



**STATE OF CONNECTICUT**  
**Department of Mental Health & Addiction Services**  
**Commissioner's Policy Statement and Implementing Procedures**



<b>SUBJECT/POLICY NAME:</b>	CONFIDENTIALITY STATEMENT
<b>POLICY CHAPTER</b>	COMPLIANCE AND ETHICS
<b>APPROVED BY:</b>	<i>Miriam Delphin-Rittmon</i> 3/16/2020 Miriam Delphin-Rittmon, Ph.D.      Date: March 16, 2020
<b>EFFECTIVE DATE:</b>	DATE: 03/12/1993
<b>LAST REVISED DATE :</b>	DATE: 01/28/2019
<b>POLICY OWNER:</b>	COMPLIANCE AND ETHICS

**STATEMENT OF PURPOSE:** The purpose of this policy is to set forth the standards of the Department of Mental Health and Addiction Services (hereafter referred to as DMHAS) governing the confidentiality, privacy and security of patients' Personal Health Information (PHI) and electronic personal health information (e-PHI) for the appropriately controlled release of such information, consistent with applicable federal and state laws, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), 42 CFR, Part 2, and Connecticut state law.

This policy is intended to provide Department of Mental Health and Addiction Services (DMHAS) employees with a basic understanding of their responsibilities to protect and safeguard the Confidential Information to which they have access as a result of their employment.

**POLICY:** This Policy Statement applies to all Workforce members of the Department of Mental Health and Addiction Services.

Privacy and security of Confidential Information is of the utmost importance at DMHAS. It is the responsibility of every employee to respect and maintain the privacy and security of Confidential Information. A violation of this policy will result in disciplinary action.

For purposes of this policy, "Confidential Information" is defined as information disclosed to an individual employee or known to that employee as a consequence of the employee's employment at DMHAS, and not generally known outside DMHAS, or is protected by law. Examples of "Confidential Information" include but are not limited to protected health information (also known as PHI); electronic protected health information (also commonly known as e-PHI) self-restricted personal data; and DMHAS financial and account information. Individual offices, departments, or programs may have additional types or kinds of information that are considered "Confidential Information" and are covered by this policy. "Confidential Information" includes information in any form, such as written documents or records, or electronic data in motion or at rest.

## **PROCEDURE:**

### **General Principles**

1. Although individual DMHAS institutions own the media on which personal health information is kept (e.g., paper records, videos, photographs, electronic storage media, etc.), they hold the personal health information stored on those media in trust for the benefit of our patients. Patients own their personal health information and, with limited exceptions set forth in the HIPAA Privacy Rule and state law (e.g., psychotherapy notes), they have a reasonable right to access their health information and to control access to it by others, to correct or comment on information contained in their medical record, and to be aware of how their personal health information is being used.
2. Uses and Disclosure of PHI: DMHAS institutions will not use, disclose, or release PHI to persons other than the patient or his/her authorized representative, except in the following circumstances:
  - To carry out treatment, payment, and health care operations, as authorized by the HIPAA Privacy Rule;
  - As required by law (e.g., to comply with statutory reporting requirements) or as permitted by law and by our Notice of Privacy Practices (e.g., in medical emergencies, for approved medical research purposes, or for public health oversight functions);
  - In certain circumstances, after giving the patient the opportunity to agree or object to the use or disclosure (e.g., relevant verbal disclosures to family members or friends involved in the patient's care or for facility directory purposes); and
  - Otherwise, only with the patient's specific written authorization.

### **Each employee shall have the following responsibilities under this policy:**

1. During employment and after the termination of employment, an employee will hold all Confidential Information in trust and confidence, and will only use, access, store, or disclose Confidential Information, directly or indirectly, as appropriate in the performance of the

employee's duties for DMHAS. An employee must comply with all applicable state and federal laws and DMHAS policies relating to access, use, and disclosure of Confidential Information, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA); Connecticut state law (relating to confidential records); DMHAS policies (e.g. Use of Computer Resources) and all other regulatory requirements relating to confidential information.

2. An employee will not remove materials or property containing Confidential Information from the employee's department or program area unless it is necessary in the performance of the person's job duties. Any and all such materials, property, and Confidential Information are the property of DMHAS. If materials or property containing Confidential Information are removed from DMHAS, the employee must safeguard the materials/property according to previously established policy and procedure and control access as necessary.
3. An employee will not seek to obtain any Confidential Information involving any matter which does not involve or relate to the person's job duties. Confidential Information or DMHAS records, documents, or other information may not be maliciously tampered with, altered, or destroyed.
4. If an employee has any question relating to appropriate use or disclosure of Confidential Information, the employee shall consult with the employee's supervisor or other appropriate DMHAS personnel.
5. Each employee must promptly report to the employee's supervisor any known violation of this policy, other DMHAS confidentiality or privacy policies, or federal or State confidentiality or privacy laws, by the employee or other DMHAS workforce, i.e., student, intern, resident, other member. Failure to report may result in progressive discipline process up to and including termination.

**REFERENCES:**

42 CFR Part 2, 45 CFR Parts 160 and 164

**FORMS AND ATTACHMENTS: N/A**