

Appendix 20

|                              |   |                       |            |
|------------------------------|---|-----------------------|------------|
| <b>Policy Name:</b>          | Process for Employees, Supervisors and/or Managers when an Employee Separates from DPH Employment | <b>Number:</b>        | ADM-04-000 |
| <b>Procedure:</b>            | See Page 1  |                       |            |
| <b>Applies to:</b>           | All Connecticut Department of Public Health (DPH) Employees                                       |                       |            |
| <b>Position Responsible:</b> | Chief, Administration Branch  |                       |            |
| <b>Effective Date:</b>       | 6/19/2015   | <b>Last Reviewed:</b> | 11/16/2015 |
| <b>Attachments:</b>          | Procedure for Employee Separation<br>Employee Separation Form<br>DPH Move/Add Change (MAC) Form   |                       |            |
| <b>Approved:</b>             | <br>11/18/2015  |                       |            |

### PURPOSE:

The purpose of this policy and procedure at the Department of Public Health (DPH) is to ensure that State property issued to DPH employees is returned to the State and accounted for whenever a DPH employee separates from employment.

### SCOPE:

This policy and procedure applies to all employees at the Connecticut DPH.

### DEFINITIONS:

State property are state owned items that are distributed and assigned to an employee to be used exclusively for work related business, e.g., laptop, cell phone, desktop, etc.

### POLICY:

The Process for Employees, Supervisors and/or Managers when an Employee Separates from DPH Employment policy ensures that State property issued to DPH employees is returned to the State and accounted for in the asset management inventory whenever a DPH employee separates from State employment.

### PROCEDURES:

See attached Procedure for Employee Separation document.



# STATE OF CONNECTICUT

DEPARTMENT OF PUBLIC HEALTH

**PROCESS:**

N/A



# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

### PROCEDURE FOR EMPLOYEE SEPARATION

| Employee   | Human Resources   | Manager/ Supervisor   | Fiscal/ Asset Manager  | IT   |
|--|---|---|--|--|
| <b>Day 1: Date employee gives notice of separation</b>   |   |   |  |  |
| 1. Submits a written signed notice of separation to his or her supervisor and provides a copy to the Human Resources Office preferably one month (minimum two weeks) before the separation date. The notice should contain information regarding the nature of the separation; i.e. separation date, transfer to another state agency, leaving state service, etc. |   |   |  |  |
| <b>Day 2-10: After separation notice is sent by employee</b>   |   |   |  |  |
|  | 1. Upon receipt of employee's notice, sends an e-mail to Information Technology, the Fiscal Office (both Budget and Core-CT Security), Payroll, Affirmative Action and the Agency Ethics Liaison notifying them that the employee is separating from DPH. |   |  | 1. Upon receipt of the employee's notice, sends a Separation Form to employee's supervisor to complete with employee (attached). |
|  | 2. Schedules an exit interview with employee (usually on their last date of service.)   |   |  |  |
| <b>Days 11-20: After separation notice is sent from employee</b>   |   |   |  |  |
|  |   | 1. Meets with employee to discuss date of separation, document retention, storage of documents, files, drives, folders and state property issued to the | 1. Determines what DPH assets have been assigned to the departing employee. (e.g., laptop, cell phone, desktop, etc.) and works with IT to coordinate/ | 1. Collaborates with Fiscal's asset manager on hardware and software items issued to employee.                                   |



# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

|  |  |  |   |   |
|--|--|--|---|---|
|  |  | employee and completes the Employee Separation Form and sends form to the IT HelpDesk (HelpDesk.dph@ct.gov).<br><u>\\exec\dfs\DPH-Shared1\Admin\Admin Branch\IT-EmployeeSeparationForm 3-10-15.doc</u> | validate asset management and inventory items for departing employee. |   |
|  |  |  |   | 2. Performs a quick site visit to employee's workstation to confirm state assets (e.g., computer, printers, phone, laptop). |

### Last Day of Employee's Employment at DPH

|  |   |  |  |   |
|--|---|--|--|---|
| 1. Arranges for out of office message on e-mails.                                      | 1. Conducts exit interview with the employee and collects their state issued photo ID, building access card and parking hang tag.   | 1. Submits DPH Move/ Add/ Change (MAC) form to Administrative Branch's assistant to deactivate the departing employee's phone line (attached)<br><u>\\exec\dfs\DPH-Shared1\Admin\Admin Branch\DPH MAC Form.doc</u> | 1. Disables employee's Core-CT access. | 1. Disables employee's computer network access. |
| 2. Updates phone message per supervisor's instructions and changes passcode to "1234". | 2. Contacts RM Bradley, the building management company, to deactivate the employee's building access card.   |  |  |   |
| 3. Participates in the exit interview scheduled with Human Resources.                  | 3. Turns in the employee's photo ID badge and building access card to RM Bradley.   |  |  |   |
| 4. Turns in building access card, parking hang tag, and ID badge to Human Resources.   | 4. On employee's last day, send an e-mail to Information Technology staff, Fiscal Office staff, Affirmative Action staff, Payroll staff, DPH Communications Office, the DPH staff member that |  |  |   |



# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

|  |   |  |  |  |
|--|---|--|--|--|
|  | coordinates cell phone assignments, Security and Building Management Company confirming that the employee no longer works at DPH. |  |  |  |
|--|---|--|--|--|

### One Week Following Separation

|          |  |                     |  |   |
|----------|--|---------------------|--|---|
|          | 1. Records and tracks all returned building access cards and ID badges for audit purposes. |                     | 1. Records and tracks all returned state cell phones for audit purposes. Tracks state asset/equipment returns on Core Asset Management System. | 1. IT staff collects IT State asset/equipment from the supervisor as appropriate. The Program must notify IT if another employee will use the equipment. IT verifies the equipment and will not remove the equipment if assigned to a new employee. |
| Employee | Human Resources  | Manager/ Supervisor | Fiscal/ Asset Manager  | IT  |
|          |  |                     |  | 2. Removes software from employee's assigned computer.  |
|          |  |                     |  | 3. Copies and archives data from employee's assigned computer.  |
|          |  |                     |  | 4. Records and tracks all returned software.  |

**CT Department of Public Health  
Administration/Information Technology**

**Employee Separation Form**

**Directions:** The Employee Separation Form is to be completed by the supervisor and sent to the IT Help Desk (HelpDesk.dph@ct.gov)

**Employee's Information** (leaving the Agency)

Name: \_\_\_\_\_ Separation Date: \_\_\_\_\_

Network access will be disabled on close of business.

Branch/Section: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Floor/Cubicle #: \_\_\_\_\_

**Supervisor/Manager's Information**

Supervisor/Manager's Name: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Floor/Cubicle #: \_\_\_\_\_

**Network Access** (P, S, U & W drives are provided to all users unless otherwise specified.)

(P: Employee's Use, S: Program's Shared Drive, U: Agency Shared Drive and W: Shared Across Programs)

Employee's P drive data will be copied to supervisor's P: drive. Please specify any other data that needs to be copied. \_\_\_\_\_

**E-Mail**

Mailbox will be disabled immediately unless otherwise specified.

Do you want to keep the separating employee's mailbox active after his/her separation date?

☐ No ☐ Yes - If yes, please complete the *Extension of Separating Employee's E-Mail Account* form.

**Equipment** (Computer, laptop, etc.)

Computers will be picked up by IT and reformatted two weeks after employee's separation date (c: drive erased).

Equipment Type: \_\_\_\_\_ Barcode #: \_\_\_\_\_

Equipment Type: \_\_\_\_\_ Barcode #: \_\_\_\_\_

Equipment Type: \_\_\_\_\_ Barcode #: \_\_\_\_\_

**Software** (MS Office 2010, Windows7 Operating System and Adobe Acrobat Reader are installed on all computers.)

Other than the default software, was other software installed on the computer?

☐ No ☐ Yes - If yes, please specify: \_\_\_\_\_

Do you want the specified software installed onto another user's computer in your program?

☐ No ☐ Yes - If yes, please provide employee's name and the computer barcode number the software is going to be installed.

Employee's Name: \_\_\_\_\_ Barcode #: \_\_\_\_\_

**Special Request(s)**

**PLEASE NOTE:** If provided, supervisors should collect VPN key fob from employee and return it to IT.

Supervisor/Manager's Signature \_\_\_\_\_

Date \_\_\_\_\_

*If you have any questions, please contact the Help Desk at (860) 509-7777 or e-mail to Helpdesk.dph@ct.gov.*

**DEPARTMENT OF PUBLIC HEALTH  
410-450 CAPITOL AVENUE COMPLEX  
TELEPHONE SYSTEM  
Move, Add, Change (MAC) /Trouble Report**

Agency Req. # \_\_\_\_\_ Date: \_\_\_\_\_  
Employee Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Prepared By and Ext: \_\_\_\_\_ Request Effective Date: \_\_\_\_\_

Procedures: ☐ **MOVE** Complete both columns  
☐ **ADD** Complete **NEW/CHANGE** columns  
☐ **CHANGE** Complete both columns  
☐ **TROUBLE** Describe below

**Present Service**

Division: \_\_\_\_\_  
Section: \_\_\_\_\_  
Building/Floor: \_\_\_\_\_  
Workstation #: \_\_\_\_\_  
Telephone #: \_\_\_\_\_  
Floor Jack #: \_\_\_\_\_

**New/Changed Service**

Division: \_\_\_\_\_  
Section: \_\_\_\_\_  
Building/Floor: \_\_\_\_\_  
Workstation #: \_\_\_\_\_  
Telephone #: \_\_\_\_\_  
Floor Jack #: \_\_\_\_\_

**PRESENT SERVICE**

Funding Code:

**53855**

**DPH Non Project**

| Fund                       | Dept | SID | Program | Account | Project | Bgt. Ref. |
|----------------------------|------|-----|---------|---------|---------|-----------|
| <b>NEW/CHANGED SERVICE</b> |      |     |         |         |         |           |

Funding Codes:

**53855**

**DPH Non Project**

| Fund | Dept | SID | Program | Account | Project | Bgt. Ref. |
|------|------|-----|---------|---------|---------|-----------|
|------|------|-----|---------|---------|---------|-----------|

Description of problem or modification requested: \_\_\_\_\_

Supervisor's Signature: \_\_\_\_\_ Title: \_\_\_\_\_

**This agency request is absolutely essential to the operation of the state agency in line with the Governor's order.**

Chief Financial Officer's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

If your request is to change buttons or features on a telephone please Use Exhibit 22C

**ALL REQUESTS SHOULD BE SENT TO:**

**Maureen Sullivan  
DPH 3<sup>rd</sup> FLOOR; MS#13ADM  
509-7215**

Do not write below this line

| Date Received  | Assigned To: | Date Closed:   | Elapsed Time | Work Order # |
|----------------|--------------|----------------|--------------|--------------|
| ____/____/____ | _____        | ____/____/____ | _____        | _____        |



## Confidentiality Agreement - 2023

### for DPH and CDC Data Security and Confidentiality Compliance

Please read through the statements below and select the check boxes for statements that you agree to and complete the fields below.

**IMPORTANT:** This Confidentiality Agreement is not a Data Sharing Agreement therefore signing this document does not enable access other DPH data systems, data sets, secure drives or files.

I have read and had an opportunity to ask questions about Connecticut Regulation 19a-25 and the current version of the Connecticut Department of Public Health (DPH) Data Security and Confidentiality Policy and Procedures for TB, HIV, STD, and Viral Hepatitis Programs. I understand and will comply with the requirements. I understand that failure to adhere to these requirements could result in administrative or legal action.

#### ***I AGREE TO:***

- |  |   |
|--|---|
| <input type="checkbox"/> Protect personally identifiable information (PII/PHI) by not sharing this information with others except as necessary to conduct DPH-authorized work (including any information maintained by DPH that can be used to distinguish an individual such as name, mother's maiden name, street address, date/place of birth, social security number, medical record number; and, other information that is linkable to an individual, such as medical, educational, financial, and employment information). | <input type="checkbox"/> Use PII/PHI only at DPH or my approved remote work location.   |
| <input type="checkbox"/> Protect encryption keys, passwords, and other security access codes from release to unauthorized persons and protect computers, servers, laptops, mobile devices, and storage media for which I am responsible from unauthorized access, loss, or theft.  | <input type="checkbox"/> <a href="#">Report breaches</a> or suspected breaches of the data, confidentiality and/or protocol or loss of PII/PHI. |
| <input type="checkbox"/> Prevent unauthorized individuals from gaining access to PII/PHI.  |   |



# STATE OF CONNECTICUT

## DEPARTMENT OF PUBLIC HEALTH

|                              |   |                       |                 |
|------------------------------|---|-----------------------|-----------------|
| <b>Policy Name:</b>          | Department of Public Health Policy and Procedures for the Protection of Confidential Data   | <b>Number:</b>        | LO-01-000       |
| <b>Procedure:</b>            | General procedures included in this document.<br>Refer to appropriate DPH Program for specific procedures.  |                       |                 |
| <b>Applies to:</b>           | This policy covers all of the Department's employees, permanent and non-permanent, full-time and part-time, and all consultants and contracted individuals having access to state data, during and after state service. |                       |                 |
| <b>Position Responsible:</b> | General Counsel   |                       |                 |
| <b>Effective Date:</b>       | March 1, 2016   | <b>Last Reviewed:</b> | March 1, 2016   |
| <b>Approved</b>              | <i>R. Agdey</i>   | <b>Date</b>           | <i>02/18/16</i> |

### PURPOSE:

This statement of policy is intended to carry out the Department's responsibilities under federal law, the Connecticut General Statutes (the "Statutes" or "C.G.S", and applicable Regulations of Connecticut State Agencies (the "Regulations") in protecting the confidential data collected and housed at the Department.

### SCOPE:

This policy covers all of the Department's employees, permanent and non-permanent, full-time and part-time, and all consultants and contracted individuals having access to state data, during and after state service.

### DEFINITIONS:

- A. "Personal data". In accordance with § 4-190(9) of the Statutes, personal data is "any information about a person's education, finances, medical or emotional condition or history, employment or business history, family or personal relationships, reputation or character which because of name, identifying number, mark or description can be readily associated with a particular person." Personal data shall not be construed to make available to a person any record described in subdivision (3) of subsection (b) of section 1-210.
- B. "Aggregate health data" means health data that is obtained by combining like data in a manner that precludes the identification of the individual or organization supplying the data or described in the data." § 19a-25-1(1) of the Regulations.

- C. "Disclosure' or 'disclose' means the communication of health data to any individual or organization outside the [D]epartment." § 19a-25-1(5) of the Regulations. Or communication to any individual within the Department who does not have specific authority to access the health data.
- D. "Health data" means information, recorded in any form or medium, that relates to the health status of individuals, the determinants of health and health hazards, the availability of health resources and services, or the use and cost of such resources and services. § 19a-25-1(6) of the Regulations.
- E. "Identifiable health data" or 'identifiable health information" means any item, collection, or grouping of health data that makes the individual or organization supplying it, or described in it, identifiable." § 19a-25-1(7) of the Regulations.
- F. "Protected Health Information [PHI]" means individually identifiable health information. 45 CFR § 160.103.
- G. "Research" is defined as a systematic investigation, which includes "research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." 45 CFR 46.102(d).
- H. "Surveillance" Section 19a-36-A1(gg) defines surveillance as "the continuing scrutiny of all aspects of occurrence and spread of a disease relating to effective control of that disease, which may include but not be limited to the collection and evaluation of: morbidity and mortality reports; laboratory reports of significant findings; special reports of field investigations of epidemics and individual cases; data concerning the availability, use, and untoward side effects of the substances used in disease control, such as rabies vaccine; and information regarding immunity levels in segments of the population."

## **POLICY:**

In accordance with appropriate Statutes and Regulations, employees, former employees, and contractors of the Department of Public Health ("Department" or "DPH") will maintain the security and confidentiality of all identifiable health data. Every employee must undergo ethics and confidentiality training at the start of their employment with the Department, and sign a confidentiality pledge.

This policy applies to:

- Release of data to the public
- Sharing of data within DPH programs
- Sharing of data for research

Appropriate statutes and regulations must be followed regarding release of data and specific information is provided in the Appendices. The duties of the Department and general legal authority are outlined in Appendix A. Information on the Requirements under Health Insurance Portability and Accountability Act of 1996 (HIPAA) is presented in Appendix B, information on Connecticut General Statutes for specific Department programs are located in Appendix C, and the Department Information Security Policy in Appendix D.

## PROCEDURES:

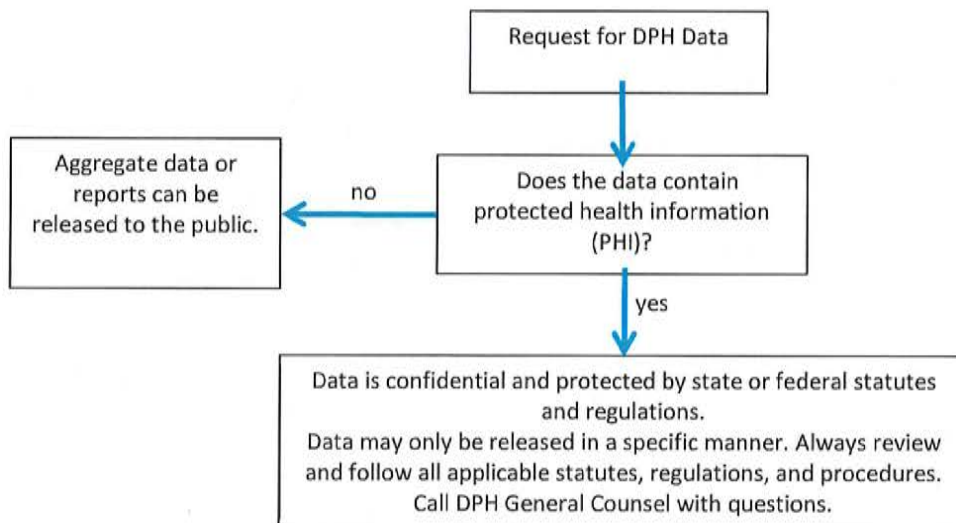
### A. Procedure for releasing data to the public

*The Department frequently receives requests for data housed at its different programs. The first question to be considered is whether the subject of the data request contains personal identifiable health information. If the answer is no, as in the case of aggregate data, reports, etc., then the data can be released to the requester.*

Conversely, if one determines that the data requested contains personal health information protected by state and/or federal statutes or regulations, the data can only be released in compliance with the applicable statutes and regulations, or not be disclosed at all. The employee handling the data request must always read the current applicable statutes and regulations.

Also, the employee handling the data request may consult with the Department's General Counsel, a staff attorney in the General Counsel's Office, and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Officer when they have questions. Covered entities must comply with HIPAA. 45 CFR §164.102. The Department's Laboratory, which performs testing on human subjects and is a "covered entity," and must comply with HIPAA. The remainder of the Department is a health oversight agency. More information on HIPAA is found in Appendix B.

Please use the diagram below as an aid in making a decision about releasing data:



## **B. Procedure for sharing data within DPH for public health practice or surveillance**

The Department developed an agency-wide procedure and form for data sharing within the Department. This form for data sharing is appropriate only when two or more programs have the statutory and regulatory authority to obtain the same data and when carrying out their legally authorized programmatic duties. This form is intended for data sharing among programs within the Department when the purpose of the request is **public health practice and/or surveillance**. The form is located on the U drive at the following address: U:/SHARED/DOC/DATASHARING.

The staff member making the request for data will determine if the request for data is for public health practice or for research. Requests for research must go to the Department's Human Investigation Committee (HIC). The Chair or Co-Chair of the HIC may be consulted to make this determination between public health practice and research.

1. Complete the Data Sharing Request Form and submit to the program holding the data that are being requested.
2. Section Chiefs of the programmatic areas requesting and holding the data in question review and sign the completed form agreeing to the sharing of data.

## **C. Procedure for sharing data for research**

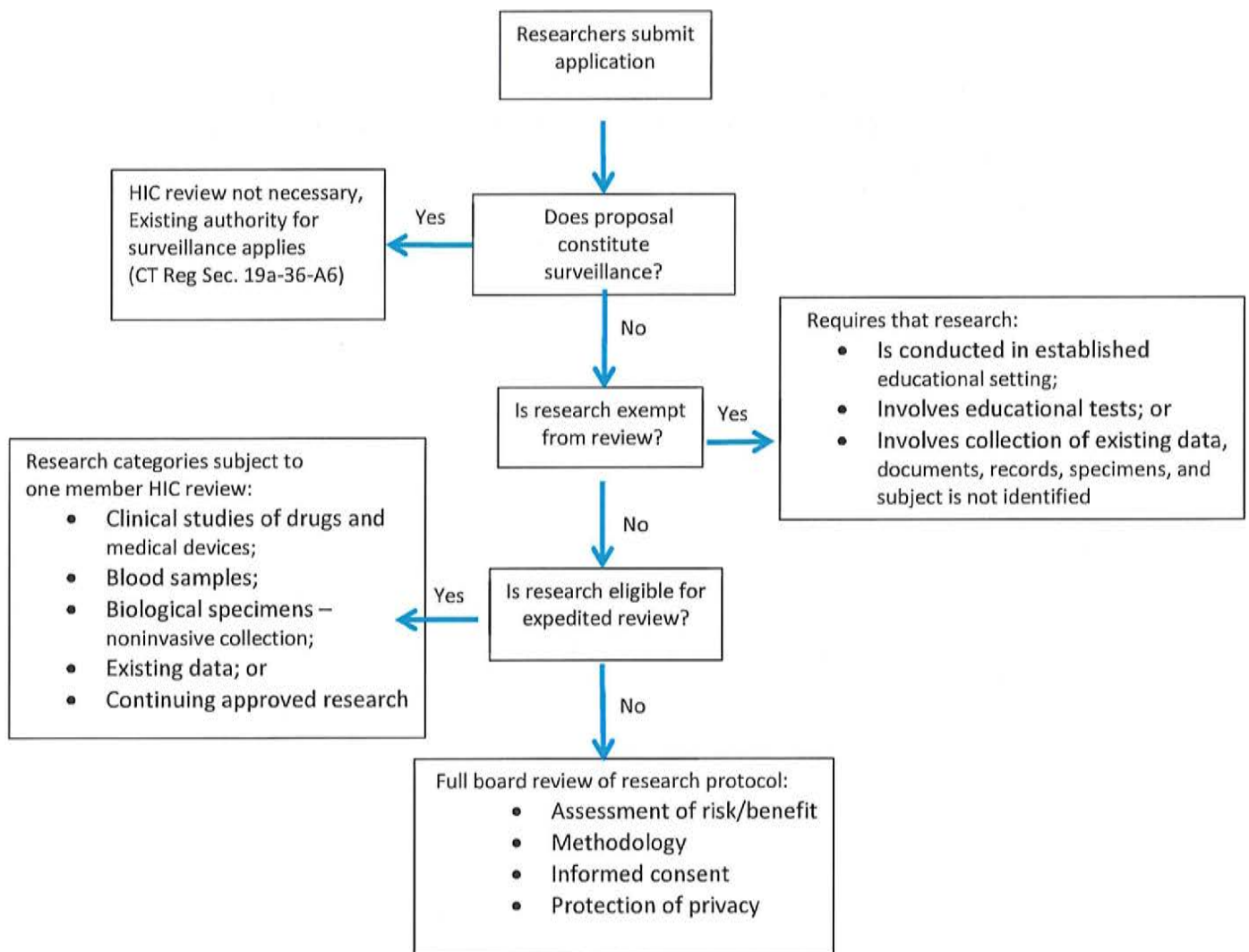
In accordance with § 19a-25 of the General Statutes, the Department may release protected health information to researchers. In order to do so, a request must be made to the HIC. The HIC reviews research proposals to determine whether the proposals comply with applicable federal and state law. Department programs are only authorized to release the requested data to the researchers after the HIC has reviewed and approved the proposal.

Proposals are reviewed according to the following procedures:

1. The HIC Chair or Co-Chair conducts a preliminary review to determine if the activity is public health surveillance or public health practice. If the activity is surveillance or public health practice then no HIC review is necessary.
2. The request for data may be exempt from HIC review if it meets one of several criteria including if it involves the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified directly or through identifiers linked to the subjects. The HIC Chair or Co-Chair

will make the determination of whether or not the request for data is exempt from HIC review.

3. Research that poses minimal risk and includes only research activities in a list approved by the HHS Secretary may eligible to be reviewed in an "expedited" manner (e.g., with one reviewer, instead of review by a convened HIC meeting).
4. If the application is found to be complete, the HIC members review the protocol and evaluate the risks versus benefits of the research. The review also considers additional factors including how the data will be protected and kept secure, the scientific merit of the proposal, analytic plan, and the qualifications of the researchers. More information on the review process can be found within the HIC application located at <http://www.ct.gov/dph/HIC>.



## Appendices

### Contents

|            |  |    |
|------------|--|----|
| Appendix A | The Department's Duties and Legal Authority .....  | 7  |
| Appendix B | Information on the Requirements under Health Insurance Portability and Accountability Act of 1996 (HIPAA)..... | 11 |
| Appendix C | Department Program Specific Information .....  | 13 |
| 1.         | Abortion Data.....   | 13 |
| 2.         | Adoption Records .....   | 13 |
| 3.         | Affirmative Action.....  | 15 |
| 4.         | AIDS .....   | 17 |
| 5.         | Birth Defects .....  | 19 |
| 6.         | Breast Cancer .....  | 21 |
| 7.         | Children and Youth with Special Health Care Needs.....   | 23 |
| 8.         | Drinking Water .....   | 23 |
| 9.         | Emergency Medical Services.....  | 24 |
| 10.        | Environmental Health Data.....   | 24 |
| 11.        | Facility Licensing and Investigation .....   | 29 |
| 12.        | Healthy Start.....   | 31 |
| 13.        | Hearing Office.....  | 31 |
| 14.        | HIC .....  | 32 |
| 15.        | Human Resources: Medical Records of Employees .....  | 33 |
| 16.        | Infectious Disease .....   | 34 |
| 17.        | Immunization .....   | 37 |
| 18.        | Laboratory .....   | 40 |
| 19.        | Newborn Screening .....  | 41 |
| 20.        | Local Health .....   | 42 |
| 21.        | Maternal and Child Health Protection Program .....   | 42 |
| 22.        | Newborn Hearing .....  | 42 |
| 23.        | Office of Health Care Access (OHCA).....   | 43 |
| 24.        | Practitioners License & Investigation .....  | 45 |
| 25.        | Planning.....  | 47 |
| 26.        | Traumatic brain injury patient registry.....   | 47 |
| 27.        | Tumor Registry .....   | 49 |
| 28.        | Vital Records: Birth, death, fetal death, and marriage records .....   | 50 |
| 29.        | WIC .....  | 57 |
| Appendix D | Information Security Policy .....  | 59 |

## Appendix A      The Department's Duties and Legal Authority

A. The Department has several duties in maintaining the confidentiality of identifiable health data pursuant to § 4-193 of the Statutes:

- Collect accurate data
- Release data when requested and such release is legally permissible (see Appendix C for specific provisions that apply to each program)
- Create procedures for accessing and releasing data
- Securely protect data
- Destroy data when no longer necessary

B. The Department has implemented regulations pursuant to § 4-190 et seq. of the Statutes (Personal Data Act), which are found in § 19a-2a-1 et seq. of the Regulations.

C. The Department also has a duty to comply with the Freedom of Information Act ("FOIA") found in § 1-210 et seq. of the Statutes.

**FOIA's general rule** is that records maintained by state agencies are public information unless one of the exceptions found in § 1-210(b) applies. Note that there are many exceptions to the general rule that apply to data maintained by the Department beyond FOIA as indicated more specifically below.

D. Certain areas of the Department such as the Laboratory have an additional duty to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as will be discussed in more detail below.

E. Section 1-84a of the Statutes prohibits the disclosure of confidential information for financial gain obtained in the course of official duties after leaving state employment.

Connecticut General Statutes applicable to all or many of the Department's programs

F. Authority to collect health information:

**Section 19a-2a(10) of the Statutes (powers and duties regarding data collection)** creates a client identifier system that complies with §17a-688 of the Statutes, stating in subsection (e) that "the commissioner may use or make available to authorized persons information from patients' records for purposes of research, management audits or program evaluations, provided such information shall not be utilized in a manner that discloses a patient's name or other identifying information."

**Section 52-146o(b) of the Statutes** authorizes physicians to release medical records to the Department in connection with an investigation of a complaint, if such records are connected to the complaint.

**Section 19a-2a-23 of the Regulations** authorizes the collection of personal data that is relevant and minimally necessary to accomplish the lawful purposes of the Department, and lists the requirements and procedures the department needs to follow in collecting such data, including protecting the data from disclosure. The data, as listed in §§ 19a-2a-2 through 19a-2a-22, includes: Business Office System, Children With Special Health Care Needs System, Division of Chronic Disease and Injury Prevention System, Community Nursing and Day Care Division Data System, Environmental Health Data System, Office of Emergency Medical Services Data System, Vital Records Data System, Long Term Care Data System, Connecticut Tumor Registry Data System, Healthy Start Data System, Infectious Disease Epidemiology Data System, Bureau of Laboratory Services Data System, Local Health Administration System, Newborn Screening System, Personnel Data System, Contract Administration Data System, Supplemental Food Program for Women Infant and Children System, Division of Medical Quality Assurance, Professional Licensure Applications System, Payroll Records Data System, Employee Assistance Program Data System, and AIDS/HIV Data System. See Appendix C for a more detailed listing of the regulations that specifically apply to each program.

G. Confidentiality & disclosure:

**Section 1-84a of the Statutes** prohibits the disclosure of confidential information obtained in the course of official duties after leaving state employment.

**Section 1-210(b) of Statutes** contains provisions that exempt certain records from mandatory disclosure under FOIA. Among the exemptions pertinent to the Department are:

- “Personnel or medical files and similar files the disclosures of which would constitute an invasion of personal privacy;”
  - “Records pertaining to strategy and negotiations with respect to pending claims or pending litigation to which the public agency is a party;”
  - Communications governed by the attorney/client privilege;
  - Test questions, scoring keys and other examinations data used to administer licensure or employment examinations;
  - “Statements of personal worth or personal financial data required by a licensing agency;”
  - Adoption records;
  - Records of complaint brought to Local Health (“LH”) authorities and information compiled in the investigation of such complaints, for the earlier of thirty days or until the conclusion of the investigation;
  - Records not otherwise available to the public for which disclosure would compromise the security or integrity of an information technology system
  - Records, the disclosure of which may result in a safety risk in a correctional facility;
  - Trade secrets; and
- “Vulnerability assessment and risks management plans, operational plans, portions of water supply plans submitted pursuant to § 25-32d of the Statutes that contain or reveal information

the disclosure of which may result in a security risk to a water company, inspection reports, technical specifications and other materials that depict or specifically describe critical water company operating facilities, collection and distribution systems or sources of supply.”

**Section 4-193** of the Statutes requires that state agencies: (a) inform employees who handle personal data about the agency’s personal data regulations, FOIA, and state and federal requirements regarding confidentiality of personal data; (b) inform employees about laws concerning disclosure of personal data kept by the agency; (c) keep record of who has access to data; (d) make data available to a person upon written request; (e) keep only necessary data; (f) if requested in writing, inform an individual whether the Department maintains personal data concerning him, (g) except when exceptions apply; and (h) create a procedure for requesting data.

**Section 19a-25** of the Statutes requires that all morbidity and mortality studies, and personal health information procured by the Department pursuant to § 19a-215 of the Statutes be confidential and be used solely for the purposes of medical scientific research, and for disease prevention and control. Note that disease prevention and control only applies to data collected pursuant to §19a-215 of the Statutes.

Case Law: *Babcock v. Bridgeport Hospital*, 251 Conn. 790, 828–29, 742 A.2d 322 (1999); *Commissioner, Dept. of Public Health v. Freedom of Information Commission*, Superior Court, Judicial District of New Britain, Docket No. CV–05–4007787–S (August 31, 2006, Keller, J.) (42 Conn. L. Rptr. 271, 276–77), held that § 19a-25 of the Statutes attaches only when the study itself is undertaken for the distinct purpose of reducing morbidity or mortality.

NOTE that § 19a-25 of the General Statutes also applies when specifically referenced by another statutory provision.

Personal health information is not subject to subpoena or similar compulsory process in any civil or criminal, judicial, administrative, or legislative proceedings. § 19a-25-2(a) of the Regulations.

Pursuant to **§19a-45a (Memorandum of Understanding between the Commissioners of Public Health and Social Services for improving public health services)**, The Department shall enter into a contract with the Department of Social Services (“DSS”) to improve public health service delivery and public health outcomes for low income population by sharing available HUSKY Health program, and Title V data if the data: (1) is directly related to the administration of the Medicaid or any other DPH or DSS plan; (2) complies with federal and state privacy, confidentiality, and security laws; (3) includes detailed description of the intended public health service/outcomes goals achieved; and, (4) can be afforded by both agencies.

### **Emergency Preparedness**

**Conn. Gen. Stat. Secs. 19a-131a-1-a-131g, 19a-131j.** Quarantine orders issued pursuant to these statutes contain personal health information that are confidential.

**Section 52-146r(b) of Statutes (Disclosure of confidential communication between government attorney and public official or employee of public agency prohibited).** “In any civil or criminal, legislative or administrative proceeding, all confidential communications shall be privileged and a government attorney shall not disclose any such communications unless an authorized representative of the public agency consents to waive the privilege and allows such disclosure.”

**45 CFR 164.514** sets a standard for de-identified information. To be de-identified, data must have the following information removed: name; all geographic subdivision smaller than a state; telephone numbers, fax numbers, e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identification and serial numbers; license plate numbers; device identifiers and serial numbers; URLs; internet protocol address numbers; biometric identifiers, including finger and voice prints; full face photograph images and any comparable images; any other unique identifying number, characteristic, or code; all elements of date (except year) including date of birth, admission date, discharge date, date of death, and all ages over 89; and all elements of date (including year) indicative of such age, except that such ages and element may be aggregated into a single category for age 90 or older.

## Appendix B Information on the Requirements under Health Insurance Portability and Accountability Act of 1996 (HIPAA)

### Basic principles of HIPAA.

- A. In accordance with 45 C.F.R. § 164.103, the Department is a “hybrid entity.” A hybrid entity is a “single legal entity” that is a covered entity under HIPAA, and “whose business activities include both covered and non-covered activities.”
- B. Covered entities are providers who engage in certain electronic transactions (e.g. laboratories, doctors, insurance companies, clearinghouses, billing entities, etc.) 45 CFR § 160.103.
- C. Covered entities must comply with HIPAA. 45 CFR § 164.102. The Department’s Laboratory, which performs testing on human subjects and is a “covered entity,” must comply with HIPAA. The remainder of the Department is a health oversight agency (“an agency or authority of . . . a State, . . . , including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system . . .”). 45 CFR § 164.501.
- D. HIPAA requires that hybrid entities designate their programs that would be “covered” entities if they were a separate legal entity, and identify them in the Notice of Privacy Practices, as the entity’s “covered component.” 45 C.F.R. § 164.103. The Department’s Laboratory and its support services are the only areas of the Department that perform business activities that are covered functions under HIPAA. The Department has posted its notice of privacy practices on its website, which states the uses and disclosures the Laboratory can undertake with the personal health information it has in its possession.

Please go to [http://www.ct.gov/dph/lib/dph/hipaa/pdf/npp\\_\(final\)\(10.3.14\).pdf](http://www.ct.gov/dph/lib/dph/hipaa/pdf/npp_(final)(10.3.14).pdf) to access the Notice of Privacy Practices posted on the Department’s website.

- A. Basic HIPAA rule regarding non-disclosure:  
A fundamental rule under HIPAA is that covered entities may not disclose personal health information except as permitted by HIPAA: a specific authorization is provided (i.e. patient’s waiver), identifying information is removed, or a HIPAA exception applies.
- B. In the case of disclosures from the Department’s Laboratory to the Newborn Screening (“NBS”) unit of the Department, there are three relevant exceptions that permit the Laboratory testing unit, the HIPAA covered entity, to disclose personal health information to the NBS program, a health oversight entity: the “required by law” exception (45 CFR 164.512(a)), disclosures to health oversight agencies for “public health activities” (45 CFR 164.512(b)), and disclosures to health oversight agencies for “public health oversight activities” (45 CFR 164.512(b)).
- C. The Department’s Laboratory has a Certificate of Compliance pursuant to the Clinical Laboratory Improvement Amendments of 1988 (CLIA, 42 USC § 263a). CLIA requires that the Laboratory promptly report to providers, findings that may indicate a serious or life-threatening condition.

- D. Pursuant to state law, the NBS unit is also responsible for promptly reporting certain life-threatening conditions as part of its responsibilities as a health oversight agency. Therefore, the NBS unit and the Laboratory have a Memorandum of Understanding (“MOU”) whereby the NBS unit is the business associate<sup>1</sup> of the Laboratory for HIPAA purposes. Under the MOU, the NBS unit makes prompt reports to comply with its statutory mandates, and on behalf of the Laboratory to comply with CLIA. The NBS unit receives the personal health information from the Laboratory as both a health oversight agency and as a business associate of the Laboratory.
- E. As a business associate of the Laboratory, the NBS unit maintains a record of disclosures of personal health information for a period of 6 years (excluding disclosures for research purposes); provides the Laboratory with such records upon request; and makes internal practices, books and records relating to use and disclosure of personal health information available to the Secretary of Health and Human Services upon request.
- F. On some occasions, covered entities such as hospitals or physicians will cite HIPAA for their refusal to disclose personal health information to the Department. Occasionally, a covered entity will claim that the Department must enter into a business associate agreement with the covered entity in order to obtain the documents. In fact, neither of these claims is correct, and the Department need not and should not enter into business associate agreements with covered entities to obtain such documents. To do so would impose unduly burdensome requirements on the non-covered programs of the Department to comply with many of the HIPAA provisions.
- G. HIPAA specifically permits covered entities to release personal identifiable health information to public health oversight agencies such as the Department’s non-covered programs without patient authorization, consent or release, and without providing the patient with an opportunity to object. In particular, HIPAA permits such disclosure to the Department’s non-covered programs (1) for their public health oversight activities, (2) for their public health activities, and (3) as required by law. 45 CFR § 164.512(d). Additionally, HIPAA requires that such non-covered programs of the Department assure the covered entities that the information they seek is what is minimally necessary to accomplish the purpose of the disclosure, and HIPAA permits the covered entity to rely on such representation.

---

<sup>1</sup> A business associate performs services on behalf of the covered entity that requires the disclosure of personal health information, among other things. 45 CFR § 164.502 (e)(1).

## Appendix C Department Program Specific Information

Note that each of the statutory and regulatory provisions listed in Appendix C are the most current version as of the date of this writing. Each employee handling a data request must review the most current version of the statutes and regulations in order to make an informed decision.

Every person working at the Department has a legal duty to protect the confidentiality of individually identifiable health data collected by and maintained at the Department. Such duty continues after leaving state employment. It is, therefore, very important that every Department employee or contractor be familiar with the confidentiality laws that apply to the data with which the employee or contractor works.

### 1. Abortion Data

#### A. Authority to collect health information:

**Section 19-13-D54(b) of the Regulations** requires that physicians report to the Department all induced abortions within 7 days of performing such procedures. The reports must specify the date of the abortion, location, age of woman, town and state of residence, approximate duration of pregnancy, method of abortion, and explanation of any complications. The name of the woman is not required and should not be provided.

#### B. Confidentiality & disclosure of information:

**Section 19-13-D54(b) of the Regulations.** The Department maintains such reports in a confidential file and only uses them for statistical purposes. Reports are destroyed after two years.

### 2. Adoption Records

#### A. Authority to collect health information:

**Section 45a-745 of the Statutes.** Probate court clerks create records of final adoption decrees and provide the records to the Department, including sufficient information to locate and

identify the original birth certificate of the adopted person, to establish the new birth certificate, and sufficient identification of the court action and proceedings.

**Section 7-53 of the Statutes- Birth certificates of adopted persons born in this state.** The Department receives the record of adoptions created pursuant to § 45a-745 of the Statutes and creates new birth certificates with all the information required in this state, except that the adopting parents are named as the parents. No new certificate shall be created, if requested by the court, adoptive parents or adoptee, if over fourteen years of age. **Section 7-54 of the Statutes-Certificates of birth registration or certificate of foreign birth for person born outside of the country and adopted by a state resident.** The Department is required to prepare a certificate of foreign birth of persons born outside the country who have been adopted by a person residing in the state, if the Probate court provides a specific written request to the Department with an authenticated and exemplified copy of the order of adoption of the court in which the adoption proceedings took place, or any other evidence the probate court considers sufficient. The foreign birth certificate shall contain the adopted person's name, sex, date of birth, place of birth, legal name of adoptive parent(s), and the date of preparation of such certificate of foreign birth.

**Section 19a-40 of the Statutes** delegates the general supervision of vital records registration, including records of marriage, death, birth, and fetal death to the Department.

**Section 19a-42 of the Statutes-Amendment of vital records.** Only the Commissioner may amend birth certificates to reflect changes in parentage, or gender. The Commissioner and the registrar of vital records shall maintain sufficient documentation to support amendments.

## **B. Confidentiality & disclosure of information:**

**Section 7-53-1 of the Regulations.** Adoption files and original birth certificates of adopted persons are confidential and must be placed in sealed envelopes. Once the Department prepares the new birth certificate, the vital records registrars of the town of birth and the town where the mother resided at the time of birth shall receive an attested copy of the amended birth certificate. The new birth certificate cannot indicate that an adoption has taken place; original birth certificates shall be kept in a separate sealed file, and unless otherwise provided by statute, access to confidential adoption records shall be restricted to the Department's or local registrar vital records' staff.

**Section 7-53-3 of the Regulations-Replacement certificate.** Replacement birth certificates must be issued as certified copies. For birth certificates of adopted persons recorded prior to 1979, the Department must redact any reference to the fact that the person was adopted when issuing the new certified copy.

**Section 7-53 of the Statutes-Birth Certificates of adopted persons born in this state.** For adoptions taking place on or after October 1, 1983, an uncertified copy of the original birth certificate shall be issued upon request of the adopted person, if at least eighteen years old, or such adopted person's adult child or grandchild. Any other person seeking to examine or obtain a copy of the original record or certificate of birth of an adopted person must first obtain a written order from the judge where the adoption took place, or a written order of the Probate Court in accordance with §45a-752 of the Statutes. If authorized by a court order, the Department will issue an uncertified copy of the original birth certificate marked with a notation that the birth certificate has been superseded by a new birth certificate.

**Section 7-54 of the Statutes.** Once the Department prepares a certificate of foreign birth for a person born abroad and adopted by residents of this state, it can subsequently issue copies of certificates in accordance with § 7-52 of the Statutes (the Department can provide certificates to the person to whom it relates, if the person is over the age of 16, or to the parent, guardian, spouse, child (if older than 18 years of age), grandparent or legal representative).

**Section 19a-42 of the Statutes-Amendment of vital records.** Any person requesting to amend a vital record must provide sufficient documentation to support the amendment. The Commissioner must ensure the confidentiality of such documentation as required by law. Once a certificate has been amended, the original certificate in the case of parentage or gender change shall be physically or electronically sealed and kept in a confidential file, and only be unsealed for viewing or issuance upon written order of a court of competent jurisdiction, except as provided by 19a-42a regarding amendments related to paternity, and section 7-53 regarding original birth certificates of adopted persons. Vital Records must forward the amended certificate to the affected registrars of vital statistics.

### **3. Affirmative Action**

#### **A. Authority to collect health information:**

**Section 46a-68 of the Statutes and § 46a-68-89 of the Regulations-Grievance procedure.** Authorizes the equal employment opportunity officer (EEOO) to investigate all discriminatory conduct within the Department. Because affirmative action ("AA") is required to prepare the annual AA Plan, AA also collects a variety of important information from Human Resources ("HR") and other branches regarding hiring, disciplinary, and training practices.

**Regulation § 46a-68-81** further requires that the Department maintain a record of each member of its diversity advisory committee, identified by name, race, position, and amount of time dedicated to such duties.

**Section 46a-68-99 of the Regulations-Access to records and personnel.** Each agency shall provide the EEOO with reasonable access to records and personnel (interviewing employees, inspecting and copying, and removing off-site copies of books, records, accounts or any other material relevant to evaluation of the Plan).

**B. Confidentiality & disclosure of information:**

**Section 46a-68-89 of the Regulations-Grievance procedure.** AA reports all findings and recommendations upon the conclusion of an investigation to the commissioner.

**Section 46a-68-89(b) of the Regulations.** All records of grievances and disposition thereof, as well as any record used to determine pattern of grievances are maintained for two years, and shall periodically be reviewed by the EEOO. Such records are confidential except when disclosure is required by law (the public has a legitimate interest in disclosure and does not fall into the §1-210(b)(2) exemption i.e., the subject matter is a private matter and disclosure of the subject matter would be highly offensive to a reasonable person).

**Case Law: Roque v. Freedom of Information Commission, 255 Conn. 651; 774 A. 2d 957 (April 2001)** held that: (1) information such as the date when and location where sexual harassment allegedly occurred was of legitimate public concern, and thus, such information was not exempt from disclosure; and (2) identity of the complainant and the sexually explicit portions of the investigation documents were exempt from public disclosure pursuant to Freedom of Information Act's invasion of personal privacy exemption. The identity of a complainant in all other cases, however, is not always exempt.

**Section 46-68-89(c) of the Regulations.** The information collected by the EEOO is used to create a summary of matters alleged indicating results, length of time required to resolve the case, number of such complaints, and whether a matter is pending or has been resolved. This information is included in the Plan. All records shall be maintained and available for examination by the Commission of Human Rights and Opportunities ("CHRO").

**Section 46a-68-98 of the Regulations-Record retention.** All records are kept for two years from the date of the making of the record about the personnel action involved. When a charge of discrimination has been filed, the agency shall preserve all personnel records relevant to the charge or action until final disposition of the matter.

**Section 46-68-101 of the Regulations-Request for information.** AA is required to disclose to CHRO records in its possession and allow the examination of persons upon request.

## 4. AIDS

### A. Authority to collect health information:

**Sections 19a-2a(9) and 19a-215 of the Statutes.** The Commissioner is authorized to compile a list of reportable diseases and providers are required to report to the Department.

**Section 19a-54a of the Statutes-Registry of data on infants exposed to AIDS medication.** The Department may establish a registry of data on infants who have been exposed to HIV or AIDS medications, and study the effects of such medications.

**Section 19a-583(a)(3) of the Statutes** permits persons to disclose HIV-related information to the Department and Local Health as mandated by §§ 19a-2a(9) and 19a-215 of the Statutes.

**Section 19a-2a-22 of the Regulations.** Physicians, institutions, laboratories, infection control practitioners, AIDS coordinators in various health care facilities or private practice provide reports to the Department about significant AIDS/HIV information. The AIDS/HIV data system also obtains relevant AIDS/HIV information from death certificates.

### B. Confidentiality & disclosure of information:

**Section 19a-215(c) of the Statutes.** Reports of reportable disease and laboratory findings are confidential pursuant to CGS §19a-25.

Pursuant to **§19a-25 of the Statutes**, all the information pertaining to AIDS/HIV is confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**Section 19a-25-1 of the Regulations** lists all of the definitions used in 19a-25-1 through 19a-25-4, inclusive.

**Section 19a-25-2 of the Regulations-Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports: (1) are prepared for the purpose of medical and scientific research; (2) and do not include identifiable health data.

**Section 19a-25-3 of the Regulations- Disclosure of identifiable health data.** The Department cannot disclose identifiable health data except that the minimum necessary may be disclosed: (1) to healthcare providers in a medical emergency to protect the health, life, or wellbeing of the person with a reportable disease; (2) to healthcare providers, the local health director, another state or public health agency, or other persons as necessary for disease prevention and control or to reduce morbidity and mortality; and, (3) for research. Identifiable health data is not subject to subpoena or compulsory process in any legal proceeding, and no one can be compelled to testify regarding such health data.

**Section 19a-25-4 of the Regulations-Use of health data for enforcement purposes.** The Department can use aggregate and identifiable health data to perform statutory and regulatory duties and to secure compliance with laws. Where such data is used in an enforcement action, disclosure to parties is permitted only if required by the administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver of the confidentiality that protects such data.

**Section 19a-124 of the Statutes.** The Needle Exchange Program created pursuant to this section is required to provide confidential services.

**Section 19a-583 of the Statutes** prevents disclosure of HIV AIDS information by the Department, among other things.

**Section 19a-584 of the Statutes-**Informing and warning of known partners of possible exposure to the HIV virus. Disclosure of HIV-related information to public health officers. Public health officials ("PHO") may inform or warn a known partner who may have been exposed to HIV under certain enumerated circumstances but, in no event, PHOs shall disclose the identity of the infected person or other partners.

**Conn. Att'y Ge. Op. No. 92-010 (April 13, 1992).** Pursuant to §19a-583(b) of the Statutes, the Commissioner cannot further disclose information received pursuant to Chapter 368x except in connection with morbidity and mortality studies (§ 19a-25 of the Statutes) and pursuant to any of the exception contained in §19a-583(a) of the Statutes. Also, "[t]o protect the confidentiality of AIDS or HIV-related information, the Department cannot publicly disclose in an allegation in a Statement of Charges that a licensee has AIDS or an HIV-related illness. Moreover, any portion of a hearing wherein evidence is received regarding a licensee's AIDS or HIV status should not be open to the public and should be held in executive session. Public disclosure of such information and evidence would violate the confidentiality provisions of §19a-583 [of the Statutes]."

## 5. Birth Defects

### A. Authority to collect health information:

**Section 19a-50 of the Statutes relating to cardiac defects** designates the Department “to administer a program and services for children with physical disabilities or who are suffering from conditions which lead to such disabilities or suffering from cardiac defect or damage.”

**Section 19a-53 of the Statutes-Reports of physical defects of children.** Enumerated licensed providers having knowledge that a child under five has any physical defect shall, within 48 hours from the time of acquiring such knowledge, file a written report with the Department in a form prescribed by the Department, which includes the name and address of the child and the child’s parents, and the nature of the physical defect.

**Section 19a-56a of the Statutes-Birth surveillance program**-authorizes the Department to maintain data about birth defects and other adverse reproductive outcome surveillance programs in order to monitor frequency of defects. It further requires that general acute care hospitals make available to the Department the medical records of patients diagnosed with birth defects/adverse reproductive outcomes for research and verification of data.

**Section 19a-2a-3 of the Regulations** authorizes the Department to collect personal health information about children with special needs and birth defects.

### B. Confidentiality & disclosure of information:

**Section 19a-56b of the Statutes.** All birth defect information collected pursuant to 19a-56a is confidential in accordance with §19a-25, and shall be solely used for the purposes of the program. The Department shall maintain records of all persons who have access to this data, which includes name, title, organizational affiliation, dates of access, and the specific purpose for the access.

Pursuant to C.G.S. §19a-25, all information, records of interviews, written reports, and statements, including data concerning a person’s medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be solely used for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that data recipient does not further disclose the data.

**PHC §19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4 of the Regulations, inclusive.

**PHC §19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC §19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **6. Breast Cancer**

### **A. Authority to collect health information:**

**C.G.S. § 19a-72 and PHC §19a-2a-10** authorize the commissioner of the Department to promulgate a list of tumors, including breast cancer, track, collect personal health information, and follow all women screened for breast and cervical cancer in the program. Hospitals, clinical laboratories, and health care providers are required to report on a form prescribed by the Department, and the Department is further authorized to access patients' records in order to perform case findings or other quality improvement audits.

**PHC §§ 19a-73-1 through 19a-73-5** require that short and long term care hospitals provide the Department with the occupational history (places, types, and length of employment) of cancer patients prior to diagnosis on a form prescribed by the Department.

**PHC §§ 19a-73-1 through 19a-73-6** require that chronic disease hospitals report to the Department, in a form prescribed by the Department, within six months of the close of the calendar year, the occupational history of each cancer patient along with information concerning diagnosis, stage of disease, medical history, laboratory data, tissue diagnosis, radiation, surgical or other methods of treatment, and annual life-time follow-up on each cancer patient at such times as are necessary to maintain the Connecticut Tumor Registry.

**C.G.S. § 19a-74** authorizes the Department investigate the cause, prevention, treatment, and mortality of cancer as well as the means to reduce mortality rates.

**C.G.S. § 19a-266a** establishes a system for early detection that tracks, collects personal health information, and follows all women screened for breast and cervical cancer.

### **B. Confidentiality & disclosure of information:**

**C.G.S. § 19a-72(e)** authorizes the Department to "enter into reciprocal reporting agreements with the appropriate agencies of other states to exchange tumor reports."

Pursuant to **C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other

governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

---

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC § 19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **7. Children and Youth with Special Health Care Needs**

### **A. Authority to collect health information:**

**Section 19a-54 of the Statutes** requires that each institution supported in part or whole by the State report to the Department, on a form prescribed by the Department, the name and address of each child under 21 years of age who is physically handicapped for whom an application has been made for admission, whether such child is admitted or rejected.

**Sections 19a-48, 19a-55, 19a-59, & 19a-61 of the Statute.** These provisions require that healthcare personnel who have professional knowledge about any child under five years of age with a physical defect or handicap, report to the Department within 48 hours of becoming aware of such information the child's personal health information.

**Section 19a-2a-3(a)(6) &(b)(1)(j) of the Regulations** provide legal authority for the collection of personal health information about children with special needs.

**Section 19a-2a-3(b)(1)(j) of the Regulations** lists medical information regarding children with special needs as one of the data sets the Department is authorized to collect.

## **8. Drinking Water**

### **A. Authority to collect health information:**

**Section 19-13-B102(e) of the Regulations** authorizes the Department to collect water testing reports.

**Section 25-32e(a) of the Statutes.** The Department has authority to collect information about the purity of water supplies.

### **B. Confidentiality & disclosure of information:**

**Section 1-210(b)(19)(ix) of the Statutes.** No water company records may be disclosed pursuant to §1-210(a) of the Statutes if the information poses a security risk, except to a law enforcement agency. Such records include: vulnerability and risk management plans, operational plans, portions of water supply plans submitted pursuant to §25-32d of the Statutes that contain or reveal information the disclosure of which may result in a security risk to a water company, inspection reports, technical specifications and other materials that depict or specifically

describe critical water company operating facilities, and collection and distribution systems or sources of supply.

**Section 1-210(d) of the Statutes** requires that, with the exception of the Judicial or Legislative Departments, when a public agency receives a request for disclosure of records described in §1-210(b)(19) of the Statutes, the agency promptly inform the Commissioner of Public Works before complying with such request, and if the record requested pertains to a water company, the agency must inform the water company before complying with such request. If the records requested are exempt pursuant to §1-210(b)(19) of the Statutes, the Commissioner can order the withholding of the records. The Commissioner of Public Works has jurisdiction to hear appeals from withholding of records.

**Section 25-32d(a) of the Statutes.** The Department should share water plans with the Commissioner of Energy and Environmental Protections and Public Utilities Regulatory Authority, and the secretary of the Office of Policy and Management.

## **9. Emergency Medical Services**

### **A. Authority to collect health information:**

**Section 19a-177(8)(A) of the Statutes** authorizes the Department to develop a data collection system that documents patient service from his/her initial entry into the emergency medical service system through arrival at the emergency room, and which may expand to include clinical treatment and patient outcome data.

**Section 19a-180(b) of the Statutes.** The Department is authorized to collect reports, documents, tapes, or other documents during investigation of any person, management service organization or emergency medical service organization. This information is not subject to disclosure pursuant to §1-210 of the Statutes for six months from the date of the start of the investigation, or until the investigation is terminated, or a hearing is convened.

**Section 19a-2a-7 of the Regulations** authorizes the collection of personal data by the office of emergency medical services in order to maintain documentation relating to technicians and instructors licensed or certified. This regulation is authorized by §§ 19a-178 to 19a-180 of the Statutes.

## **10. Environmental Health Data**

### **A. Authority to collect health information:**

***Asbestos***

**PHC §§ 19a-2a-6 and 19a-332-4** authorizes the Department to request information regarding asbestos abatement projects, including the names, social security numbers, and control access of all personnel working in asbestos abatement sites from asbestos contractors (authority for promulgating regulation: §19a-332a).

**PHC §19a-332a-4(b)(8)** references OSHA regulations requiring medical testing of employees and authorizes the Department to obtain records.

**Section 19a-332-4(b)(6) of the Regulations.** Records may include records maintained by a contractor pursuant to §19-332-4(b) of the Regulations requiring that asbestos contractor maintain a complete list of names and social security numbers of asbestos abatement workers, site supervisors and other agents involved in the asbestos abatement activity and working for the asbestos contractor on projects, and individuals entering the enclosed work area.

**Section 20-435 of the Statutes.** License applications for asbestos contractors must be made on a form provided by the Department and provide information regarding the applicant's qualifications as required by the regulations.

#### ***Environmental Health Practitioner Licensing***

**Section 19a-14 of the Statutes.** The Department has the power to collect information in order to evaluate credentials, and in the course of exercising its investigatory powers.

**Section 17b-137a(a) of the Statutes** requires that applicants for licensing record their social security number in their applications.

**Section 20-435 to 20-439, 20-341, 20-475 to 20-477, and 20-361 of the Statutes, as well as §§ 19-13-B103e(b), 20-440-3-5, 20-440-8, 20-440-2, 20-478-2 of the Regulations.** Applications for asbestos worker, site supervisor, consultant, inspector, management planner, project designer, project monitor, contractor, and training provider; lead abatement contractor, supervisor, worker, consultant contractor, inspector, inspector risk assessor, planner, project designer, and training provider; registered sanitarian; and subsurface sewage cleaner, and installer are required to provide name, address, list of states where applicant holds licenses, certifications, and accreditations, and list consultants for whom applicant has worked for on a form provided by the Department.

#### ***Occupational Health***

**Section 19a-215 of the Statutes.** The following are environmental/occupational conditions that are on the laboratory reportable disease list: carbon monoxide poisoning (carboxyhemoglobin

>=9%), lead poisoning (lead blood levels>=10 ug/dl), and mercury poisoning (urine creatinine >=35ug/dl; blood creatinine >=15 ug/dl).

**Section 31-40a of the Statutes.** Physicians must report to the Labor Department and Department of Factory Inspection the name of persons suffering from poisoning from lead, phosphorus, arsenic, brass, wood alcohol or mercury or their compounds, anthrax, compressed-air illness, or any other disease contracted as a result of the nature of the employment.

**Section 31-400 of the Statutes** authorizes the Commissioner of the Department and the Commissioner of the Labor Department to conduct investigatory studies and surveillance during a health emergency, suggested disease cluster, or imminent hazard.

**Section 19a-2a-6 of the Regulations** authorizes the collection of environmental health data for the environmental health data system for professional licenses, professional registrations, certifications, environmental inspection results, and occupational exposure results (lead exposure, education, employment history, inspectional, training and work experience, and medical information). The purpose of this data is to document reduced morbidity and mortality and improve the living conditions of state residents by educational and regulatory programs, and passive programs that address hazards. This regulation is authorized under §19a-110 to 19a-111d; 19a-421; 19a-426; and 20-435 to 20-439 of the Statutes.

**Section 19a-332a-4(b)(8) of the Regulations** requires medical testing of employees and authorizes the Department to obtain such records.

#### ***Food Borne Illness Protection Program***

**Section 19a-36 of the Statutes.** Power to establish the Public Health Code

**C.G.S. § 19a-14(d)** Records obtained by the Department as part of an investigation are not subject to disclosure under **§ 1-210 of the Statutes** for one year from the commencement of the investigation, or until such time as the investigation is terminated pursuant to a withdrawal or other informal disposition, or until a hearing is convened.

**Section 19a-215 of the Statutes. Reports of disease on the commissioner's list of reportable disease and laboratory findings. Confidentiality.** This section requires physicians to report to the Department or LH cases in the reportable disease or laboratory findings included on the Commissioner's list (*See* § 19a-2a of the Statute, and Department's Website) within 12 hours of becoming aware of such disease or laboratory findings. Reports of reportable disease and laboratory findings are confidential pursuant to § 19a-25 of the Statutes.

**Section 19-36-A5 of the Regulations. Confidential Data.** All epidemiologic information containing personal health information gathered during the investigation of reported cases or

suspected cases of disease or during the investigation of outbreaks of disease by the state or local health shall be confidential.

### ***Lead***

**Section 19a-110 of the Statutes. Report of lead poisoning. Availability of information regarding lead poisoning.** This section requires community health centers, laboratories, etc. to report to the Department, personal health information about persons with levels of lead in the blood equal to or greater than ten micrograms per deciliter of blood or any other abnormal body burden of lead.

**Section 19a-111 of the Statutes** requires that the Department maintain comprehensive records of all reports submitted pursuant to § 19a-110 of the Statutes (report of elevated blood levels from hospitals, laboratories, and local health officials), § 19a-111-3(a) of the Regulations (when inspector finds toxic levels of lead requiring abatement and potential lead poisoning of children, the inspector must report to the Commissioner), and § 19a-113-8 of the regulations (reports from local code enforcement agencies about medical status of lead poisoned children, and corrected and uncorrected violations).

**Section 19a-111-3(e) of the Regulations.** Local Health inspectors shall report to the Commissioner toxic levels of lead requiring abatement, in a form prescribed by the Department two days after the completion of such report.

**Section 19a-215 of the Statutes** requires physicians to report to the Department or LH cases in the reportable disease or laboratory finding included on the Commissioner's list (*See* § 19a-2a of the Statute, and Department's Website) within 12 hours of becoming aware of such disease or laboratory finding. Reports of reportable disease and laboratory findings are confidential pursuant to § 19a-25 of the Statutes.

**Section 19a-36-A4 & A6 of the Regulations** authorize the Department to obtain medical information when investigating cases in the reportable disease list. Each report of a case or suspected case of reportable disease shall include the full name and address of the person reporting and of the physician attending; the diagnosed or suspected disease and date of onset; the full name, age, race/ethnicity, sex and occupation of the affected individual; and other facts the department or local director of health requires for purposes of surveillance, control and prevention of reportable diseases. The reports shall be sent in envelopes marked "CONFIDENTIAL."

Pursuant to **C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of

medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

---

**PHC §19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

---

**PHC §19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC §19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical and scientific research.”

“No identifiable health data obtained in the course of activities undertaken or supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **11. Facility Licensing and Investigation**

### **A. Authority to collect health information:**

#### **Section 19a-127n of the Statutes. Adverse events. Reporting requirements. Regulations.**

**Confidentiality.** Significant medical errors along with the status of any corrective steps shall be reported in writing not later than seven days after the date on which the adverse event occurred; and a corrective plan shall be submitted within 30 days of that same date. Such reports are not subject to subpoena, discovery, or introduction into evidence in any judicial or administrative proceeding except where otherwise specifically prescribed by law, or in disciplinary or licensing proceeding as prescribed by §19a-499 of the Statutes.

#### **Section 19a-498 of the Statutes-Inspections, investigations, examinations and audits.**

**Retention of records.** The Department is authorized to conduct biennial licensure inspections of all institutions and any other inspections deemed necessary, and order the production of records necessary to conduct investigations and hearings.

**Section 52-146o of the Statutes.** Physicians, surgeons, or health care providers can disclose privileged information received from patient or patient's conservator or guardian to the Department when authorized by statute or regulation or in connection with an investigation of a complaint, if such records are related to a complaint; child abuse; abuse of an elderly, physically disabled or incompetent person; or abuse of an individual with mental retardation.

In accordance with **§19-13-D4a(i)(7) of the Regulations**, short-term hospitals are required to file reports of suicides, accidents, or injuries which may result in a permanent defect, scar, or handicap within 24 hours.

**Section §19-13-D6 of the Regulations** authorizes the collection of personal health information about residential care home residents.

**Section 19-13-D8t(f)(3) of the Regulations** authorizes the collection of long-term care residents' personal health information and the creation of a data system.

**Section 19a-2a-5 of the Regulations** authorizes the collection, maintenance and use of nursing data.

**Section 19a-495-551 of the Regulations.** Private Freestanding Mental Health Residential Living facilities are required to provide incident reports to the Department, which contain medical and personal health information.

**Section 19a-2a-9 of the Regulations** is the authority for collection of long-term care residents' personal health information and the creation of a data system.

HIPAA 45 C.F.R. §§ 164.508(a)(2)(ii), 164.512(a) & (b), and 42 C.F.R. 2.53 permit the Department to conduct audits and evaluations of drug and alcohol treatment facilities and require access to treatment records only in the capacity of a state agency performing regulatory activities as an oversight agency authorized by law to conduct such activities. Thus, the Department is authorized to obtain psychotherapy notes, and any other personal health information in such facilities. The Department, when records are copied or removed from the premises, must agree in writing to: maintain information in accordance with 42 C.F.R. 2.16; destroy identifying information upon completion of audit or evaluation; and only disclose back to the specific program from which it obtained the information (see 42 C.F.R. 2.53(d)).

**B. Confidentiality & disclosure of information:**

**Section 19a-14(d) of the Statutes** authorizes the Department to conduct any necessary investigation and follow-up. With the exception provided by § 20-13e of the Statutes, which applies to physicians, the records obtained by the Department as part of an investigation are not subject to disclosure under § 1-210 of the Statutes for one year from the commencement of the investigation, or until such time as the investigation is terminated pursuant to a withdrawal or other informal disposition, or a hearing is convened. A complaint is subject to disclosure pursuant to § 1-210 of the Statutes from the time it is mailed to the respondent. Public records remain subject to disclosure even if they are part of an investigation.

**Section 19a-499 of the Statutes.** With the exception of questions of licensure or proceedings before the Office of Health Care Access, investigation or inspection reports of health care institutions received or created by the Department cannot be released to the public if the reports identify patients or institutions for the earlier of six months from the date of initiation, until the investigation is resolved, or until a contested case hearing is convened.

**Section 20-578 of the Statutes.** With the exception of proceedings involving the question of the right to practice, the Department cannot disclose names of individuals or institutions mentioned in investigatory reports.

**Section 52-146f(6) of the Statutes. Disclosure of communication, Consent not required for disclosure.** Communication of records may be disclosed to the Commissioner in connection with any inspection, investigation or examination of an institution, as defined in subsection (a) of section 19a-490 of the Statutes, authorized under section 19a-498 of the Statutes.

**Section 19a-127n of the Statutes. Adverse events. Reporting requirements. Regulations. Confidentiality of reports.** Significant medical errors and corrective plan reports are not subject to subpoena, discovery, or introduction into evidence in any judicial or administrative proceeding except where otherwise specifically prescribed by law, or in disciplinary or licensing proceeding as prescribed by §19a-499 of the Statutes.

## **12. Healthy Start**

Information from Healthy Start Grantees Providing Services to Women, Infant, and Children  
(Healthy Start-Information from Grantees Providing Services to Women, Infant, and Children)

### **A. Authority to collect health information:**

**Section 19a-59b of the Statutes** provides authority to create the healthy start data system that includes personal medical health information from needy pregnant women and children under the age of six who have an income equal to or less than one hundred eighty-five per cent of the poverty level.

**Section 19a-2a-11 of the Regulations.** The Department creates a healthy start system to maintain personal data in order to provide services, monitor program accountability, carry out program evaluation, and apply for federal financial aid. The data is obtained from grantees and community health centers providing services to women, infants, and children.

## **13. Hearing Office**

### **A. Authority to collect health information:**

**Section 19a-87b-10(j)(3) of the Regulations.** Licensees are required to report to the Department of Children and Family any actual or suspected child abuse or neglect. This regulation is authorized by §§17a-101 and 17a-102 of the Statutes.

### **B. Confidentiality & disclosure of information:**

**Sections 17a-101(g), 17a-101(k), and 19a-80f of the Statutes.** All records concerning child abuse or neglect are confidential and their unauthorized disclosure is criminal. DCF findings of abuse and/or neglect in the registry are confidential. All references to the children involved are to be redacted from the transcript, maintained in sealed exhibits, or otherwise kept confidential.

**Section 19a-87b-14(b) of the Regulations. Confidentiality of Child Abuse and/or Neglect Investigations.** Complaints that allege or that may constitute allegations of child abuse or neglect and information, including but not limited to the identity of the complainant, are

confidential. Information that can be disclosed: number of cases, types and dates of the Department's contact with the provider about the complaint issues, the general status of a current investigation about the complaint or the Department's findings if the investigation has been completed.

**CT. Attorney General Opinion No. 93-010 (April 13, 1992).** To protect the confidentiality of AIDS or HIV-related information, the Department cannot publicly disclose any allegation in a Statement of Charges that a licensee has AIDS or an HIV-related illness. Moreover, any portion of a hearing where evidence regarding a licensee's AIDS or HIV status, should not be open to the public and should be held in executive session. Public disclosure of such information and evidence would violate the confidentiality provisions of §19a-583 of the Statutes.

## 14. HIC

### **Confidentiality & disclosure of information:**

Pursuant to **C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) "the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers,

the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

**Note:** Please see the General Provisions as well as the specific provisions for each program.

## **15. Human Resources: Medical Records of Employees**

### **Confidentiality & disclosure of information:**

**Section 1-214 of the Statutes** requires state agencies to notify an employee and his/her collective bargaining representative of requests for access to personnel or medical files or similar files which the agency believes would constitute an invasion of privacy. Should an objection to disclosure be filed pursuant to such notice, the state agency is prohibited from disclosing the records unless ordered to do so by the Freedom of Information Commission pursuant to § 1-206.

**Section 4-190 et seq. of the Statutes** contains provisions of the Personal Data Act. Personal data encompasses personal identifiable information about a person’s education, finances, medical or emotional condition or history, employment or business history, family or personal

relationships, reputation or character. These provisions complement the provisions of the FOIA and § 19a-25 of the Statutes.

**Section 31-128f of the Statutes. Medical Records of Employees.** Employers may not disclose personal health without written authorization by employees. Exceptions: Affiliated entity, emergency, apprise employee, subpoena, court order, summons, warrant, discovery or grand jury request, to comply with state or federal law, pursuant to terms of collective bargaining agreement. Employer must inform employee of any such disclosure.

## **16. Infectious Disease**

### **A. Authority to collect health information:**

**Section 19a-215(c) of the Statutes. Reports of disease on the commissioner's list of reportable disease and laboratory findings.** Healthcare providers are mandated to report to the Department and Local Health Departments cases of reportable disease or laboratory finding included on the Commissioner's list (See §19a-2a of the Statutes, and the Department's Website) within 48 hours of becoming aware of such disease or laboratory finding.

**Section 19a-262 of the Statutes.** Physicians are required to provide to the Department personal health information about patients known or suspected of having tuberculosis.

**Section 10-204a-4(b) of the Regulations. Reporting of School Immunization Record.** Once per year, schools are required to prepare a summary immunization survey form and provide such survey to the Department.

### **B. Confidentiality & disclosure of information:**

**Section 19a-215(d) of the Statutes.** Reports of reportable disease and laboratory findings are confidential pursuant to §19a-25 of the Statutes.

**Section 19a-216 of the Statutes.** Any municipal health department, state institution or facility, licensed physician or public or private hospital or clinic, may examine and provide treatment for venereal disease to a minor. Treatment and consultation shall not be divulged, including the sending of a bill for the services to any person other than the minor, except for purposes of reports under § 19a-215 of the Statutes.

**Section 19a-216a of the Statutes. Examination of treatment of minor for venereal disease.**

Epidemiologic information about persons with communicable diseases must be kept strictly confidential and shall not be released by directors of health except in the following cases: de-identified information for statistical purposes, with informed consent, to health care providers to the extent necessary, to authorized agencies, and by court order necessary to enforce statutes or regulations. The information sought must be material, relevant and reasonably calculated to be admissible evidence during legal proceeding, the probative value must outweigh the individual's and public's interest, the merits of the litigation cannot be resolved without it, must be necessary to avoid substantial injustice, and no significant harm will result to the person examined or treated. Evidence must be examined in camera.

Except as listed above, no local health official shall be forced to testify without written consent of person examined or treated.

Pursuant to C.G.S. § 19a-25, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC §19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) "the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable

health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

**Section 19a-262 of the Statutes.** Reports and records of persons known or suspected of having tuberculosis Provides for the nondisclosure of records received by the Department pertaining to tuberculosis cases.

**Section 10-204a-4(c) of the Regulations.** All immunization information collected by the Department is confidential.

**Section 19a-2a-12, 19a-36-A1 through 19a-36-A6 of the Regulations-** These sections list the purpose, use, collection, and maintenance of infectious disease & personal data from Department of Correction, schools, Local Health directors, health counselors and educators by the Department, authorized researchers, for disease surveillance and evaluation of health education, and program intervention.

**Section 19-36-A5 of the Regulations. Confidential Data.** All epidemiologic information containing personal health information gathered during the investigation of reported cases, suspected cases of disease, or during the investigation of outbreaks of disease by the state or local health shall be confidential.

**Section 19a-36-A10 of the Regulations. Presumably exposed person may be examined and controlled.** Authorizes Local Health authorities to confer with physician and investigate suspected reportable disease, when a person has been exposed to a communicable disease, such as in the commission of an offense involving sexual promiscuity or illicit sex relations.

## 17. Immunization

### A. Authority to collect health information:

**Section 19a-7f of the Statutes** authorizes the Commissioner to gather data that identifies children that have fallen behind the required immunization schedule, and assist hospitals, and local health providers and departments in identifying such children, and develop outreach programs.

**Section 19a-7h of the Statutes** authorizes the Commissioner to create and maintain an immunization registry in order to ensure timely childhood immunization of all children who have not begun first grade, including all newborns, and requires health care providers to report to the Commissioner sufficient information to identify the child and the name and date of each vaccine dose given to that child, or when appropriate, contradictions or exemptions to administration of each vaccine dose.

**Section 19a-7h-1 of the Regulations** defines “Immunization registry” as the Department’s ongoing computer-based registry of children who have not yet begun first grade and their complete immunization history as authorized by 19a-7h of the Statutes.

**Section 19a-7h-2(a) of the Regulations** requires that the Connecticut birth registry provide the immunization registry with an electronic birth record of all children born after January 1, 1999 in Connecticut, within 7 days of receiving such information. The electronic birth record includes the infant’s name, birth date, hospital, birth certificate number, birth document control number, address, social security if available, infant’s parent names, birth dates, and address.

**Section 19a-7h-2(b) of the Regulations** requires that health care providers who vaccinate or provide an exemption from vaccination to any child born after January 1, 1999, report to the immunization registry within 14 days of such action, in a form prescribed by the Department: the child’s name, birth date, state of birth, current address, telephone number, and, if available, social security number; the child’s parents/guardians’ name, date(s) of birth, current address and telephone number; and the name, work address and work telephone number of the childcare provider.

Pursuant to **§ 19a-7h-2(c) of the Regulations**, health care providers provide any known change of identifying or locating information of children who the provider vaccinated and were born on or after October 1, 1994.

**Section 19a-7h-3 of the Regulations** requires that health care providers in outpatient settings and neonatal units vaccinating or providing permanent exemptions for vaccinations inform the Department of such vaccination within 14 days of providing the vaccination or exemption. In the case of a neonatal setting, the director of such neonatal clinic shall appoint an agent who should biweekly report to the Department the vaccination information of every newborn child. In the

case of outpatient settings, the report shall include: vaccinated or exempted child's name and date of birth; name of each vaccine exempted, whether exemption is for medical, religious, or because the child has a laboratory confirmation of natural infection with an infecting agent; the date the vaccine was provided or permanently exempted; and the name of the health care provider who order the doses, provided the exemption, and/or evidence of laboratory confirmation of natural infection

In the case of a neonatal care unit, the report shall include: the vaccinated child's name, date of birth, and hospital of birth; the biological mother's name; the name of each vaccine given; and the date the vaccine was administered.

**B. Confidentiality & disclosure of information:**

**Section 19a-7h(b) of the Statutes.** Each health care provider intending to administer vaccine to a child on the immunization registry, and each parent/guardian shall be provided current immunization records in order to determine whether additional doses are recommended to meet the school/child care immunization requirements.

Pursuant to §19a-7h(c) of the Statutes, all vaccination records are confidential pursuant to §19a-25 of the Statutes, and shall not be further disclosed without the authorization of the child or child's legal guardian.

**Section 19a-45a of the Statutes. Memorandum of understanding between the Commissioner of Public Health and Social Services for improving public health services.** DPH and DSS shall enter into MOU to improve public health service delivery and public health outcomes for low income populations by sharing HUSKY Health Program and Title V data if the data: (1) is directly related to Medicaid or any other DPH, or DSS plan; (2) complies with federal and state privacy, confidentiality, and security laws; (3) includes detailed description of the intended public health service/outcomes goals achieved; and, (4) can be afforded by both agencies.

**Section 19a-7h-4 of the Regulations. Release of information by the immunization registry.** The immunization registry shall provide immunization records to physicians who need to complete immunization records for school and entry requirements, provide sufficient identifying information about the child, and information about the need for additional doses. The provider must sign and complete a form prescribed by the Department where s/he acknowledges compliance with § 19a-7h of the Statutes and §§ 19a-7h-1 through and including 19a-7h-5 of the Regulations. The information is provided to the physicians by: a secure computer connection, fax to a telephone number provided by physician, telephone followed by mailing or faxing, or by other means approved by the Commissioner.

Pursuant to C.G.S. § 19a-25, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant

to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the

enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

**C.G.S. § 19a-7h(c)** provides for the confidentiality of medical and personal information, including vaccination status and dates of vaccines, on the childhood immunization registry.

**PHC § 19a-7h-4** allows the Department to release immunization records to health care practitioners who will be administering vaccination to a child and need to know the child’s vaccine history; parents or guardians; and, Local Health directors, if done in the appropriate form and attest to complying with PHC §§ 19a-7h-1 through 19a-7h-5.

## **18. Laboratory**

### **Confidentiality & disclosure of information:**

**Section 19a-36-A3(b) of the Regulations.** The director of a laboratory is required to report to the Local Health Department where the affected subject of the test resides, or to the Department any reportable laboratory finding within 48 hours that receives on forms provided by the department. All such reports are to be marked “confidential.”

**Pursuant to § 19a-36-A5 of the Regulations,** “all epidemiologic information, which identifies an individual and which is gathered by the state or local health department in connection with the investigation of reported cases or suspected cases of disease or during the investigation of outbreaks of disease, shall be kept in compliance with current confidentiality statutes.”

**Section 19a-36-D32 of the Regulations. Reports of findings.** Laboratories shall directly report findings to the licensed provider who ordered it, and laboratories other than the Department’s laboratory may provide laboratory findings to lay persons upon the written request of the provider who ordered the testing. Laboratories other than the Department’s laboratory may provide findings to statutorily authorized providers upon written request. Laboratories other than the Department’s laboratory may also provide findings upon the written request of providers who did not order the testing, so long as the requesting provider is also statutorily authorized to order such testing, and is providing care to the subject of the test. This section does not prohibit the release of findings to town, city or health officials when required by regulations, or the inspection or impounding of records of such reports by representative of the department.

**42 C.F.R. 493.1231** provides for the confidentiality of clinical laboratory test results.

**CLIA Regulation 42 C.F.R. § 493.1291(f)&(g). Report.** Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test. The laboratory must immediately alert the

individual or entity requesting the test and, if applicable, the individual responsible for using the test results when any test result indicates an imminent life-threatening condition, or panic or alert values.

**Section 19a-30a(a) of the Statutes.** Each clinical laboratory, which discovers a medical error shall promptly notify, in writing, to the authorized person ordering the test of the existence of such error, and promptly issue a corrected report or request for a retest, with the exception of HIV testing, in which case, errors shall be reported in person and counseling provided in accordance with chapter 368x.

HIPAA provisions apply to the laboratory data.

## **19. Newborn Screening**

### **A. Authority to collect health information:**

**Section 19a-55 of the Statutes** requires that the administrative officers or other persons in charge of institutions caring for newborn infants cause such infants to be tested for: HIV, Phenylketonuria and other metabolic disorders, hypothyroidism, galactosemia, sickle cell disease, maple syrup urine disease, homocystinuria, biotinidase deficiency, congenital adrenal hyperplasia, inborn error of metabolism. The Commissioner has jurisdiction for administering the newborn screening program and adopt regulations.

**Section 19a-56a of the Statutes. Birth Defects surveillance program.** Collection of birth defects data. Authorizes the Commissioner to establish a system for the collection of information about birth defects, and to have access to personal health information in hospital discharge records about patients with birth defects or other adverse reproductive outcomes.

**Section 19a-2a-15 of the Regulations. Newborn screening system.** The purpose of the newborn screening system is to track infants found to have a serious problem as a result of a blood test done right after birth. The director of the maternal infant health division is the official responsible for the newborn screening system. Data is received from any laboratory carrying out a newborn screening test. The data collected includes: name, sex, birthdate, place of birth, and medical information of infant; and the name and age of mother, address and telephone number of parents, and services received by the infant. This data is used to ensure that the infant received proper treatment and follow-up. Legal authority for this regulation is provided by § 19a-55 of the Statutes.

### **B. Confidentiality & disclosure of information:**

**Section 19a-2a-15 of the Regulations.** Retention of newborn screening system is governed by schedules prepared by the Connecticut State Library, the Connecticut Department of Public Records Administration, and records retention schedule provided in C.G.S. § 11-8a. Such records shall be maintained at the office of the official responsible for the records, and may be examined during normal business hours.

**Section 19a-55-3 of the Regulations.** Parents of an infant who object to their infant being tested because it is in conflict with their religion shall report their objection on a waiver form provided by the DPH, sign the waiver form, place the original in the infant's medical record, and submit a copy with the infant's unused specimen collection to the DPH Laboratory.

## **20. Local Health**

### **Confidentiality & disclosure of information:**

**Section 1-210(b)(3) of the Statutes.** Records of law enforcement agencies, including identity of informants/witnesses, not otherwise available to the public, are not required to be disclosed if the informant/witness would be endangered or intimidated.

**FOIA Docket #FIC1991-125; #FIC196-086;# FIC1998-144; #FIC2009-094.** Indicate that health authorities are law enforcement agencies, the identity of a complaining person constitutes an informant, and the identity of a complainant in a Local Health case is exempt from disclosure.

**Section 1-210(b)(16) of the Statutes.** Records of complaint, or information compiled in the investigation brought to a municipal health authority are not subject to release until such time as the investigation is concluded or thirty days from the date of receipt of the complaint.

## **21. Maternal and Child Health Protection Program**

### **A. Authority to collect health information:**

**Section 19a-59b of the Statutes** authorizes the Commissioner to establish a maternal and the child health protection program to provide maternal health services, and labor and delivery services to needy pregnant women and children under the age of six.

## **22. Newborn Hearing**

**A. Authority to collect health information:**

**Section 19a-59 of the Statutes. Program to identify newborn infants at high risk for hearing impairments.** Authorizes the Department to establish, implement, and operate a program of early identification of infant hearing impairment in order to identify infants at high risk, and inform parents of resources available for testing, treatment, and financial aid. The provisions of this subsection do not apply to any infant whose parents object to hearing screening as being in conflict with their religious tenets and practice.

**Section 19a-59-1 of the Regulations.** Institutions that provide childbirth services shall develop and implement newborn hearing screenings generating monitoring reports that consist of personal health information about the infant, in addition of the name of the person performing the screening, method and result of the screening, and whether the newborn was referred for further evaluation.

**23. Office of Health Care Access (OHCA)**

**A. Authority to collect health information:**

**Section 19a-654 of the Statutes.** OHCA is authorized to collect inpatient discharge data, outpatient surgery and emergency department data which includes individual patients' identifiable and physicians' data from short-term, acute care, general, and children's hospitals and outpatient surgical facilities. The data includes data extracted from patients' medical record abstracts and bills.

**B. Confidentiality & disclosure of information:**

**Section 19a-654(d) of the Statutes.** Data received by OHCA is confidential and is not considered public records under §1-200 of the Statutes. The data can be released if it is aggregate and/or de-identified pursuant to 45 CFR 1646.514 and Section 19a-167g-94 of the Regulations. Confidential data, however, may be released pursuant to §19a-25-3 of the Regulations or to: a) a state agency working to improve health care service delivery; b) a federal agency or the office of the Attorney General investigating hospital mergers and acquisitions; or c) another state's health data collection agency having a reciprocal data-sharing agreement with OHCA for certificate of need review or evaluation of health services purposes. OHCA and the requesting agency must have a written agreement which requires the latter to protect confidentiality of the data and to prohibit use of the data as the basis for any decision concerning a patient.

**Section 19a-654(e)** of the Statutes. Effective October 1, 2011, OHCA has a memorandum of understanding with the Comptroller for the Comptroller to access and to safeguard confidential information on individual patient and provider in the data.

**Section 19a-167g-94** of the Regulations. All hospital inpatient, outpatient surgical and emergency department data and outpatient surgical facility data procured by OHCA are confidential. The section provides information on how to create, to request and to release non-confidential or aggregate data.

**Pursuant to C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC §1 9a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) "the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to {C.G.S.} § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research."

"No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **24. Practitioners License & Investigation**

### **A. Authority to collect health information:**

**Section 19a-332a-4 of the Regulations** (Re OSHA regulations) requires the medical testing of asbestos workers and authorizes the Department to obtain such records.

**Section 19a-498(b) of the Statutes** authorizes the Department to obtain records, which may contain personal health information, during investigations and inspections of institutions under the Department’s jurisdiction.

### **B. Confidentiality & disclosure of information:**

**Section 19a-12a of the Statutes.** Information about the referral and investigation of the health care professional participating in the Assistant Program, created pursuant to § 19a-12a(b) of the Statutes, is confidential for the duration of such participation, and upon successful completion of the program, provided such participation is in accordance with terms agreed upon by the Department, the health care professional, and the Assistant Program.

**Section 19a-12a(i) of the Statutes.** If the Assistant Program Oversight Committee, created pursuant to § 19a-12b(a) of the Statutes, determines that a health care professional in the Assistant Program fails to comply with the terms and conditions of the program or refuses to participate in the program, the Assistant Program will disclose to the Department all records and files about the health care practitioner. The Department will determine if the health care

practitioner at issue is still a candidate for participation in the Assistant Program, if so, the records and files will remain confidential pursuant to §19a-12a(h) of the Statutes.

**Section 19a-12b(e)(3) of the Statutes.** If the Assistant Program Oversight Committee, created pursuant to § 19a-12b(a) of the Statutes, determines that an Assistant Program has not acted in accordance with the provisions of §§ 19a-12a and 19a-12b of the Statutes, or a corrective action plan issued pursuant to §19a-12b(e)(2) of the Statutes, the Oversight Committee will determine if the Assistant Program shall refer to the Department records and files of each of the health care professionals participating in the Assistant Program. The Department will, in turn, determine if the health care professional at issue is still a candidate for participation in the Assistant Program, if so, the records and files will remain confidential pursuant to § 19a-12a(h) Statutes.

**Section 17a-101k of the Statutes.** All information regarding records obtained by DCF while investigating allegations of abuse/neglect is confidential.

**Section 19a-14(d) of the Statutes.** Records obtained by the Department as part of an investigation, except in the case of physicians and veterinarians, are not subject to disclosure under § 1-210 of the Statutes for one year from the commencement of the investigation, or until such time as the investigation is terminated pursuant to a withdrawal or other informal disposition, or until a hearing is convened.

**Section 20-13e of the Statutes** requires that the Department initiate investigations of physicians within 18 months of filing of the petition that initiated the investigation. The Department can neither confirm nor deny the existence of an investigation. The record is confidential during the investigation and up until the Department files charges. If the complaint is dismissed, the record remains confidential unless the physician at issue requires otherwise. If probable cause exists and a statement of charges is issued, the entire record of the investigation becomes a public record, unless the physician qualifies and agrees to participate in a rehabilitation program approved by the Department. If at any time after the filing of a petition and during the 18-month period, it is determined that no probable cause exists, the petition and the entire record of the investigation is confidential.

**Section 20-204a of the Statutes.** Investigations and complaints about licensed veterinarians are confidential and not subject to disclosure to a third party under § 1-210 of the Statutes. If the Department, after such investigation makes a finding of no probable cause, or fails to make a finding within 12 months, the record of the investigations remains confidential unless the veterinary at issue requests that it be disclosed. If the Department makes a finding of probable cause and takes the steps described in § 20-202 of the Statutes to take disciplinary actions against the licensee, the record becomes a public records.

**Section 52-146f(6) of the Statutes** permits the disclosure of privileged communication between psychologist/psychiatrist-patient to the Department when it is conducting an investigation or inspection pursuant to § 19-498 of the Statutes.

## **25. Planning**

### **A. Authority to collect health information:**

**Section 19a-7(a) of the Statutes.** DPH is charged with planning and assisting communities with health priorities, policy, recommendations, quantitative goals, and the evaluation of deliverables. Thus, the Department can access patient and hospital discharge data.

### **B. Confidentiality & disclosure of information:**

**Section 19a-7-2 of the Regulations.** The Department may, at the discretion of the Commissioner, disclose aggregate data/reports for public health planning, and may disclose confidential data only for quality assurance to another state agency, and/or the federal government upon written application solely for public health planning, and upon a written agreement to return or destroy the data after a specific date or event.

## **26. Traumatic brain injury patient registry**

### **A. Authority to collect health information:**

**Section 19a-6e of the Statutes** governs collection of data from patient suffering from traumatic brain injury. Data is not subject to FOIA pursuant to § 1-200 of the Statutes.

### **B. Confidentiality & disclosure of information:**

**C.G.S. § 19a-6e.** Traumatic brain injury registry data maintained by the Department is confidential, not subject to § 1-210 of the Statutes, and can only be released pursuant to § 19a-25 of the Statutes.

Pursuant to **C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical

information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC §1 9a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC § 19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the

enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **27. Tumor Registry**

### **A. Authority to collect health information:**

**Section 19a-74 of the Statutes.** The Department is authorized to conduct investigations about cancer, including, prevention, treatment, and mortality, and can take any actions it deems necessary to decrease mortality.

**Sections 19a-2a-10, 19a-73-1 through 73-7 of the Regulations.** Short term and long term hospital records of all cancer patients must include occupational history. Hospitals and laboratories must report tumor information as the department requires concerning diagnosis, stage of disease, medical history, laboratory data, tissue diagnosis, radiation, surgical or other methods of treatment, and annual lifetime follow-up on each cancer patient at such times as are necessary to maintain the Connecticut Tumor Registry.

**Section 19a-2a-10 of the Regulations.** Data collected includes: race, ethnicity, sex, place of birth, social and medical risk factors, and health outcomes. The data is used by the Department’s Occupational Health Division and the Environmental Epidemiology Division, authorized researchers, the National Cancer Institute for community based health planning, program development, statistical research, and program compliance.

### **B. Confidentiality & disclosure of information:**

Pursuant to C.G.S. § 19a-25, all information, records of interviews, written reports, and statements, including data concerning a person’s medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC §19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC §19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

## **28. Vital Records: Birth, death, fetal death, and marriage records**

### **A. Authority to collect health information:**

**Sections 7-47, 7-47b, 7-48, 7-60, and 19a-40 through 19a-44 of the Statutes** authorize the compilation & amendments of vital records, including birth death, fetal death and marriage data routinely obtained from hospitals, funeral directors, and town clerks. Data collected includes name, hospital name, medical record and social security number, name of mother and father, date of birth, date of death, address, race, sex, ethnicity, marital status, religion, and social and medical risk factors. Data is used for state agencies, federal government, researchers, community-based planning, statistical research about health status, and population estimates by the US Census Bureau and Department.

**Section 7-42 of the Statutes** authorizes the Department to maintain and amend records of birth, death, marriage, and fetal death.

**Section 7-47 of the Statutes. Indexes.** Each registrar of vital statistics shall be kept alphabetically arranged in separate indexes for each group of vital events and shall include the name of each person whose birth, marriage, death or fetal death is recorded by the registrar.

**Section 7-48 of the Statutes. Birth Certificates: Filing requirements.** Each birth certificate must contain the information prescribed by the Department, and must be completed in its entirety. Medical information required by the Department and other information such as voluntary acknowledgments of paternity and whether the child was born out of wedlock must be recorded in the confidential portion of the certificate, and sent directly to the Department.

**Section 19a-40 of the Statutes** delegates to the Department the general supervision of the vital record registration, including records of marriage, death, birth, and fetal death.

**Section 19a-42 of the Statutes. Amendment of vital records.** Only the Commissioner may amend birth certificates to reflect changes in parent, age, or gender. The Commissioner and the registrar of vital records shall maintain sufficient documentation to support the amendments. The original certificate in the case of parentage or gender change, or in the case of a death certificate that has been amended due to a change in the cause or manner of death, shall be kept confidential.

**Section 19a-44 of the Statutes.** Vital records are mandated to match birth and death certificates and to post the facts of death to the appropriate birth certificate.

**Section 19a-45 of the Statutes** authorizes the transmittal of vital records to other states and the US Department of Health and Human Services, when it relates to residents of other jurisdictions.

**Section 7-53 of the Statutes. Birth certificates of adopted persons born in this state.** Upon receipt of adoptive records pursuant to § 45a-745(e) of the Statutes, the Department shall prepare a new birth certificate in which the adoptive parents' names are listed on the birth certificate in place of the names of the biological parents. However, no new birth certificate should be prepared if the court decreeing the adoption, the adoptive parents or the adopted person, if over fourteen years of age, so requests.

**Section 7-54 of the Statutes. Certification of birth registration or certificate of foreign birth for person born outside of the country and adopted by a state resident.** The Department is required to prepare a certificate of foreign birth of a person born outside the country and who has been adopted by a person who is a resident of this state, if the Probate court provides a specific written request to the Department with (1) an authenticated copy of the order of adoption of the court in which the adoption proceedings took place, or (2) any other evidence the probate court considers sufficient. The foreign birth certificate shall contain the adopted person's name, sex, date of birth, place of birth, the legal name of adopting parent(s), date of preparation of such certificate, and the probate court for the district in which the adoptive proceedings occurred.

**Section 19a-2a-8 of the Regulations** provides the legal authority for creation of the vital records data system.

**Section 7-59 of the Statutes. Report of foundling.** The executive authority of an agency accepting the temporary custody of any foundling child, or a member of an emergency room nursing staff who has been authorized to take custody of an infant under section 17a-58 of the statutes, shall, within 10 days of such event, provide the registrar of vital records of the town or city where the child was found, a report of foundling, in a form prescribed by the Department. The report of foundling shall include the following information: date and place of finding, sex, race, approximate age, name and address of the agency or institution, and the name given to the child. If the child is later identified and the birth certificate is later obtained, the previous report of foundling shall be substituted with the original birth certificate, and the foundling report shall be sealed and filed as confidential.

**Section 7-60(a) of the Statutes. Fetal Death.** A fetus delivered after a gestational period of 20 weeks or more, in which there is no attempt at respiration, no action of heart and no movement of voluntary muscle, must have a fetal death certificate signed by the physician or nurse midwife in attendance at the birth, or a medical examiner as required by §§ 7-48, 7-51, and 7-52 of the Statutes.

**Section 7-61 of the Statutes. Birth and fetal death certificates to state whether blood test has been made.** Birth and fetal death certificates shall indicate whether the mother who bore the child was tested for syphilis, the date of the blood test, and whether the mother was not tested. The birth certificate must not contain the test result.

**B. Confidentiality & disclosure of information:**

Pursuant to C.G.S. § 19a-25, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant

to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; (2) the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality..., [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or

supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” § 19a-25-3(c).

**PHC § 19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the

enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

**Section 7-48 of the Statutes.** The Department has discretion to release the confidential part of the certificates of birth records for statistical and health purposes to the Department, or local health director of the town where the birth occurred or where the mother resided at the time of the birth.

**Section 7-50(b) of the Statutes.** The Department must restrict access to and issuance of certified copies of acknowledgments of paternity as provided in §19a-42.

**Section 7-51 of the Statutes.** Access to and examination and issuance of certified copies of birth and fetal death certificates is subject to three levels of confidentiality.

**Section 7-51(a) of the Statutes.** Birth and fetal death records that are less than one hundred years old are confidential and may only be released to the person whose birth is recorded, if over eighteen years of age, or an emancipated minor or certified homeless youth; the person’s children, grandchildren, spouse, parent, guardian or grandparent; the chief executive officer of the municipality where the birth or fetal death occurred, or the chief executive officer’s authorized agent; the LH director for the town or the city where the birth or fetal death occurred or where the mother was a resident at the time of the birth or fetal death; members of genealogical societies incorporated or authorized by the Secretary of the State to do business or conduct affairs in this state; researchers approved by the department pursuant to § 19a-25 of the Statutes, or agents of a state or federal agency as approved by the Department.

**Section 7-51(a) of the Statutes** also prohibits access to confidential files on paternity, adoption, gender change or gestational agreements, or information contained within such files, including the eligible parties listed in subsection *a* above, except with a court order, and to the persons listed in § 19a-42a of the Statutes concerning amendments related to paternity or an original birth certificate in accordance with § 7-53.

**Section 7-51(b) of the Statutes.** The Social Security number of the parent or parents listed on any birth certificate shall not be released to any party, except to those persons or entities authorized by state or federal law. This information, other than the excluded information set forth in this subsection, shall not be subject to subpoena or court order and shall not be admissible before any court or other tribunal.

**Section 7-51(b) of the Statutes** prohibits the release of “information for health and statistical use only” or the “administrative purposes” section of the birth certificate unless specifically authorized by the Department for statistical or research purposes only.

**Section 7-51(c) of the Statutes** permits the issuance of a certified copy of a birth or fetal death certificate to the persons mentioned in subsection (a) above.

**Section 7-51(b) of the Statutes** prohibits the release of “information for health and statistical use only” or the “administration purpose only” section of the birth certificate unless specifically authorized by the Department for statistical or research purposes only.

**Section 19a-41-2 of the Regulations.** Anyone authorized to inspect or receive copies of birth certificates pursuant to § 7-51 of the Statutes must provide a photographic identification proving that such person is entitled to access the birth certificate. If a photographic identification is not available then the person must submit substitute documentation as prescribed by this regulation.

**Section 7-51 of the Statutes.** The Department may issue **certified copies of death and marriage certificates, and certified copies of birth and fetal death certificates that are more than one hundred years old**, to anyone who is at least 18 years old. The Department may only issue **uncertified copies of birth, death, marriages, and fetal death certificates** to researchers approved pursuant to § 19a-25 of the Statutes, and to state and federal agencies approved by the Department.

Genealogists incorporated or authorized by the Secretary of the State have full access to all vital records, and can purchase certified copies of such records and derive statistics from such records for use in publications of genealogical societies, except for the part of the record containing the social security number, and confidential files on adoptions, gender change, gestational agreements and paternity.

**Section 7-51a(b) of the Statutes.** **Marriage and civil union certificates** must include the social security number of the parties in the “administrative purposes” section of the marriage or civil union certificate. All parties mentioned in the certificate shall have access to the social security numbers listed on the certificate. Any other individual, researcher, or state or federal agency requesting a certified or uncertified copy of a marriage or civil union certificate pursuant to this section must receive such copy with the social security redacted or with the “administrative purposes” section omitted.

**Section 7-51a(c) of the Statutes.** **Death certificates for deaths occurring after December 31, 2001.** The following information will be placed in the “administrative purposes” section of the death certificate: social security number, occupation of the deceased person, business or industry, race, Hispanic origin if applicable, and educational level of the deceased, if known. All the administrative information shall be available to all parties specified on the certificate, including the informant, licensed funeral director and/or embalmer, conservator, surviving spouse, physician and town clerk for the purpose of processing the certificate.

**For deaths occurring after July 1, 1997**, the social security number and information contained in the “administrative purposes” section of the death certificate is only available to the surviving spouse, funeral director, next of kin, or state or federal agencies authorized by law. Any approved researcher requesting death certificates occurring after July 1, 1997, may obtain the

information contained in the “administrative purposes” section, except for the decedent’s social security number.

**Section 7-51a(d) of the Statutes.** The local registrars of vital statistics may have access to electronic vital records in order to issue certified copies of birth, death, fetal death or marriage certificates that are electronically filed in the system.

**Section 7-53 of the Statutes. Birth Certificates of adopted persons born in this state.** For adoptions taking place on or after October 1, 1983, an uncertified copy of an original birth certificate shall be issued upon request of the adopted person, if at least eighteen years old, or such adopted person’s adult child or grandchild. Any other person seeking to examine or obtain a copy of the original record or certificate of birth of an adopted person must first obtain a written order from the judge where the adoption took place, or a written order of the Probate Court in accordance with § 45a-752 of the Statutes. If authorized by the Probate court, the Department will issue a certified copy of the original birth certificate marked with a notation that the birth certificate has been superseded by a new birth certificate.

**Section 7-54 of the Statutes.** Once the Department prepares a certificate of foreign birth, it can subsequently issue copies of certificates in accordance with § 7-52 of the Statutes (the Department can provide certificates to the person to whom it relates, if the person is over the age of 16, or to the parent, guardian, spouse, child (if older than 18 years of age), grandparent or legal representative).

**Section 7-59 of the Statutes. Report of foundling children.** Except for an infant voluntarily surrendered under the provisions of 17a-58, if a child for whom a report of foundling has been registered is later identified and a certificate of birth is obtained, the certificate of birth shall be substituted and the report of foundling shall be sealed and filed at the Department. The sealed foundling report can only be released upon order of a court of competent jurisdiction.

**Section 7-60(b) of the Statutes. Fetal death certificates** contain a confidential portion with additional information obtained by the Department, which must only be used for medical or health purposes.

**Section 19a-41-2 of the Regulations.** The Department only provides access to birth records to authorized individuals.

**Section 19a-41-4 of the Regulations** authorizes the electronic transmittal of birth records to the Department.

**Section 19-13-D54(b) of the Regulations** requires that in the case of induced abortions, a death certificate will be issued for fetuses born dead resulting from a gestational period not less than twenty weeks, and a live birth certificate for each fetus born alive regardless of gestational age as provided by §§ 7-48 and 7-60 of the Statutes. If a live born fetus subsequently dies, a death certificate will be issued pursuant to § 7-62b of the Statutes.

**Section 19-13-D14(e) of the Regulations.** For each woman admitted into a hospital maternity ward, a complete record of each case shall be kept that includes information required by the Department and all items necessary to fill out a death certificate for the mother and all items necessary to fill out a birth or death certificate for the infant.

## **29. WIC**

### **A. Authority to collect health information:**

**Section 19a-59c of the Statutes and § 19a-2a-18 of the Regulations. Statewide WIC Information System.**

The Department is authorized to administer the WIC program, and create a database of Connecticut residents enrolled in WIC. Participants' information is maintained for documentation of certification of eligibility as well as to enable the issuance of WIC checks, accountability, and program evaluation.

**Section 19a-2a-18(c)(2) of the Regulations.** The collection, maintenance, retention, and use of personal health information and WIC data is authorized by the § 11-8a of the Statutes.

### **B. Confidentiality & disclosure of information:**

Pursuant to **C.G.S. § 19a-25**, all information, records of interviews, written reports, and statements, including data concerning a person's medical or emotional condition or history, procured by the Department in connection with studies or morbidity and mortality, or pursuant to statutory reporting requirements are confidential and may be used solely for the purposes of medical or scientific research or for disease prevention and control. Confidential medical information may not be disclosed except as may be necessary for the purpose of furthering the research project to which it relates. The Department may exchange personal data with other governmental agencies or private research organizations for the purpose of medical research provided that the data recipient does not further disclose the data.

**PHC § 19a-25-1. Disclosure of health data.** Definitions used in 19a-25-1 through 19a-25-4, inclusive.

**PHC § 19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality.** The Department may publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and

reports (1) are prepared for the purpose of medical and scientific research; and (2) do not include identifiable health data.

**PHC § 19a-25-3. Disclosure of identifiable health data.** The Department may not disclose identifiable health data unless: (1) “the disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to [C.G.S.] § 19a-215; the disclosure is to healthcare providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control... or [to] reduc[e] morbidity and mortality...; [and] every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose; and (3) the disclosure is to an individual, organization, government entity in this or another state or to the federal government... [if necessary] for [ ] medical or scientific research.”

“No identifiable health data obtained in the course of activities undertaken or supported under this section shall be subject to subpoena or seminal compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.” §19a-25-3(c).

**PHC § 19a-25-4. Use of health data for enforcement purposes.** Allows the Department to “utilize, in any manner, health data including... aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law[, or disclosure is made to an] administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.”

**7 CFR Section 246.26(d)** of the Federal WIC Regulations prohibits the disclosure of the identity of WIC applicants, participants and vendors identifying information to third parties, but allows the records to be audited.

## Appendix D Information Security Policy

- A. In developing its Information Security Policy, the Department is taking appropriate steps to ensure its information system is properly protected from all security threats, regardless of storage or transmission medium.

All users of the electronic system housed at the Department carry the responsibility of maintaining the security, confidentiality, integrity, and availability of information stored at the Department. Violation of the Department's Information Security Policy may result in disciplinary action.

Please access the Department's Information Security Policy at:

[http://www.ct.gov/insidedph/lib/insidedph/informationtechnology/policies/information\\_security\\_policy.pdf](http://www.ct.gov/insidedph/lib/insidedph/informationtechnology/policies/information_security_policy.pdf)

### B. Protection of data in mobile computing and storage devices

1. General requirements: In addition to complying with state and federal confidentiality laws, the maintenance and sharing of all personal health information must also comply with state policies on security of data, including security for mobile computing and storage devices.
2. The Department of Administrative Services Bureau of Enterprise Systems and Technology ("BEST") has established a policy on the secure implementation and deployment of mobile computing and storage devices within state government for the protection of state data. This policy covers all state Executive Branch agencies and employees, permanent and non-permanent, full-time and part-time, and all consultants and contracted individuals having access to state data.

### C. Mobile devices and removable media.

1. Mobile devices and removable media: Mobile devices include any non-fixed equipments that contain an operating system, which may be used to create, access or store data. Such devices include but are not limited to laptops, personal digital assistants (PDAs), and smart phones. Removable media include CDs, DVDs, MP3 players, removable memory, and USB drives (thumb drives).
2. General Rule: No confidential or restricted state data shall reside on any mobile devices or removable media unless:
  - the agency authorizes it;
  - it is necessary;
  - only the minimum data necessary is utilized;

- the data is only stored for the time needed;
- the data is encrypted and physically protected (screen savers);
- the data is stored on secure devices/media in accordance with Best Policies Standard and Guidelines;
- approved encryption standards are employed (must be FIPS-140 compliant and include Advanced Encryption Algorithm (AES) that uses a 128, 192, or 256-bit key size);
- if the data is lost or stolen, such loss is reported to the Department's contact person within 24-hours or on the first business day after discovering the loss;
- a Department approved virtual processing network ("VPN") is utilized;
- when using non-state assigned PC, such PC supports the VPN; and
- used on password protected and encrypted home-based computers.

**Connecticut Department of Public Health**  
**CONFIDENTIALITY PLEDGE**

I recognize the importance of maintaining the confidentiality of personal and personal health information collected by the Connecticut Department of Public Health (DPH), and of assuring the right to privacy of persons, physicians, healthcare providers, facilities, clients of facilities, and agencies, which cooperate with programs within DPH, are regulated by DPH, or participate in DPH's information collection efforts.

I also understand that DPH is legally obligated to protect the privacy of personal health information. I have been provided Connecticut General Statutes §19a-25 and §§19a-7-1, 19a-7-2, 19a-25-1 through 19a-25-4, and 19a-36-A5 of the Regulations of Connecticut State Agencies, which address confidentiality of records, and have been advised that DPH can take necessary action if a breach of confidentiality occurs.

Therefore, I pledge that I will NOT access or accept the identifying or personal information of patients, physicians, healthcare providers, facilities, clients of facilities, or agencies, except as needed for the proper discharge of my duties.

I also pledge that I will NOT, unless permitted by law and/or required by law, divulge such confidential information except to another DPH employee or associate of DPH who is approved for access to the information and has either signed a DPH confidentiality pledge or executed a contract or Memorandum of Agreement authorizing such disclosure.

I understand that my adherence to this pledge applies during and after my employment at the Department of Public Health.

I agree to protect all confidential information during its collection, use, storage, and destruction. My disclosure or acquisition of confidential information will be what is minimally necessary for the proper discharge of my duties (including reporting duties imposed by legislation) and based on a programmatic need to know. I further understand that if I violate this pledge I will be subject to disciplinary action, up to and including dismissal.

Date: \_\_\_\_\_

**Individual Pledging to Maintain Confidentiality**

Name \_\_\_\_\_  
(Print)

Title \_\_\_\_\_

Address \_\_\_\_\_

\_\_\_\_\_

**SIGNATURE:**

\_\_\_\_\_  
**Individual Pledging to Maintain Confidentiality**

DEPARTMENT OF ADMINISTRATIVE SERVICES  
BUREAU OF ENTERPRISE SYSTEMS AND TECHNOLOGY  
VMS Interview/Selection

The following is a list of hyperlinks that direct you to information about technology and Internet related policies and guidelines.

- [Acceptable Use Policy](#)
- [Data Classification](#)
- [Disposal of Digital Media Policy](#)
- [Domain Name Registration and Usage](#)
- [Electronic & Voice Mail Management and Retention Guide](#)
- [Electronic Mail Records Management Policy](#)
- [HIPAA Security Policy](#)
- [Implementation/Deployment of State Agency Internet Sites and Extranet Sites](#)
- [Management of State Information Technology Projects](#)
- [Network Security and Procedures](#)
- [Open Data Policy](#)
- [Personal Wireless Device Policy](#)
- [Security for Mobile Computing and Storage Devices](#)
- [Social Media Policy](#)
- [Software Management Policy](#)
- [State Property Control](#)
- [Telecommunications Equipment](#)
- [State of Connecticut Information and Telecommunications Strategic Plan](#)
- [Universal Website Accessibility Policy](#)
- [Use of Relational Data Base Systems](#)
- [Violence in the Workplace](#)
- State Contractors Code of Ethics  
[http://www.ct.gov/ethics/lib/ethics/guides/2016/contractors\\_guide\\_to\\_the\\_code\\_of\\_ethics\\_revjan2016b.pdf](http://www.ct.gov/ethics/lib/ethics/guides/2016/contractors_guide_to_the_code_of_ethics_revjan2016b.pdf)

This is to certify to the best of my knowledge and belief, I have no financial interest, ownership interest, employee interest, personal interest or seeking employment with any of the products/services I may recommend. If at any time prior or during the project a conflict of interest arises, I affirm that I will report the conflict immediately to the State Project Lead. I will comply with all of the above workplace and technology policies during the time I am performing consulting services for the State of Connecticut.

---

Signature of Consultant

---

Certified By Agency

---

Date

### **Supervisory Notification of Field Activities**

DIS (disease intervention specialists) are expected to maintain communication with immediate supervisor while conducting field activities. DIS are expected to exercise good judgement in effective use of time offsite. The following are procedural guidelines for notification of field activities.

- Upon leaving the office, if supervisor is available, DIS are required to notify supervisor of number of field visits being conducted, cities being visited, and if they will be returning to the office.
- If the supervisor is not available the DIS is responsible to communicate field activities by text to immediate supervisor. The same information should be provided as required for verbal notification. Number of field visits, cities being visited, and if they are returning to the office or returning car back to the lot.
- During field activities if there is a change in field destination, the DIS should call the supervisor and inform them of the change.
- If the DIS is scheduling lunch break while conducting field activities, this information also needs to be communicated to the supervisor.
- Upon returning from the field if supervisor is not available notify supervisor by text that you have returned from the field.
- Cell phone should be charged at all times- this is the only device that DIS have to communicate if there is an emergency. The cell phone will be used to address any problem that may occur in the field that may require immediate attention.
- DIS should document all cities visited on the mileage report at the conclusion of the day of field activity.
- DIS should document all field visits and their outcome on the field record including the time of visit on the day that the field visit is conducted.

These guidelines are to ensure safety in the field environment in addition to accountability in the field. Quarterly audits will be completed by supervisor and reviewed with DIS. Any discrepancies will be documented and if patterns concerning questionable time documentation continue, disciplinary action may result. Any questions or suggestions on these procedures should be discussed with supervisor.



## TB, HIV, STD & Viral Hepatitis Section

### Periodic Assessment Checklist - 2018

This checklist can be used to guide the periodic assessment of a program's compliance with the Standards for Data Security and Confidentiality.

**For the answer to be "yes" to a question with multiple parts, all boxes must be checked. For each "No" response, provide additional information describing how the program intends to achieve compliance with that standard.**

Name of Program being assessed

Name of person assessing the program

CT DPH TB, HIV, STD & Viral Hepatitis Programs

Heather Linardos

## 1.0 PROGRAM POLICIES AND RESPONSIBILITIES

### STANDARD 1.1

In your program, how are staff members who are authorized to access HIV/VH/STD/TB information or data made aware of their data confidentiality and security responsibilities?

46

*Are the following points addressed in your policies and agreements?*

- |   |                             |  |
|---|-----------------------------|--|
| <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No | Are staff provided training on security policies and procedures and where to find resources?                               |
| <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No | Does the program have written data security and confidentiality policies and procedures?                                   |
| <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No | Are written policies and procedures reviewed at least annually and revised as needed?                                      |
| <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No | Are data security policies readily accessible to all staff members who have access to confidential, individual-level data? |
|   |                             | Where are the policies located? <u>Policy is emailed to staff annually</u>   |

## STANDARD 1.2

☒ Yes ☐ No

In your program, is there a policy that assigns responsibilities and designates an ORP for the security of the data that is stored in various data systems?

☒ Yes ☐ No

Does the ORP have sufficient authority to make modifications to policies and procedures and ensure that the standards are met?

## STANDARD 1.3

☒ Yes ☐ No

Does your program have a policy that defines the roles and access level for all persons with authorized access?

☒ Yes ☐ No

Does your program have a policy that describes which standard procedures or methods will be used when accessing HIV/VH/STD/TB information or other personally identifiable data?

## STANDARD 1.4

☐ Yes ☒ No  
**Ongoing**

Does the program have a written policy that describes the methods for ongoing review of technological aspects of security practices to ensure that data remain secure in light of evolving technologies?

## STANDARD 1.5

☒ Yes ☐ No

Are written procedures in place to respond to breaches in procedures and breaches in confidentiality?

Where are those procedures stored? Section Data Security & Conf. Policy, DPH website

☒ Yes ☐ No

Is the chain of communication and notification of appropriate individuals outlined in the data policy?

☒ Yes ☐ No

Are all breaches of protocol or procedures, regardless of whether personal information was released, investigated immediately to determine causes and implement remedies?

☒ Yes ☐ No

Are all breaches of confidentiality (i.e., a security infraction that results in the release of private information with or without harm to one or more persons) reported immediately to the ORP?

☒ Yes ☐ No

Do procedures include a mechanism for consulting with appropriate legal counsel to determine whether a breach warrants a report to law enforcement agencies?

☒ Yes ☐ No

If warranted, are law enforcement agencies contacted when a breach occurs?

### STANDARD 1.6

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Are staff trained on the program's definitions of breaches in procedures and breaches in confidentiality?  |
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?   |
| <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | Are staff trained on policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold?     |
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?  |
| <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | Is every staff member, information technology (IT) staff member, and contractor who may need access to individual-level information or data required to attend security training annually? |
| <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No | Is the date of the training or test documented in the employee's personnel file?   |

### STANDARD 1.7

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Do all authorized staff members in your program sign a confidentiality agreement annually?   |
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Do all newly hired staff members sign a confidentiality agreement before they are given authorization to access individual-level information and data? |

### STANDARD 1.8

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Do policies state that staff are personally responsible for protecting their own computer workstation, laptop computer, or other devices associated with confidential public health information or data? |
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Are staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?   |

### STANDARD 1.9

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No | Does your program certify annually that all program standards are met? |
|---|--|

## 2.0 DATA COLLECTION AND USE

### STANDARD 2.1

☒ Yes ☐ No

When public health data are shared or used, are the intended public health purposes and limits of how the data will be used adequately described?

### STANDARD 2.2

☒ Yes ☐ No

When data are collected or shared, do they contain only the minimum information necessary to achieve the stated public health purpose?

### STANDARD 2.3

☐ Yes ☒ No

Does your program explore alternatives to using identifiable data before sharing data, such as using anonymized or coded data?

What alternatives are currently in use in your program? Typically PII/PHI is  
not shared with unauthorized parties

### STANDARD 2.4

☒ Yes ☐ No

Does your program have procedures in place to determine whether a proposed use of identifiable public health data constitutes research requiring IRB review?

## 3.0 DATA SHARING AND RELEASE

### STANDARD 3.1

☒ Yes ☐ No

In your program, is access to HIV/VH/STD/TB information and data for any purposes unrelated to public health (e.g., litigation, discovery, or court order) only granted to the extent required by law?

What non-public health use of the data are required or allowed by law?

### STANDARD 3.2

When a proposed sharing of identifiable data is not covered by existing policies, does your program assess risks and benefits before making a decision to share data?

☒ Yes ☐ No

How are these risks assessed? ORP, DSM and program staff would likely meet to discuss but PII/PHI are not shared with unauthorized parties

### STANDARD 3.3

When sharing personally identifiable HIV/VH/STD/TB information and/or data with other public health programs (i.e., those programs outside the primary program responsible for collecting and storing the data), is access to this information and/or data limited to those for whom the ORP:

☒ Yes ☐ No

☒ has weighed the benefits and risks of allowing access; and

☒ can verify that the level of security established is equivalent to these standards?

### STANDARD 3.4

Is access to confidential HIV/VH/STD/TB information and data by personnel outside the HIV/VH/STD/TB programs:

☐ Yes ☐ No

☐ limited to those authorized based on an expressed and justifiable public health need?; and

☐ arranged in a manner that does not compromise or impede public health activities?; and

**N/A: Access is not permitted**

☐ carefully managed so as to not affect the public perception of confidentiality of the public health data collection activity and approved by the ORP?

Before allowing access to any HIV/VH/STD/TB data or information containing names for research or other purposes (e.g., for other than routine prevention program purposes), does your program require that the requester:

☒ Yes ☐ No

☒ demonstrate need for the names?; and

☒ obtain institutional review board (IRB) approval (if it has been determined to be necessary)?; and

☒ sign a confidentiality agreement?

### STANDARD 3.5

---

☒ Yes ☐ No

Does your program have written procedures to review data releases that are not covered under the standing data release policy?

If not, does your program have unwritten policy to review data releases that are not covered under the standing data release policy?

☒ Yes ☐ No

Describe briefly those procedures or policies: \_\_\_\_\_

\_\_\_\_\_

---

### STANDARD 3.6

---

☒ Yes ☐ No

Does your program routinely distribute nonidentifiable summary data to stakeholders?

---

### STANDARD 3.7

---

☒ Yes ☐ No

Does your program assess data for quality before disseminated?

---

### STANDARD 3.8

---

☒ Yes ☐ No

Does the program have a data-release policy that defines access to, and use of, individual-level information?

☒ Yes ☐ No

Does the data-release policy incorporate provisions to protect against public access to raw data or data tables that include small denominator populations that could be indirectly identifying information?

---

## 4.0 PHYSICAL SECURITY

### STANDARD 4.1

Are workspaces and paper copies for persons working with confidential, individual-level information located within a secure, locked area?

☒ Yes ☐ No

☒ Are sensitive documents stored in cabinets?

☒ Are the cabinets locked?

☒ Are cabinets located in an area to which there is no access by unauthorized employees?

☒ Are cabinets located in an area to which there is no public access?

### STANDARD 4.2

☒ Yes ☐ No

Do program staff members shred documents containing confidential information with a cross-cutting shredder before disposing of them?

### STANDARD 4.3

☒ Yes ☐ No

Does your program have a written policy that outlines procedures for handling paper documents which could contain confidential information that are mailed to, or from, the program?

☒ Yes ☐ No

Do staff members in your program ensure that the amount and sensitivity of information contained in any piece of correspondence remains minimal?

### STANDARD 4.4

☒ Yes ☐ No

Is access to all secured areas where confidential, individual-level HIV/VH/STD/TB information and data are stored limited to persons who are authorized within policies and procedures (this includes access by cleaning or maintenance staff)?

#### STANDARD 4.5

☒ Yes ☐ No

Do policies include procedures for securing documents containing PII when they cannot be returned to a secure work site by the close of business?

☒ Yes ☐ No

Do policies outline specific reasons, permissions and physical security procedures for using, transporting and protecting documents containing PII in a vehicle or personal residence?

☐ Yes ☐ No

If no such procedure exists, is approval obtained from the program manager?

#### STANDARD 4.6

When identifying information is taken from secured areas and included in on-line lists or supporting notes, in either electronic or hard-copy format:

☒ Yes ☐ No

☒ is it assured that the documents contain only the minimum amount of information necessary for completing a given task?, and

☒ is the information encrypted?, and

N/A ☐ is it coded to disguise information that could be easily associated with individuals?

☒ Yes ☐ No

Do staff members in your program ensure that terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of data transmissions, including sender and recipient addresses and labels?

### 5.0 ELECTRONIC DATA SECURITY

#### STANDARD 5.1

☒ Yes ☐ No

In your program, are HIV/VH/STD/TB analysis data sets stored securely using protective software (i.e., software that controls the storage, removal, and use of the data)?

☒ Yes ☐ No

Are personal identifiers removed from HIV/VH/STD/TB analysis data sets whenever possible?

## STANDARD 5.2

In your program, do transfers of HIV/VH/STD/TB data and information and methods for data collection:

☒ Yes ☐ No

☒ have the approval of the ORP?, and

☒ incorporate the use of access controls?, and

☒ encrypt individual-level information and data before electronic transfer?

☐ Yes ☒ No

When possible, are databases and files with individual-level data encrypted when not in use?

## STANDARD 5.3

☒ Yes ☐ No

Does your program have a policy that outlines procedures for handling electronic information and data (including, but not limited to, e-mail and fax transmissions) which may contain confidential information that are sent electronically to or from the program?

☒ Yes ☐ No

When individual-level HIV/VH/STD/TB information or data are electronically transmitted and the transmission does not incorporate the use of an encryption package meeting the encryption standards of the National Institute of Standards and Technology and approved by the ORP, are the following conditions met?

☒ The transmission does not contain identifying information.

☒ Terms easily associated with HIV/VH/STD/TB do not appear anywhere in the context of the transmission, including the sender and recipient address and label.

#### STANDARD 5.4

For all laptop computers and other portable devices (e.g., personal digital assistants [PDAs], other handheld devices, and tablet personal computers [tablet PCs]), which receive or store HIV/VH/STD/TB information or data with personal identifiers, are all the following steps taken to ensure the security of the data?

- ☒ Yes ☐ No
- ☒ The devices have encryption software that meets federal standards.
  - ☒ Program information with identifiers is encrypted and stored on an external storage device or on the laptop's removable hard drive.
  - ☒ External storage devices or hard drives containing the information are separated from the laptop and held securely when not in use.
  - ☒ The decryption key is kept some place other than on the device.

- ☒ Yes ☐ No
- Do the methods employed for sanitizing a storage device ensure that the information cannot be retrieved using "undelete" or other data retrieval software?

Does the program have policies or procedures to ensure that all removable or external storage devices containing HIV/VH/STD/TB information or data that contain personal identifiers:

- ☒ Yes ☐ No
- ☒ include only the minimum amount of information necessary to accomplish assigned tasks as determined by the program manager, and
  - ☒ are encrypted or stored under lock and key when not in use, and
  - ☒ are sanitized immediately after a given task (excludes devices used for backups)?

Where are these policies or procedures stored? HIV Surveillance secure drive

- ☒ Yes ☐ No
- Are hard drives that contain identifying information sanitized or destroyed before the computers are labeled as excess or surplus, reassigned to nonprogram staff members, or sent off site for repair?

#### STANDARD 5.5

- ☒ Yes ☐ No
- Does your program have policies for handling incoming and outgoing facsimile transmissions to minimize risk of inadvertent disclosure of PII?

**DATA SECURITY AND CONFIDENTIALITY  
CDC SITE VISIT CHECKLIST**

|  |   |
|--|---|
| <b>Recipient Name:</b>                       | Connecticut Department of Public Health |
| <b>Recipient Award Number:</b>               | PS18-1802                               |
| <b>Site Visit Dates:</b>                     | September 10-12 , 2018                  |
| <b>HICSB PHA (Program Consultant):</b>       | Yolanda I. Gonzalez-Alvarez             |
| <b>HICSB Surveillance Project Officer:</b>   | Angela Hernandez                        |
| <b>PPB Prevention Project Officer:</b>       | Carla Alexander-Pender                  |
| <b>Recipient Overall Responsible Party:</b>  | Heidi Jenkins                           |
| <b>Point of Contact for form completion:</b> | Heather Linardos                        |

**POLICY AND RESPONSIBILITY**

|   |  |   |
|---|--|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 1. Does your program have an Overall Responsible Party (ORP)?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 2. Does the ORP have authority to approve, modify, and enforce S&C policy and procedural standards, modifications?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Are written security policy and procedures consistent with the CDC 2011 guidelines?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. Are written policies and procedures reviewed annually, at minimum, and revised when needed?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 5. Does your program define the roles and access level for all persons with authorized access?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Are data security policies accessible to all staff and others with access to confidential, individual-level data?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 7. Is this an integrated program? (e.g. HIV S/P integrated with TB, STD, VH or another program(s)?)   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 8. Are all staff (and others) with access to PII trained annually on the S&C policy and do they sign the S&C agreement?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 9. Does staff training include how to protect keys, use passwords, and codes that would allow access to confidential information or data?   |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 10. Does staff training include policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold? |

|   |                             |  |
|---|-----------------------------|--|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 11. Do policies outline procedures for using, transporting and protecting documents containing PII in a vehicle or residence?                      |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 12. Have all persons authorized to access individual-level information trained on the organization's information security policies and procedures? |

#### **Additional Comments or Recommendations:**

The Policy is revised annually

---



---



---

#### **RECORDS RETENTION POLICY**

|   |                             |   |
|---|-----------------------------|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 1. Does the program have written policies for records retention, also for the disposal of paper copies?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 2. Are the policies flexible enough to address shredding of hard copies of all records (e.g. the creation of electronic medical records (ELR), Lab Slips, case reports, etc?) |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 3. Is the Record Retention Policy reviewed on a periodic schedule?<br>a. If so, how often?<br>b. When was the last review (date or month/year)?                               |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 4. Are staff aware of the records retention policy?   |

#### **Additional Comments or Recommendations:**

---



---



---

#### **SECURITY BREACHES**

|   |                             |  |
|---|-----------------------------|--|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 1. Are written procedures in place to respond to breaches in procedures and breaches in data security and confidentiality?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 2. Does the policy require all breaches (and potential breaches) of protocol or procedures be investigated immediately to determine causes and implement remedies? |

|   |  |   |
|---|--|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Are all breaches of security & confidentiality reported immediately to the jurisdiction's IT security point of contact and to the specific program's Overall Responsible Party?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. Are all breaches that result in the release of PII required to be reported immediately to the CDC? (inform must be reported within 1 hour after initial reporting within the jurisdiction #3 above; that means within 2 hours to CDC)  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 5. Do procedures include a mechanism for consulting with appropriate legal counsel to determine whether a breach warrants a report to law enforcement agencies?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Is staff trained on ways to protect keys, use passwords, and codes that would allow access to confidential information or data?  |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 7. Is staff trained on policies and procedures that describe how staff can protect program software from computer viruses and computer hardware from damage due to extreme heat or cold?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 8. Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?  |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 9. Is every staff member, information technology (IT) staff member, and contractor who may need access to individual-level information or data required to attend security training annually? (Have all persons authorized to access individual-level information been trained on the organization's information security policies and procedures?) |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 10. Have any breaches, potential breaches, or instances of unauthorized access been identified in the past twelve months? If yes, provide details.  |

**Additional Comments or Recommendations:**

---



---



---

## ANNUAL TRAINING

|   |  |   |
|---|--|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 1. Do all authorized staff members in your program sign a confidentiality agreement annually?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 2. Are all newly hired staff members required to complete S&C policy training and sign an S&C agreement before being given authorization to access individual-level information and data?                             |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Do all staff from TB, VH, STD, and HIV Surveillance and Programs having access to PII receive annual training, review the CDC 2011 guidelines, and are required to sign an S&C agreement form?                     |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. Are IT staff with access to servers trained annually on the S&C data security policies, review the CDC 2011 guidelines, and required to sign an S&C agreement form?  |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 5. Is the S&C annual training date and attestation signing documented in the employee's personnel file?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Does the training include a review of physical and electronic data security procedures, confidentiality procedures, and the release & sharing procedures on an ongoing basis, as well as HIV laws and regulations? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 7. Are there different training components or specific modules related to job-specific responsibilities?  |

### Additional Comments or Recommendations:

Signed Confidentiality Agreements are stored electronically in a 3rd party cloud-based application

## PHYSICAL and ELECTRONIC ENVIRONMENTS

|   |  |  |
|---|--|--|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 1. Is access to all secured areas where confidential, individual-level HIV/VH/STD/TB information and data are stored limited to persons who are authorized as described within the S&C policy? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 2. Do security policies address access to secure and file storage areas by cleaning crews and maintenance staff?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Is the level of security adequate in office areas where program data is available and processed? Describe what type of security levels, e.g. access code, keys, etc.                        |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. If keys are required to secure data, are the keys adequately secured?   |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 5. Can program data or records be viewed or accessed through windows?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Were room/office configurations assessed to limit viewing by others entering the workspace?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 7. Are privacy screens on monitors, as needed, and are the monitors turned away from view by those entering the workspace?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 8. Are there security measures in place to limit access to computers with PII?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 9. Is there an adequate process in place for handling all hard copies of lab results (includes via U.S. mail or printouts)?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 10. Is the security level adequate in the area where hard-copies of case reports/lab results are stored?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 11. Are crosscutting shredders present in the secure area?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 12. Is the fax machine in a secure location?   |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 13. Can phone conversations on clients' disease status be overheard by staff whom have not completed S&C confidentiality requirements?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 14. Are electronic protections in place for field work, telework and remote access to data on laptops or other storage devices?  |

|   |  |  |
|---|--|--|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 15. Are there secure procedures for transporting and protecting electronic information containing PII in a vehicle or residence? |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 16. Is encryption used for data transfer through SDN, VPN or SFTP and while at rest?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 17. Do data policies prohibit e-mailing of public health data?   |

**Additional Comments or Recommendations:**

**DATA COLLECTION, USE, RELEASE, and SHARING**

|   |                             |   |
|---|-----------------------------|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 1. Is the minimum information needed to conduct specified public health activities and achieve the stated public health purpose collected/used?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 2. Are all proposed data elements justifiable in terms of their contribution toward achieving the public health goal?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 3. Is access to PII limited to the fewest number of persons necessary (i.e. "Need to Know")?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 4. Does your program have formal agreements, such as a data-sharing agreements or Memorandum of Understanding (MOU) when sharing within or outside the health department or with any other public health organizations? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 5. Is there a data release policy?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 6. Does the policy address restrictions on access to and release of surveillance and program data?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 7. Are staff aware of the data release policy?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 8. Does the policy address restrictions on access to and release of surveillance and program data?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 9. Does the policy incorporate provisions to protect against public access to raw data?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 10. Does the policy incorporate provisions to protect small denominator populations?  |

|   |                             |   |
|---|-----------------------------|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 11. Does your program routinely distribute non-identifiable summary data to stakeholders?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 12. Does your program assess data for quality before disseminated?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 13. Does your program have formal agreements, such as a data-sharing agreements or Memorandum of Understanding (MOU) when sharing within or outside the health department or with any other public health organizations?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 14. Does your program ensure that any public health program with which personally identifiable public health data are shared has data security standards equivalent to those in the CDC 2011 Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs?      |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | 15. Is data sharing of confidential or identifiable information limited to those with a justifiable public health need; ensuring that any data-sharing restrictions do not compromise or impede public health program or disease surveillance activities and that the ORP or other appropriate official has approved this access? |

**Additional Comments or Recommendations:**

---



---



---

**DATA BACKUP, DISASTER RECOVERY, and EMERGENCY MODE PLANS**

|   |  |   |
|---|--|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 1. In case of an emergency or disaster, is there a business continuity plan (known as a COOP)?  |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 2. If applicable, is the business continuity plan reviewed on a regular basis?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Do written data security & confidentiality procedures include a plan for any of the following (identify which): data backup, disaster recovery, and emergency mode in the event of a natural disaster or even a crisis (e.g. cybersecurity attack)? Meaning, do you have data back-up, disaster recovery, and continuity plans in place? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. Are information technology and security staff included in the development and review of these policies?  |

|   |  |   |
|---|--|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 5. Is the disaster recovery plan reviewed on a regular basis?<br>a. If so, how often? Annually<br>b. When was the last review (date or month/year)? 12/2017   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Does the data backup plan include any of the following capabilities or functionalities: user password authentication; role-based limited access; data encryption of electronic protected health information; offsite storage; storage facility security with necessary safeguards; and reporting verifiable status data ensuring that the proper resources can monitor and be proactive to any potential problems with the solution? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 7. Are back-ups tested to assure that they can restore eHARS?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 8. Are any back-ups stored or protected on-site or off-site?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 9. Are back-ups tested to assure that they can restore eHARS?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 10. Do you have an offsite alternative for recovery in case the building where the servers are located is destroyed?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 11. Are there physical safeguards such as limited facility and electronic access controls for an alternate site used during a disaster or emergency mode?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 12. Do policies implement technical security measures to guard against unauthorized access to electronic protected health information that transmitted over an electronic communications network?   |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 13. Are there audit controls to record and examine health information systems activities containing protected health information?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 14. Are there procedures supporting restoration of lost data?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 15. Do you perform backup of data?  |
|   |  | 16. Where are the backups stored?<br>In a secure, off-site location, updated weekly. Database backups are performed on a scheduled daily basis at the database level and then these backups are integrated into the off-site tape rotation.   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 17. Do you ever test the backups?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 18. Does policy include the handling of server hardware failure?  |

|  |  |  |
|--|--|--|
|  |  | DPH has redundant hardware installed for seamless failover and detail VM or host restoration procedures.                 |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 19. Does policy include the handling of disk drive failure?  |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 20. Does policy include data corruption issues (e.g. viruses, malware, etc.)?  |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 21. Are the rooms where any equipment and data get stored protected/locked?  |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 22. Is there fire/heat protection (heat/temperature control, (e.g. multiple air conditioners and halon protected, etc.)? |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 23. Is there snow/ice/cold protection?   |
| Yes <input checked="" type="checkbox"/>  | No <input type="checkbox"/>            | 24. Is there water/flooding protection?  |
| Yes <input type="checkbox"/>   | No <input checked="" type="checkbox"/> | 25. Is there earthquake/tornado protection?  |
| Yes <input type="checkbox"/>   | No <input checked="" type="checkbox"/> | 26. Is there protection against chemical spills?   |
| <p>27. Briefly, give an overview of your firewall and how you monitor/prevent external attacks (e.g. firewall is monitored by the state IT department; they have a security operations center that monitors reports from the firewalls).</p> <p>The external portal and primary fire wall and is secured at the State data center. All DPH HIV applications and databases are hosted in a more secured subnet in the agency data center and configured using 3 tier architecture and dedicated server instances to prevent data mixing or cross platform access.</p> |  |  |

#### **Additional Comments or Recommendations:**

All servers hosting HIV allocations are patched on a regular schedule and have McAfee virus scan configured installed on them.

#### **INFORMATION TECHNOLOGY / TECHNICAL and LOGISTICAL POLICY**

|   |                             |   |
|---|-----------------------------|---|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | <p>1. Will the CDC PHA be able to visit the server hosting area and see the eHARS servers (and any other server hosting other HIV information systems)?</p> <p>Yes, but it is a virtual environment. Viewers will be able to see the hosts but not the logical servers. Those can be viewed on the Management console for the VM environment.</p> |
|---|-----------------------------|---|

|   |  |  |
|---|--|--|
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 2. Are eHARS servers inventoried, as well as databases, all computers, hardware, and software such as SQL licenses)?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 3. Are all servers located in the hosting area and are the on-site or off-site?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 4. Is the eHARS server hosting area protected from unauthorized access: (e.g. computer room is behind two locked doors, sign in required to get access to both so long as you are on the list of approved access staff)? |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 5. Is the server hosting area partitioned into specific areas (i.e., database servers, application servers, intranet servers, or internet servers)?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 6. Is the eHARS server hosting area protected from unauthorized access.  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 7. Is eHARS connected to the network?  |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 8. Are the servers reasonably accessible to HIV Surveillance staff?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 9. Is the security level adequate for rooms where servers are stored?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 10. Is the security level adequate for personal computers and laptops?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 11. Are electronic data, including backups adequately handled and stored?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 12. Is eHARS data being hosted on a virtual server?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 13. If applicable, are the server resources used to host virtual environments shared with other applications outside of eHARS?   |
| Yes <input type="checkbox"/>            | No <input checked="" type="checkbox"/> | 14. Are cloud hosting services used for eHARS software applications or HIV databases?  |
| Yes <input type="checkbox"/>            | No <input type="checkbox"/>            | 15. If applicable, has this cloud service completed the FedRAMP approval? N/A - nothing is in the cloud  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 16. Are IT staff with access to servers trained on the S&C policy and required to sign an S&C attestation form, which is kept in the personnel files?  |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 17. Are there contracted IT staff responsible for the eHARS servers and equipment?   |
| Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/>            | 18. Was due diligence taken to assure the following was considered prior to using contracted IT staff?<br>a. Potential Risks and Mitigations   |

|   |  |   |
|---|--|---|
|   |  | b. Responsibilities for Protections<br>c. Responses to Breaches   |
| Yes <input checked="" type="checkbox"/>   | No <input type="checkbox"/>            | 19. Does the contract address the following?:<br>a. Require annual staff training, and also upon hire, on Data Security and Confidentiality consistent with the CDC 2011 guidelines.<br>b. Require all staff with access to HIV surveillance information systems and data sign S&C agreements, which is kept in the personnel files.<br>c. Clearly delineate reporting requirements for security breaches, which result in release or unauthorized access to personally identifiable information (PII). |
| Yes <input type="checkbox"/>  | No <input checked="" type="checkbox"/> | 20. Has the eHARS Server Security and Confidentiality Review form been submitted and accepted?  |
| 21. What is the name of the eHARS server (s)? (e.g. dhssPreHarsAP01, dhssPRDB01, dhsstseharsap01, dhsstsd01) DPH-AP036 – Staging, DPH-AP037 - Production  |  |   |
| 22. What is their bit size? (e.g. 64Bit OS, 4GB mem, 1 vCPU) <b>Server Model:</b> Virtual, Operating System: 2008 R2 Standard SP1 64-bit. CPUs : Inter(R) Xeon(R) CPU-E5-2640 0 @ 2.50 GHz ( 2 Processors), Memory: 6 GB  |  |   |
| 23. What is the “Enter on Duty” date for the eHARS server (s)?<br><br>CT DPH current eHARS application and database servers are on a series of VM Ware hosts with varying ages. The Virtual servers themselves are currently running Windows Server 2008R2 Service Pack 1 and is receiving monthly Windows patches and Virus updates.   |  |   |
| 24. When do you anticipate having to retire the eHARS server(s)?<br><br>The OS on both the application and MS--SQL Database servers are current supported Microsoft products with an expected end of life of 1/14/2020. We anticipating replacing the servers with Windows Server 2016 in the first quarter of 2019.  |  |   |
| 25. What happens when eHARS servers, databases, all computers, hardware, and software (e.g. SQL database) are retired?<br><br>DPH IT follows the below steps to properly surplus both software and hardware.<br><br><b>Disposal of Surplus Software:</b><br>When it is determined that software is no longer needed by an agency, the software is removed from the inventory. |  |   |

Disposal of Hardware:

When it is determined that hardware is no longer needed by an agency, the hard drive is degaussed and then surplused.

26. How many IT staff are employed and have access in the server hosting area or to HIV information systems and SQL databases

There are currently:

- 31 employees on the IT support staff for the Department of Public health
- 10 support staff have physical access to the secured data center controlling the VMWare Hosts.
- 3 have access to the VMWare Server controls themselves, as this is limited by additional user name and password controlled security.

**Additional Comments or Recommendations:**

Additionally, in order to assure separation of duties, none of these employees with physical access to the hardware are the same support staff that have access to the Application front end or database directly.



**Heather Linardos, MPH**

HIV Surveillance Program Director  
TB, HIV, STD & Viral Hepatitis Section  
Connecticut Department of Public Health  
410 Capitol Avenue, MS #11 ASV  
Hartford, CT 06134  
e: [heather.linardos@ct.gov](mailto:heather.linardos@ct.gov)

Subject: **Security and Confidentiality Validation**  
Connecticut Department of Public Health  
PS18-1802, Cooperative Agreement No. NU62PS924521

Project Period 01/01/2018 – 12/31/2022

Dear Ms. Linardos:

This letter serves as **OFFICIAL NOTIFICATION** that the CDC monitoring team has completed review of the comprehensive processes that ensure policies and procedures in your program comply with the requirements of PS18-1802 and the National Center for HIV/AIDS, Viral Hepatitis, STD and TB Prevention's (NCHHSTP) Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs and approve validation of your program. In addition, security and confidentiality findings identified during inspection of the physical environment are acceptable and documented in site visit reports and related correspondence.

We congratulate you and your staff on the completion of this effort to ensure high-level policies and practices are in place to protect the confidentiality of the citizens of Connecticut and the security of routinely collected and stored program data.

Sincerely,

*June Mayfield*  
Program Consultant

*Angela Lee Kinsey*  
Surveillance Project Officer

*Jennine Kinsey*  
Prevention Project Officer

Cc: Delores Greenlee, CT Public Health Section Chief  
Portia Brewer, Grants Management Officer (GMO)  
Tonia Gray, Team Lead (HSB)  
Reginald Carson, Prevention, Team Lead (PDIB)  
File