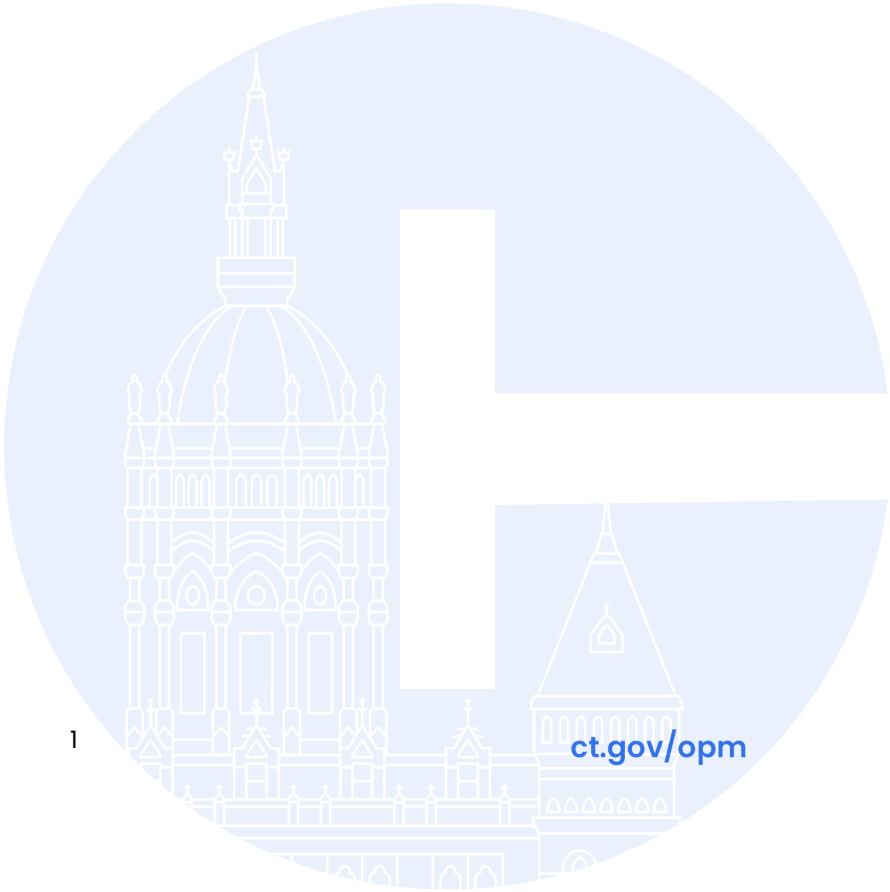
2025

Legal Issues in Interagency Data Sharing

Submitted pursuant to C.G.S. Sec. 4-67z.

CONNECTICUT
Policy and Management



Introduction

Pursuant to C.G.S. Sec. 4-67z, the Chief Data Officer each year, in consultation with the Attorney General, agency data officers and executive branch agency legal counsel, will review "methods to facilitate the sharing of … high-value data [of executive branch agencies] to the extent permitted under state and federal law, including, but not limited to, the preparation and execution of memoranda of understanding among executive branch agencies." This report provides an update on the development of these methods, through January 16, 2025.

The state has continued to make progress in three areas which the report describes in more depth:

I. **Coordinated statewide governance structure:** The state continued expansion of the Preschool through 20 Workforce Information Network (P20 WIN), which provides a common framework for interagency data sharing. In addition, a November 2024 report on cross-agency information sharing described a "data enablement service" as a way to expand data sharing beyond the cases facilitated through P20 WIN, with a coordinating body for governance.
II. **Flexible, durable data sharing agreements:** Data sharing agreement templates are in use for the major legal and regulatory frameworks applicable to agencies participating in P20 WIN. The templates provide a flexible, durable way to define the data sharing process between agencies and with third parties and have been developed and reviewed by agencies, the Office of the Attorney General (OAG) and the Privacy Technical Assistance Center of the Department of Education. OPM will embark on an update to these agreements in 2025 to enable use of a secure data enclave.
III. **Process improvements:** This report focuses on two areas for process improvements:
    a. **Data enablement service:** A data enablement service is the set of people, process and technology that would rely on "a coordinated group of individuals to implement…to function as a resource to state agencies who seek assistance or guidance with data sharing initiatives by curating use cases, identifying potential solutions, and supporting the implementation of these solutions."[1]
    b. **Secure data enclave:** To provide more secure and efficient data sharing, in 2024, the Office of Policy and Management (OPM) and the P20 WIN participating agencies agreed to develop a secure data enclave. The secure data enclave will provide a secure, private platform for interagency data sharing, with increased security and control over data which will allow agencies to engage in complex data sharing efforts with greater ease. The agencies will develop privacy and security controls for the

[1] Cross-Agency Information Sharing Report, issued by OPM in November 2024: https://portal.ct.gov/datapolicy/home/knowledge-base/articles/cross-agency-information-sharing-final-report?language=en_US

secure data enclave in 2025, which will be paired with revision of the related legal agreements.

Background

In addition to this report, pursuant to C.G.S. Sec. 4-67p, the Chief Data Officer is also required every two years to develop and implement a State Data Plan, in consultation with executive branch agency leadership and agency data officers. The State Data Plan is required to similarly "provide a timeline for a review of any state or federal legal concerns or other obstacles to the internal sharing of data among agencies, including security and privacy concerns."

The 2025 – 2026 State Data Plan was issued in December 2024 with a goal to identify "new opportunities for an enterprise data sharing approach." The focus on data sharing enhances decision-making by enabling agencies to gain deeper insights from integrated datasets and supports interdisciplinary efforts like environmental justice and social determinants of health by combining diverse data sources, including spatial data. Legal and technical safeguards are essential to ensure secure and ethical data sharing. A related OPM report from November 2024 on "Cross-Agency Information Sharing" recommends the implementation of a *process* for agencies to share data enabled by the people and technology supporting a "Data Enablement Service," which this report will describe in more detail.

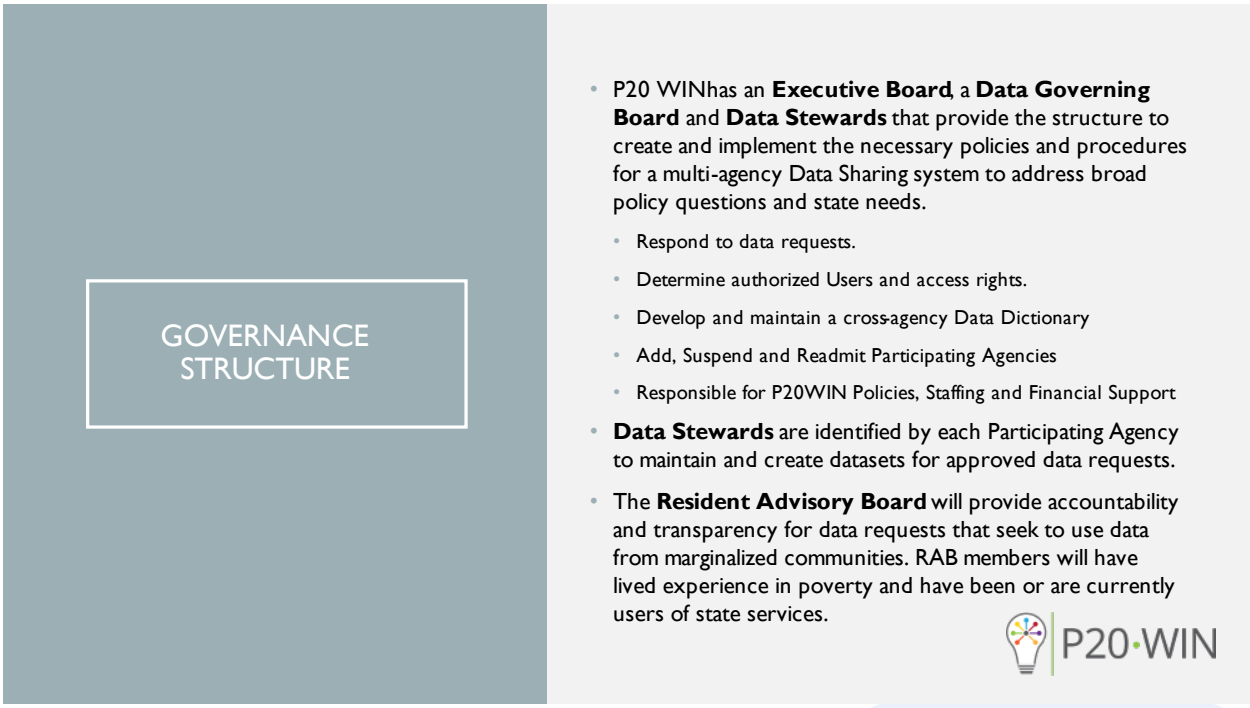
The initial report on legal issues in interagency data sharing from 2020[2] included the following recommendations, which are based on survey results from agency data officers and agency legal counsel, review of data sharing agreements, analysis of state and federal laws and regulations, and consultation with state agency staff and national experts:

I. **Establish a coordinated statewide governance structure for cross-agency data sharing:** The absence of a statewide governance structure leads to fragmented approaches to sharing data on high-priority issues which reduce the ability of the state to mobilize a response; and
II. **More flexible, durable data sharing agreements:** A proliferation of data sharing agreements makes oversight difficult and reduces the ability to protect clients' data and manage risk.

[2] All prior reports are posted here: https://portal.ct.gov/datapolicy/knowledge-base/articles/data-sharing-resources?language=en_US

Coordinated Statewide Governance Structure

The P20 WIN governance structure provides a standard set of policies and procedures for data sharing, while allowing each agency to retain administrative authority over their data. Program management for P20 WIN is provided by the staff of the OPM Data and Policy Analytics division(Operating Group), under the supervision of the Chief Data Officer. The graphic below describes the main elements of the governance structure for P20 WIN:



The function of securely linking the proposed data from participating agencies is undertaken through staff at the Connecticut Department of Labor (Data Integration Hub). Technical expertise is provided through participation of Bureau of Information Technology Services (BITS) in data governance.

The coordinated governance structure is further enabled by adopting a mission for P20 WIN that is focused on all aspects of individuals navigating state services. In 2021, Public Act 21-2, Section 250, June Special Session[3] expanded the purpose of P20 WIN "to inform policy and practice for education, workforce and supportive service efforts," covering the full cradle-to-career lifecycle and related health and human services supports. The changes to the statutory basis for P20 WIN expanded the types of requests that P20 WIN can fulfill and clarified aspects of the governance framework, including a definition for the E-MOU and reconstituting the Executive and Data Governing Boards. The

[3] Public Act 21-2 can be found at: https://www.cga.ct.gov/2021/ACT/PA/PDF/2021PA-00002-R00SB-01202SS1-PA.PDF

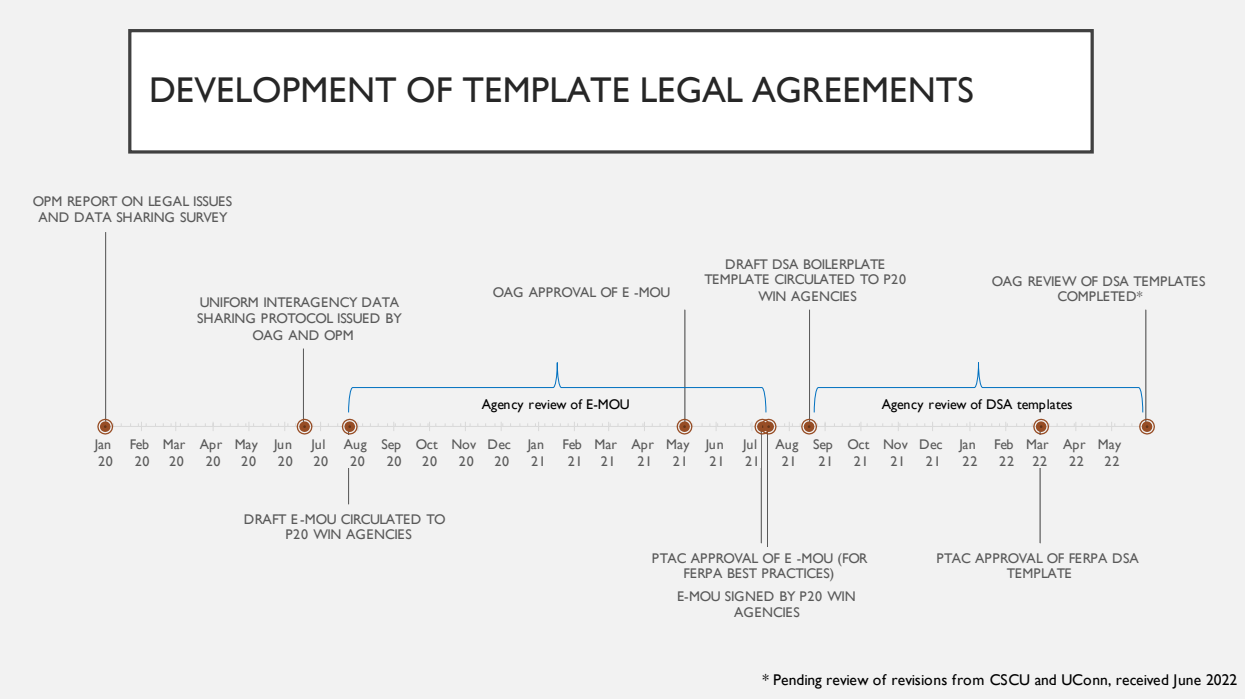
P20 WIN agencies have the authority to "to establish and implement policies related to cross-agency data management, including, but not limited to, data confidentiality and security," pursuant to C.G.S. Sec. 10a-57g(c), in consultation with OPM.

Flexible, Durable Data Sharing Agreements

The legal agreements for P20 WIN facilitate the decision-making and movement of data across agencies. The primary agreement for P20 WIN is an Enterprise Memorandum of Understanding (E-MOU),[4] which sets forth the "rules of the road" for how data are shared for all current and future participating agencies. The United States Commission on Evidence-Based Policymaking recommended the Enterprise Memorandum of Understanding (E-MOU) as a "best practice" method for data sharing.[5] The P20 WIN E-MOU was developed by the participating agencies in P20 WIN, OPM and OAG, in accordance with the framework and "uniform interagency data sharing protocol" shared in the 2022 report to the Legislature.

Data sharing agreements (DSAs) are the agreements that describe sharing data across agencies for a specific, limited purpose, and for specific agencies in accordance with the applicable relevant state and federal laws and regulations. The templates function similarly to the "boilerplate" language used for contracting and other written agreements – a template that can be modified easily for a specific agreement, without requiring development or review of an entirely new agreement.

[4] A copy of the E-MOU and related documentation are maintained at: https://portal.ct.gov/OPM/P20Win/Governance
[5] The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking, September 2017.



The templates were developed in an iterative process, described in the timeline above, which included review by state agencies, OAG and federal agencies where possible. The templates are crafted to work within the existing P20 WIN governance framework, although they can also be modified for "standalone" use outside P20 WIN.

The "template" approach allows flexibility by tailoring agreements to the specific context for each agency and each request and promotes durability by developing templates that draw on common elements which can be re-used and revised as needed. Templates have been developed and are continually reviewed for the following legal and regulatory frameworks:

Template	Child welfare	Financial aid	Education	Homelessness	Medicaid	SNAP	TANF	Workforce and wage data
Relevant federal and state laws	Title IV-E and IV-B, CAPTA	Higher Education Act (FAFSA and student loans)	FERPA	HUD HMIS regulations and standards	Medicaid, HIPAA, C.G.S. § 17b-90	SNAP federal law (7 CFR § 272.8(a)(4))	TANF federal law (45 CFR § 205.50)	Unemployment compensation (20 CFR 603.4), CGS §31-254, WIOA, TAA, JFES, Apprenticeship
Process changes			Designation of authorized representative, improper disclosure bars recipient from data access for 5 years	Designates CCEH as HMIS lead agency	DOL and Recipient sign Business Associate Agreements; Specific requirements for SUD and HIV/AIDS data			Penalties for misuse of UC data
Agency	DCF	OHE	OEC, CSDE, OHE,	CCEH	DSS	DSS	DSS	DOL

Template	Child welfare	Financial aid	Education	Homelessness	Medicaid	SNAP	TANF	Workforce and wage data
coverage			CSCU, CCIC, UConn					

Process and Technical Improvements for Data Sharing

As the governance and legal frameworks for agency data sharing have been firmly established and documented in prior installments of this report, this report will focus on two areas for process improvements, to allow more secure and efficient implementation of those frameworks.

Data Enablement Service: In November 2024, OPM issued a report on "Cross-Agency Information Sharing" which recommends implementation of a "Data Enablement Service" (DES), a *process* for agencies to share data for operational as well as analytical use cases. The report was based on a legislative requirement to develop a "secure online portal," but recommended implementation of a *process* for agencies to share data rather than development of a portal *per se*.

The report describes the core activities of a "data enablement service":

1. **Inventory Existing Tools and Initiatives:** Take stock of current data-sharing initiatives, technical tools, and governance structures to understand what resources can be leveraged.
2. **Establish a Coordinating Body:** Form a centralized group responsible for overseeing the implementation of standards, coordinating agency requests, and facilitating collaboration.
3. **Develop Shared Governance and Technology Standards:** Establish clear policies, processes, and tools that guide how agencies can securely share and manage data.
4. **Generate Quick Wins:** Deliver tangible results early by prioritizing low-complexity, high-impact use cases that demonstrate the value of the data-sharing framework.
5. **Measure Progress with Process Metrics:** Focus on tracking real-world impact, such as the number of data pipelines created, insights generated, and service improvements realized.
6. **Iterate through Retrospectives:** Continuously improve by regularly assessing completed initiatives, identifying lessons learned, and refining processes.

Many of these activities are in place or in development for analytical and evaluation purposes, through the requirements related to the State Data Plan, the P20 WIN system and the work of the Data and Policy Analytics division at OPM. Agencies inventory tools and data each year; governance is coordinated through agency data officers and OPM, which has supported implementation of a series of "quick win" use cases for data sharing, with progress measured through implementation of the goals of the State Data Plan. These same processes could be leveraged to develop the Data

Enablement Service with a focus on operational use cases, including sharing of identified data for improved service delivery and case management, increased program enrollment and participation. The DES would review each proposed use case to ensure the project is in line with agency priorities and in compliance with federal and state privacy and security laws before proceeding with technical and implementation guidance.

Secure Data Enclave: In addition, OPM, the Department of Labor (DOL) and BITS are developing a "secure data enclave" to facilitate secure interagency data sharing and storage. Development of the secure data enclave is based on a privacy and security risk assessment from the Data Integration Support Center (DISC) of WestEd, which provided technical assistance on the assessment and a roadmap for development of the secure data enclave. In June 2024, the P20 WIN Executive Board adopted a board resolution, attached as Appendix A, that states the priorities for this development to allow use for approved P20 WIN data requests. The enclave would improve secure use of data by developing rigorous audit, tracking and access controls and reducing the movement of data to reduce risk of a security incident. Development of the enclave is expected to begin in 2025, in consultation with privacy, security and legal experts from the P20 WIN participating agencies.

Legal Update

The following section reviews changes to relevant Federal and State laws during 2024. We do not anticipate any changes to current governance processes or data sharing agreements and process to be required based on these changes.

Drug and Alcohol Use Disorders

Federal Laws

On February 8, 2024, the U.S. Department of Health & Human Services (HHS), through the Substance Abuse and Mental Health Services Administration (SAMHSA) and the Office for Civil Rights (OCR), announced a final rule modifying the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations at 42 CFR part 2 ("Part 2"). With this final rule, HHS is implementing the confidentiality provisions requiring HHS to align certain aspects of Part 2 with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules and the Health Information Technology for Economic and Clinical Health Act (HITECH).

The Part 2 statute[6] protects "[r]ecords of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research,

[6] 42 U.S.C. §290dd-2

which is conducted, regulated, or directly or indirectly assisted by the any department or agency of the United States." Confidentiality protections help address concerns that discrimination and fear of prosecution deter people from entering treatment for SUD.

The final rule includes modifications to Part 2 in the following subject areas:[7]

Patient Consent

1. Allows a single consent for all future uses and disclosures for treatment, payment, and health care operations.
2. Allows HIPAA-covered entities and business associates that receive records under this consent to re-disclose the records in accordance with the HIPAA regulations. (However, these records cannot be used in legal proceedings against the patient without the specific consent or a court order, which is more stringent than the HIPAA standard.)
3. Prohibits combining patient consent for the use and disclosure of records for civil, criminal, administrative, or legislative proceedings with patient consent for any other use or disclosure.
4. Requires a separate patient consent for the use and disclosure of SUD counseling notes.
5. Requires that each disclosure made with patient consent include a copy of the consent or a clear explanation of the scope of the consent.

Other Uses and Disclosures

1. Permits disclosure of records without patient consent to public health authorities, provided that the records disclosed are de-identified according to the standards established in the HIPAA Privacy Rule.
2. Restricts the use of records and testimony in civil, criminal, administrative, and legislative proceedings against patients, absent patient consent or a court order.

Penalties

1. Aligns Part 2 penalties with HIPAA by replacing criminal penalties currently in Part 2 with civil and criminal enforcement authorities that also apply to HIPAA violations.[8]

Breach Notification

1. Applies the same requirements of the HIPAA Breach Notification Rule[9] to breaches of records under Part 2.

Patient Notice

1. Aligns Part 2 Patient Notice requirements with the requirements of the HIPAA Notice of Privacy Practices.

Safe Harbor

1. Creates a limit on civil or criminal liability for investigative agencies that act with reasonable diligence to determine whether a provider is subject to Part 2 before making a demand for

[7] The following section draws from the Fact Sheet for 42 CFR Part 2 Final Rule: https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html

[8] *See* 42 U.S.C. §§ 1320d-5 and 1320d-6

[9] 42 U.S.C. §§17921 and 17932

records in the course of an investigation. The safe harbor requires investigative agencies to take certain steps in the event they discover they received Part 2 records without having first obtained the requisite court order.

2. Clarifies and strengthens the reasonable diligence steps that investigative agencies must follow to be eligible for the safe harbor. Before requesting records, an investigative agency must look for a provider in SAMHSA's online treatment facility locator and check a provider's Patient Notice or HIPAA Notice of Privacy Practices to determine whether the provider is subject to Part 2.

Segregation of Part 2 Data

1. Adds an express statement that segregating or segmenting Part 2 records is not required.

Complaints

1. Adds a right to file a complaint directly with the Secretary for an alleged violation of Part 2.

SUD Counseling Notes

1. Creates a new definition for an SUD clinician's notes analyzing the conversation in an SUD counseling session that the clinician voluntarily maintains separately from the rest of the patient's SUD treatment and medical record and that require specific consent from an individual and cannot be used or disclosed based on a broad Treatment, Payment, and Operations consent. This is analogous to protections in HIPAA for psychotherapy notes.

It is important to acknowledge that records obtained in an audit or evaluation of a Part 2 program cannot be used to investigate or prosecute patients, absent written consent of the patients or a court order that meets Part 2 requirements.

Health

Federal Laws

On February 16, 2024, the U.S. Department of Health & Human Services (HHS) issued a Final Rule to modify the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to support reproductive health care privacy and to protect access to and privacy of reproductive health care, especially in light of the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* that has led to extreme state abortion bans and other restrictions on reproductive freedom in at least 21 states.

The Final Rule strengthens privacy protections by prohibiting the use or disclosure of protected health information (PHI) by a covered health care provider, health plan, or health care clearinghouse, or their business associates (collectively "regulated entities"), for either of the following activities:

1. To conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or

facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided.
2. The identification of any person for the purpose of conducting such investigation or imposing such liability.

Under the Final Rule, the prohibition applies where a regulated entity has reasonably determined that one or more of the following conditions exists:

1. The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided. For example, if a resident of one state traveled to another state to receive reproductive health care, such as an abortion, that is lawful in the state where such health care was provided.
2. The reproductive health care is protected, required, or authorized by federal law, including the U.S. Constitution, regardless of the state is which such health care is provided. For example, if use of the reproductive health care, such as contraception, is protected by the Constitution.
3. The reproductive health care was provided by a person other than the regulated entity that receives the request for PHI and the presumption described below applies.

The Final Rule continues to permit regulated entities to use or disclose PHI for purposes otherwise permitted under the Privacy Rule where the request for the use or disclosure of PHI is not made to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

The Final Rule includes a presumption that the reproductive health care provided by a person other than the regulated entity receiving the request was lawful. In such cases, the reproductive health care is presumed to be lawful under the circumstances in which it was provided unless one of the following conditions is met:

1. The regulated entity has actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided. For example, an individual discloses to the doctor that she obtained reproductive health care from an unlicensed person and the doctor knows that the specific reproductive health care must be provided by a licensed health care provider.
2. The regulated entity receives factual information from the person making the request for the use or disclosure of PHI that demonstrates a substantial factual basis that the reproductive health care was not lawful under the circumstances in which it was provided. For example, a law enforcement official provides a health plan with evidence that the information being requested is reproductive health care that was provided by an unlicensed person where the law requires that such health care be provided by a licensed health care provider.

To implement the prohibition, the Final Rule requires a regulated entity, when it receives a request for PHI potentially related to reproductive health care, to obtain a signed attestation that the use or

disclosure is not for a prohibited purpose. This attestation requirement applies when the request is for PHI for any of the following:

- Health oversight activities[10]
- Judicial and administrative proceedings[11]
- Law enforcement purposes[12]
- Disclosures to coroners and medical examiners[13]

The requirement to obtain a signed attestation gives a regulated entity a way of obtaining written representations from persons requesting PHI that their requests are not for a prohibited purpose. Additionally, it puts persons making requests for the use or disclosures of PHI on notice of the potential criminal penalties for those who knowingly and in violation of HIPAA obtain individually identifiable health information (IIHI) related to an individual or disclose IIHI to another person.
The Final Rule requires regulated entities to revise their Notice of Privacy Practices (NPP) to support reproductive health care privacy. The Final Rule also requires revisions to NPPs to address proposals made in the Notice of Proposed Rulemaking for the Confidentiality of Substance Use Disorder (SUD) Patient Records.[14]

State Laws

In 2022, the Connecticut General Assembly passed provisions concerning legal protections related to other states' laws regarding reproductive health services (including but not limited to abortion procedures) that are legal within the State of Connecticut.[15] Therefore, neither agencies nor P20 WIN will permit the sharing of such information pursuant to a request that would or could violate these laws.

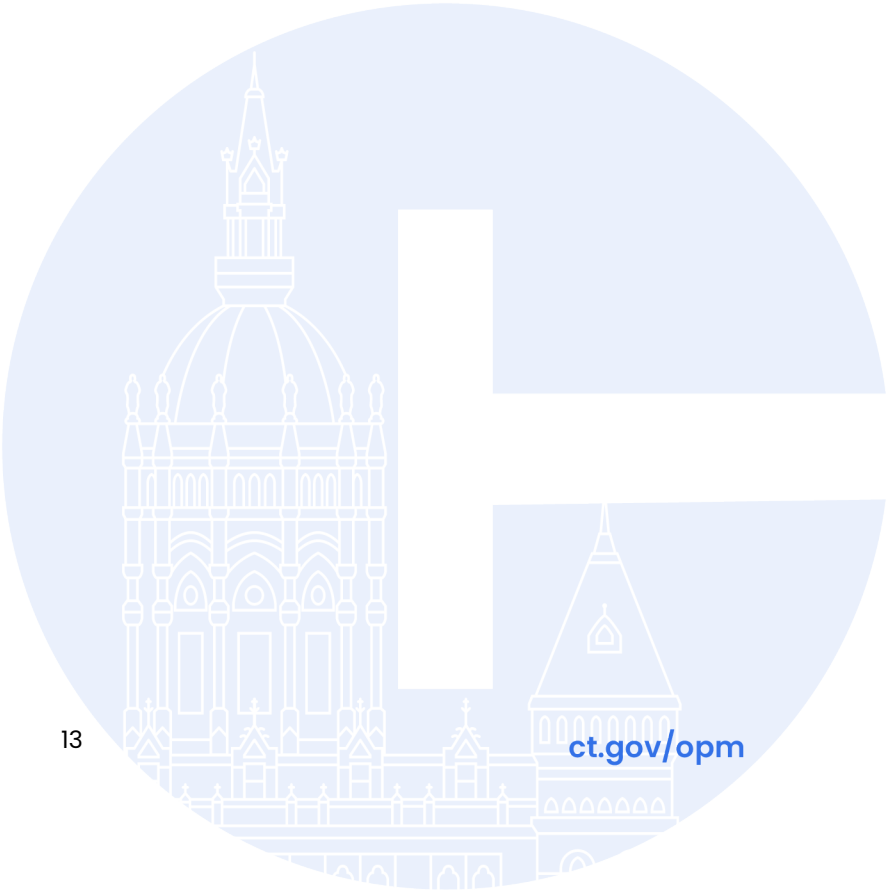
These state laws establish a cause of action for people against whom a judgment is entered in another state based on allegedly providing or receiving, or helping another person to provide or receive, or providing materials support for reproductive health care services that are legal in Connecticut.[16] The laws also limit the assistance that the state courts, public agencies, and certain health care providers may provide in legal actions related to reproductive health services that are legal in Connecticut. The laws prohibit public agencies, or individuals acting on their behalf, from providing information or expending resources to support an interstate investigation seeking to

[10] 45 CFR 164.512(d)
[11] 45 CFR 164.512(e)
[12] 45 CFR 164.512(f)
[13] 45 CFR 164.512(g)(1)
[14] 87 FR 74216,74237 (Dec. 2, 2022)
[15] PA 22-10 and PA 22-118 §§ 484-488.
[16] The cause of action is not available under particular circumstances, include (1) when no part of the acts that formed the basis for liability occurred in Connecticut; or (2) when the judgment entered in another state is based on a claim similar to one that exists under Connecticut law and meets certain criterial (e.g. patient claiming medical malpractice).

impose criminal or civil liability and prohibit certain health care providers, payors or information processors from disclosing protected health information without the written consent from the patient/authorized legal representative.

Conclusion

The intersection of the legal and governance framework and the supporting people, process and technology will serve to make data sharing more efficient, safe, ethical, equitable and secure. Coordinated data governance will create a consistent process for development and review of interagency data requests, improving the experience for agencies and data requestors. Flexible, durable data sharing agreements will allow a consistent approach with templates that can be tailored to individual agency use. Process and technical improvements to the data sharing process will provide transparency and allow for data to be used to inform decision-making on an ongoing basis.



Appendix A: P20 WIN Executive Board Resolution to Create Secure Data Enclave

P20 WIN EXECUTIVE BOARD RESOLUTION TO MODERNIZE THE P20 WIN SYSTEM
DULY PASSED ON JUNE 26, 2024

WHEREAS, this Executive Board, consistent with its roles providing the oversight of the P20 WIN network and advancing a vision for P20 WIN, supporting improvements, and responding to issues from the Data Governing Board, pursuant to the legislative mandate under C.G.S. Sec. 10a-57g;

WHEREAS, this P20 WIN Executive Board agrees that it is important to continue to improve and expand upon its infrastructure that supports data sharing across State and other agencies allows for a more holistic view of individuals, families and households, often served by multiple government and nonprofit agencies;

WHEREAS, the development of a modern data infrastructure for P20 WIN will improve data privacy, security, system capabilities, and the ability to use data for legitimate state purposes;

WHEREAS, the Office of Policy and Management (OPM) shall coordinate with the Connecticut Bureau of Information Technology Solutions (BITS) within the Department of Administrative Services (DAS) to assist the P20 WIN Executive Board in such development process.

BE IT RESOLVED, as a step towards developing such a modern data infrastructure, and based on a unanimous vote in favor of this Resolution, this Executive Board agrees to authorize the Operating Group, with the Data Governing Board, to develop the related policies and procedures to build an infrastructure for a hybrid cloud-based solution that accomplishes the following:

1. Combines aspects of a federated and centralized model;
2. Centralizes the platform for matching, analysis and data movement in a single cloud-based platform;
3. Ensures agency authority over the release and use of data through centralized access controls;
4. Allows for auditing and tracking movement, access, and usage of data by agency staff and researchers;
5. Develops a process for maintaining persistent linked identifiers to accelerate the request process, reduce the burden on agencies, and improve data quality;
6. Allows agencies to determine the frequency and nature of updates to a central cloud-based repository, whether regular (annual or quarterly) or project-based;
7. Reduces the movement of data and use of manual processes; and
8. Complies with all relevant agencies, P20 WIN, state and federal policies and procedures.

BE IT FURTHER RESOLVED that the Operating Group may pursue additional options, including but not limited to the Administrative Data Research Facility, to provide flexibility and to support project-based or interstate data use.