Legal Issues in Interagency Data Sharing

Report for Public Act 19-153

January 15, 2020

Table of Contents

Introduction

The Office of Policy and Management (OPM) submits this report pursuant to Public Act No. 19-153, which provides that:

> (a) The Chief Data Officer, in consultation with the Attorney General and executive branch agency legal counsel, shall review the legal obstacles to the sharing of high value data of executive branch agencies, inventoried pursuant to section 4-67p of the general statutes, among agencies and with the public.
>
> (b) Not later than January 15, 2020, and annually thereafter, the Chief Data Officer shall submit a report, developed in consultation with the Attorney General, agency data officers, and executive branch agency legal counsel, that includes any recommendations on (1) methods to facilitate the sharing of such high value data 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, and (2) any necessary legislation, to the Connecticut Data Analysis Technology Advisory Board and the joint standing committee of the General Assembly having cognizance of matters relating to government administration, in accordance with the provisions of section 11-4a of the general statutes.

The following submission reflects OPM's preliminary conclusions based on data from agencies and consultation with a national expert on state government data sharing.[1] While time did not allow for extensive consultation with executive branch agency legal counsel, OPM obtained preliminary feedback, where possible, and intends to utilize this report as a tool to further engage agency data officers and legal counsel in our efforts to streamline agency data sharing to further improve state policy-making, program outcomes, and the overall well-being of people. As this report is annual, OPM intends to utilize the next year to work with experts inside and outside state government to hone in on the challenges and preliminary suggestions identified below and to provide recommendations on any necessary legislation in the 2021 report. We believe we have made substantial progress on this important issue since the legislature passed Public Act No. 19-153 and look forward to working with the committees of cognizance as we move forward.

[1] Richard Gold, JD - Consultant on Confidentiality and Data Sharing. The report also reflects review and comments by staff from OPM, the Office of the Attorney General and Agency Data Officers and counsel from executive branch agencies.

Overview

Databases in state government are an underutilized resource among policy-makers, public officials, case managers, and advocates. Today, individuals who receive governmental services are often involved with multiple systems. For example, a young mother and her child may receive SNAP benefits, child care subsidies, child support payments, or other state-delivered services. Each of these programs was designed to fulfill a distinct purpose, and each collects different data and follows different rules and requirements. Each program's database only identifies patterns or characteristics of those served within that particular agency or program. Isolated databases omit information from other agencies or programs that could be analyzed to increase wellbeing, long-term personal success and reduce costs to state and local government.

The demand for interagency data has increased with recent developments in performance management and evidence-based policymaking. This report makes two primary recommendations to facilitate the sharing of data across government agencies. The recommendations are based on analysis of survey results from executive branch agencies, review of current data sharing agreements, analysis of state and federal laws and regulations on data sharing, and consultation with state agency staff and national experts:

1. **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. This report describes three high-profile use cases for data sharing that are opportunities to coordinate state efforts and data governance. The appendix to the report is intended to serve as the starting point of a resource to enable coordination and knowledge-sharing across agencies.

2. **Develop 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. Flexible, durable data sharing agreements would protect clients' information and reduce the effort needed to share data. The report describes one approach to creating templates for flexible, durable legal agreements.

The recommendations are consistent with the focus in Connecticut on taking a data-driven approach to pressing policy challenges, particularly those that can only be addressed across institutional boundaries.

As providers of services, states must find balanced approaches that promote information sharing, protect confidentiality and privacy, keep data secure, improve services and outcomes, increase efficiency, and reduce duplication of efforts for both clients and the state employees. Federal and state statutes and regulations, summarized in Appendix A of this report, are in place to protect privacy and confidentiality. Improved access to data under more privacy-protective conditions can lead to an increase in both the quantity and the quality of evidence to inform important program, practice, and policy decisions. Connecticut would be remiss to not take advantage of the tremendous technological advances of today to improve outcomes and efficiency for residents where statutory and regulatory authority exists. OPM looks forward to supporting agency efforts to protect the confidentiality, privacy, and security requirements of the law.

Connecticut State Government Data Sharing Use Cases

Connecticut's State Data Plan recognizes that data is a valuable asset that the State must manage in the public trust on behalf of its residents, and includes 'identify[ing], and where appropriate, remove[ing] data sharing barriers between state agencies,' as a goal of the plan.[2]

Connecticut requires the ability to integrate its data across agencies at the individual level and in aggregate up to the level of the family, household, school, neighborhood, town, and region. Depending on the interests and priorities of the user, multi-agency data can potentially be used to improve:

- **Program administration:** providing key providers with the total cross-system case record for an individual client and her family, for purposes of case management; providing unified enrollment and eligibility systems to create more generous, client-friendly social supports; helping clients experience less trauma by avoiding the need to repeat their story to every bureaucracy that is providing services
- **Policy analysis**: quantifying cost-savings to health systems achieved by recipients of housing subsidies
- **Research**: utilizing child welfare, juvenile justice, public school, and college enrollment records to identify predictors of high school dropout
- **Evaluating outcomes and managing performance:** measuring the budgetary and social consequences of a new investment in supportive housing across several agencies serving homeless populations

Connecticut is currently engaged in several efforts to use cross-agency data to improve program administration, inform policy and research, and to evaluate outcomes and performance. These efforts ('use cases') recognize the necessity of integrating data across multiple agencies to reflect the reality that people receiving governmental services are often involved with multiple systems.

Each of the following efforts seeks to achieve better outcomes for individuals and families through integrated data. The following enterprise efforts were chosen to highlight in this report because they are high priorities under the current administration of Governor Lamont, and each seeks to integrate data across more than two state agencies. In other words, each requires finding a legal framework for data sharing outside an agency structure:

1. **Housing and Supports for Vulnerable Populations:** The Governor's Office has established a Task Force on Housing and Supports for Vulnerable Populations.[3] The mission of this task force is to enhance coordination across agencies "to ensure that the state evaluates vulnerability and prioritizes resources consistently, coordinates effectively to serve shared clients, and implements best practices reliably to meet resident's housing/housing support needs with the goals of improving outcomes and conserving resources." The pilot will identify frequent utilizers of state services, and then coordinate the services to these recipients to improve participant outcomes while reducing state expenses. The task force aims to complete a data match between the state's Homeless Management Information System (HMIS), which is run by non-profit partners, with data from key social service agencies including:

[2] The State Data Plan, submitted by OPM in December 2018, can be found at: https://portal.ct.gov/CTData
[3] https://portal.ct.gov/Office-of-the-Governor/Working-Groups/Task-Force-on-Housing-and-Supports-for-Vulnerable-Populations

- Department of Social Services (Medicaid agency),
- Department of Mental Health and Addiction Services,
- Department of Children and Families,
- Department of Correction, and
- Court Support Services Division.

The data match pilot will allow the state to quickly identify data-sharing challenges, and then bring the appropriate parties to the table to work towards solutions. The data match aims to enable the task force to identify initial drivers of household crisis; gain visibility with regard to patterns of service use; and create service cost estimates for these households' past engagement with state agencies to compare to the cost of services needed to stabilize these households. The lessons learned from the task force will also assist the state as it works to set up the infrastructure for interagency data sharing.

2. **Two-Generational Initiative Interagency Plan:** In 2015, Connecticut became the first state in the nation to pass legislation to codify a two-generational initiative in statute (§401 of Public Act No. 15-5, June Special Session).[4] Two-Generational (2Gen), or whole family approaches, focus on creating opportunities for, and addressing the needs of, children and adults together by taking a family-centered, results-oriented approach so that children and families get the education, workforce training, and social supports they need to secure economic stability that passes from one generation to the next. Connecticut's statute established a 2Gen Advisory Board, which coordinates with three action-oriented subgroups that work collaboratively to develop solutions for core 2Gen initiatives: parent engagement, workforce development, and minimizing benefits cliffs. As part of the 2Gen efforts, Public Act No. 19-78 requires the state to develop "infrastructure to promote data sharing within and between state agencies to the extent permissible under federal and state law." By July 2020, PA 19-78 further requires the attorney general's office to "develop a uniform interagency data-sharing protocol to remove legal barriers to promote cross-agency and cross-sector collaboration under the act to the fullest extent permitted under state and federal laws," in consultation with OPM, the Chief Data Officer and the P20-WIN longitudinal data system.

3. **Governor's Workforce Council**: In fall 2019, Governor Lamont issued Executive Order No. 4, to create the Governor's Workforce Council (GWC). Among the provisions of the order is a requirement that "state agencies shall enact appropriate data-sharing agreements with one another and with the Governor's Workforce Council to facilitate" analysis of workforce development programs and services, funding streams, and the associated outcomes. While Executive Order 4 does not create the necessary infrastructure for data sharing, it does provide a further imperative for agencies to share data. Agencies participating in the GWC include those participating in the state's longitudinal data system, P20-WIN, and additional representatives from administrative services, social services, aging and disability and higher education. The Executive Order requires the Council to submit a report by January 1, 2021 with recommendations on workforce, including an emphasis on "data-driven outcomes," with consistent measurement and improvements in data systems "across different programs and agencies."

[4] Connecticut General Statutes §17b-112

As these efforts are implemented, they will help to identify both successful practices and barriers in cross-agency data sharing in Connecticut. Close coordination between the agencies involved in these initiatives, the Chief Data Officer, the Office of the Attorney General, and the Connecticut Data Analysis Technology Advisory Board will help to ensure consistency with the goals and legal framework of the individual use cases and the State Data Plan.

Survey to Executive Branch Agencies

To better understand the data sharing landscape in Connecticut state government, OPM surveyed 23 Executive Branch agencies about their current data sharing agreements and the laws and regulations that govern the data maintained at each agency.[5]

The survey asked questions about the sharing of high value data, defined by statute as "any data that the department head determines (A) is critical to the operation of an executive branch agency; (B) can increase executive branch agency accountability and responsiveness; (C) can improve public knowledge of the executive branch agency and its operations; (D) can further the core mission of the executive branch agency; (E) can create economic opportunity; (F) is frequently requested by the public; (G) responds to a need and demand as identified by the agency through public consultation; or (H) is used to satisfy any legislative or other reporting requirements."[6]

Agencies were asked to respond to the following two questions in the survey:

1) Have you been able to execute and implement any interagency data sharing agreements to support advancing your or your partner agency's mission?

   If yes, agencies were asked to inventory their data sharing agreements, providing the following information about each agreement:

   a. How would you characterize the agreement (e.g. MOU, MOA, data sharing agreement, intergovernmental agreement, etc.)?
   b. List the agencies, programs, or organizations that are included in the agreement.
   c. What data does your agency provide through this agreement? Provide the data source name if possible.
   d. At what level is the data shared (e.g. individual-level or aggregated)?
   e. Briefly describe the purpose of this data sharing arrangement.
   f. Provide the date when the agreement began.
   g. Provide the date when the agreement has or will end.
   h. How often is the data shared (e.g. once, continuously, monthly, annually etc.)?
   i. Indicate whether the agreement is active or inactive.

2) Are there laws, regulations, or policies that pertain to the sharing of data that is maintained at your agency?

[5] Surveys were sent to Agency Data Officers via email on September 15, 2019. The original deadline (October 10) was later extended until October 21, 2019 to allow agencies more time to collect the data requested.
[6] Connecticut General Statutes, Section 4-67 p, https://www.cga.ct.gov/current/pub/chap_050.htm

If yes, agencies were asked to inventory the laws, regulations, and policies that govern data at the agency, providing the following information:

a. List the statues, regulations, and/or policies regulating the sharing of the data maintained at your agency.
b. What data at your agency is impacted?
c. Are there exceptions to the limitations on data sharing in this statute/regulation/policy? If so, please describe.
d. Provide a brief description of how this law/regulation/policy impacts data sharing at your agency (e.g. if data sharing is prohibited completely, if you can only share some fields or must de-identify the data, which would prevent data linking, etc.)
e. Has your agency previously declined an interagency data sharing request in light of the law/regulation/policy?
f. If available, provide a link to the statute, regulation, or policy.

Seventeen agencies had responded to the survey at the time this report was written. The results of the survey are summarized in the following sections.

Existing Data Sharing Agreements

The first question of the survey asked agencies to inventory their existing data sharing agreements. Reporting agencies inventoried 224 data sharing agreements. However, the results of this survey do not represent the entirety of data sharing agreements between Connecticut state agencies. Some agencies reported having more agreements in place than they had the resources to inventory, so they submitted a representative sample of their agreements instead of providing information about all the agreements in place. It should be noted that the sum of agency data sharing agreements contains some duplicates in cases where multiple agencies reported the same agreement. The table below summarizes the data sharing agreements reported in the survey.

Data Sharing Agreements by Agency: Responses to Survey for P.A. 19-153

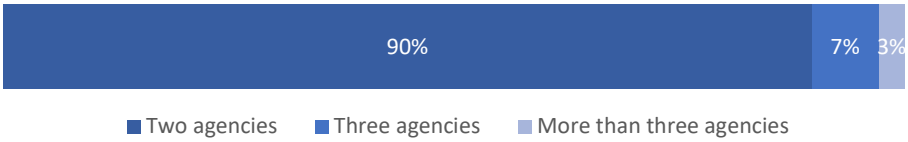
Agency Name	Data Sharing Agreements Inventoried
Department of Administrative Services	7
Department of Banking	5
Department of Children and Families	17
Department of Consumer Protection	9
Department of Correction	19
Department of Developmental Services	4
Department of Emergency Services and Public Protection	4
Department of Energy and Environmental Protection	4
Department of Housing	1
Department of Insurance	0
Department of Labor	45
Department of Motor Vehicles	36

Department of Public Health	47
Department of Transportation	3
Office of Early Childhood	20
Office of Policy and Management[7]	0
State Department of Education	3
Total	**224**

While this listing is not a complete inventory of every agreement in the state due to the limitations noted above, the survey results demonstrate that significant data sharing is taking place between Connecticut state agencies.

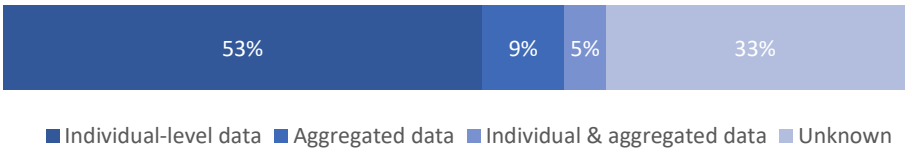
Ninety percent of the agreements inventoried involved data sharing between two agencies (157). Seven percent of the agreements were between three agencies (13), and three percent were between more than three agencies (5).

Number of agencies involved



Fifty-three percent of the data sharing agreements listed involved the sharing of individual-level data (93), while nine percent of the agreements involved sharing aggregated data (16), and five percent of the agreements inventoried involved sharing both individual and aggregated data (8). Thirty-three percent of the agreements listed did not indicate the level of data shared (58).

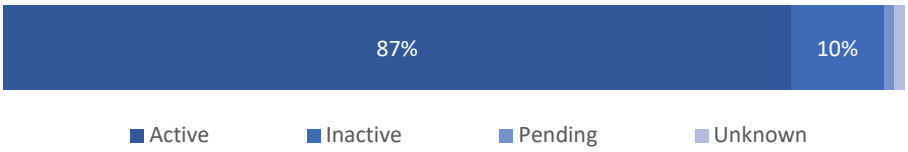
Level of data shared



Eighty-seven percent of the agreements listed in the inventory were active at the time the survey was submitted (153), while ten percent were reported as inactive (18). An additional one percent of agreements was listed as pending (2), and one percent did not indicate the status of the agreement (2).

Agreement status

[7] This does not report data sharing agreements specific to the Criminal Justice Policy and Planning Division.



The data sharing agreements inventoried through the survey serve a variety of purposes, and the primary purpose of the agreements can be grouped into the following categories:

1) **Program administration** - To facilitate the administration of state programs;
2) **Research and policy analysis** - To inform research conducted at state agencies or outside entities and to shape state policy;
3) **Monitoring and evaluation** - To monitor trends and compliance of entities regulated by the state; and
4) **Reporting and performance** - To assess the performance of state programs and initiatives.

The most common purpose for data sharing reported was program administration. Examples of the data sharing agreements in each of these categories include the following:

Program Administration

- The Department of Administrative Services (DAS) and the Department of Labor (DOL) share individual-level data on a daily basis to administer the state's Workers' Compensation Program.
- The Department of Children and Families (DCF) and the Department of Social Services (DSS) share individual-level data on a daily and weekly basis to verify an individual's social security number and to obtain state and federal benefits information to administer DCF programs.
- The Department of Motor Vehicles (DMV) shares driver's license images with the Department of Consumer Protection (DCP) to facilitate the DCP permitting process.
- The Department of Public Health (DPH) shares individual-level data on participants in the Women, Infants, and Children (WIC) program with DSS upon request to identify dual participants and to refer women and children who have aged out of the WIC program to other programs.

Research and Policy Analysis

- The Department of Correction (DOC) shared individual-level data with the Court Support Services Division (CSSD) and Central Connecticut State University (CCSU) to conduct research on the Sexual Offender Registration System for a one-time study.
- DOC, CSSD, the Department of Mental Health and Addiction Services (DMHAS), the Board of Pardons and Paroles (BOPP), and the Department of Emergency Services and Public Protection (DESPP) share data annually to link arrest, incarceration, parole, and probation data with behavioral health treatment data to create a de-identified, analytic database for the mutual benefit of all parties.
- The Department of Transportation (DOT) shares data with the University of Connecticut (UConn) to provide data for the crash data repository on a daily basis.
- The Office of Early Childhood (OEC) and the State Department of Education (SDE) both share individual-level data with DOL upon request as part of the state's P20 WIN longitudinal data

system, which securely links data between education and workforce agencies for audits and evaluations of publicly funded education programs.

Monitoring and Evaluation

- DPH and DCP share data from the Prescription Monitoring Program (PMP) to review PMP indicators related to opioid prescriptions. Individual-level linked data is shared upon requested, and aggregate data is shared quarterly.
- DPH and DCP share data on regulated food implicated in a case of foodborne illness upon incident.
- DMHAS and DCP share reports from the Electronic Nicotine Delivery System to streamline retailer inspections.

Reporting and Performance

- DCF shares individual-level data with UConn on a quarterly basis, and the UConn Performance Improvement Center uses the data to evaluate and support the delivery of high-quality services by DCF Community Partner Agencies within the Differential Response System.
- OEC receives data from DCF on an annual basis for the federal grant reporting for the Maternal, Infant, and Early Childhood Home Visiting program.

In addition to providing an inventory of data sharing agreements, many agencies shared example MOUs for review, as well as information about which laws and regulations govern data at their agency.

Laws and Regulations Governing Agency Data Sharing

Agencies reported a variety of laws and regulations that govern the data they collect and maintain. Agencies reported 136 laws and regulations that affect their high value data. The list of laws and regulations collected through this survey does not represent all laws/regulations governing data at state agencies, as some may have been omitted and not all agencies responded to the survey. As in the previous section, the sum of the agency laws and regulations cited contains duplicates in cases where multiple agencies reported the same law or regulation. In other cases, agencies reported individual sections of a single law or regulation, where those sections described different types of data. The table below summarizes the laws and regulations cited by agencies responding to the survey for P.A. 19-153.

Laws and Regulations by Agency: Responses to Survey for P.A. 19-153

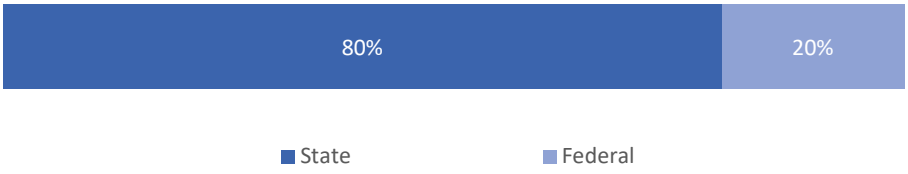
Agency Name	Laws/Regulations Cited
Department of Administrative Services	7
Department of Banking	3
Department of Children and Families	28
Department of Consumer Protection	25
Department of Correction	6
Department of Developmental Services	7
Department of Energy and Environmental Protection	7
Department of Housing	1
Department of Insurance	9
Department of Labor	8

Department of Motor Vehicles	1
Department of Public Health	29
Department of Transportation	2
Office of Policy and Management	2
State Department of Education	1
Total	**136**

DPH cited the most laws and regulations in the survey (29), followed by DCF (28), and DCP (25). These three agencies listed far more laws and regulations than the other reporting agencies; on average, agencies reported nine laws and regulations that impacted the high value data they collect and maintain.

Eighty percent of the laws and regulations listed in the survey were at the state level (109), while 20 percent of the laws and regulations listed were at the federal level (27).

State vs. federal laws and regulations



For almost all agencies that responded to the survey, most laws and regulations governing data cited were at the state level. For instance, 72 percent of the laws/regulations listed were at the state level at DPH, with 75 percent at DCF and 100 percent at DCP. Only DOL reported more federal laws/regulations than state, with 88 percent at the federal level.

A more detailed analysis of the key laws and regulations are attached as Appendix A to this report.

Recommendations to Facilitate Data Sharing

In preparing this report, we have learned that a great deal of data sharing is occurring within the State of Connecticut. A review of existing data sharing agreements shows that there are hundreds of existing agreements between state agencies and with outside entities. Review of legal agreements and agency processes shared for this report shows that, while these agreements fall into standard categories, such as program administration or research, each agency tends to have its own format and process for legal agreements to facilitate data sharing.

While this report does not contain a detailed analysis of the time and effort involved in creating data sharing agreements, it is hard to discount anecdotal evidence that it is a time-consuming and laborious process each time there is a request to share data. Lack of explicit authorization leads to different interpretations by different legal counsel charged with recommending whether they can be included in integrated data sharing agreements.

Connecticut is currently receiving training and technical assistance from Actionable Intelligence for Social Policy (AISP), at the University of Pennsylvania, to develop and improve the integrated data system governance, legal considerations, data standards, and technologies.[8] Based on our engagement with AISP and the research and outreach conducted in preparation for this report, broadly speaking, we recommend that Connecticut implement the following practices to facilitate the sharing of high-value data in a way that is compliant with both state and federal laws:

- **Establish a coordinated statewide governance structure for cross-agency data sharing**. A thoughtfully established governance system can reduce the risk to individual agencies through shared decision-making, increase transparency about data sharing agreements, and enable learning across agencies. Such a successful governance process must include the following six common attributes:[9]

    1. Identify and assemble strong executive leadership,
    2. Create a shared vision,
    3. Formalize and document the governance structure,
    4. Establish clear decision-making process,
    5. Evaluate governance system and adapt as necessary, and
    6. Maintain transparent communications.

    The use cases identified in the report speak to the need for such a governance structure, since the three cases identified are high priority efforts, involving executive leadership, that are not housed within a single agency. Examples of governance structures along these lines already exist within some domains, such as the P20-WIN system, which has facilitated a long-standing collaboration between education and workforce agencies.

- **Develop more flexible, durable data sharing agreements.** Data sharing would be advanced through the development of more flexible, durable data sharing agreements to be used across state government. Flexible agreements encourage consistency across agencies, by using a single template or set of templates that can be adapted for different uses. Durable agreements stand the test of time and can be used for different arrangements between the same parties, reducing the frequency with which new agreements need to be drafted and negotiated. Much progress has been made by groups like AISP, that recommend a four-document approach:

    1. **Policy agreement of the participating agency leaders to achieve an integrated data sharing process.** This can be an agreement, or a letter signed by the highest-level executives. This is in addition to an executive order and/or legislation. The use cases in this report can help to identify potential agencies to participate in such an agreement.

    2. **An Enterprise Memorandum of Understanding (E-MOU).** This type of Memorandum of Understanding (MOU) sets forth the "nuts and bolts" of how data

[8] AISP works with state and local governments to develop integrated data systems that link data across government agencies to provide the government and their partners with the ability to better understand the needs of individuals and communities and improve programs and practices through evidence-based collaboration. AISP works with new sites

[9] A handbook for States: *Establishing Governance for Health and Human Services Interoperability Initiatives.*

is shared for all the participating state agencies, regardless of whether the data is identifiable or de-identified. The Enterprise MOU will avoid the need to negotiate and draft a new MOU document every time data needs to be shared, saving time and money. (Such a document is operational currently and successfully in Virginia, Illinois, California, Colorado and other states, counties, and localities.) The United States Commission on Evidence-Based Policymaking recommended the Enterprise Memorandum of Understanding (E-MOU) as a "best practice" method for data sharing.[10]

3. **A Data Sharing Agreement (DSA).** This is a document that is signed by the provider of data for the purposes of sharing the data with a particular party or parties. It provides the legitimate governmental purpose for the data sharing, the legal basis for what is shared, and who can have access to the data.

4. **A Data Use Agreement (DUA).** This is a document that is signed by the receiver of data and sets forth the security provisions for the data, who will have access to the data, the use of the data, and how the data will be returned to the sender or destroyed after the legitimate purpose is completed.

Progress in these areas is most likely when supported by frequent, active communication among state agencies, the Chief Data Officer, and the Connecticut Data Analysis and Technology Advisory Board. The State Data Plan asks the Chief Data Officer to "facilitate interagency coordination through round table discussions and other communication methods"[11] and this type of coordination should continue and expand.

The conclusions in this report rest primarily on analysis of the survey on legal agreements for data sharing, review of sample legal agreements, and the summaries of state and federal laws contained in Appendix A. Consequently, this initial report devotes little attention to questions of technology, public engagement, and informed consent. However, each of these topics merits further attention and should inform the development of governance and flexible, durable data sharing agreements. Legal agreements help agencies to know how their data is being used, and residents and recipients of government services deserve the same level of security. A principle in the State Data Plan is to 'improve data sharing and access with ongoing input from users and other stakeholders, including those whose personal and protected data are collected in state agency systems' and future reports should increase the focus on increasing transparency on this front.

Connecticut should continue to explore the following topics in parallel to implementation of the above practices:

- **Investigate new technical solutions that reduce the degree and risk of data exchange necessary to make decisions based on integrated, evidence-based data.** Technology can simplify the creation of the associated legal frameworks, with access to the data tailored to the request, whether it be for research, program evaluation, or case management. Technology can be used to ensure that the legal confidentiality requirements are met (by

[10] *The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking.* September 2017.
[11] Connecticut State Data Plan, December 2018.

building them into the operation of the system) and enable data to be shared for use in decision-making.

- **Enhance the ways in which existing and future data sharing efforts engage the public, including how residents consent to or authorize the use of their data.** If everyone has a shared understanding of why and how data will be shared, with basic privacy safeguarded, the families and individuals being served and those who advocate on their behalf will become allies of these efforts, rather than skeptical observers or outright opponents. Transparency and engagement about goals and processes – with partners and the public – is critical to getting to "yes" and sustaining a meaningful program.[12]

OPM is currently conducting ongoing work to develop and implement these recommendations. The opportunity for Connecticut to participate in training and technical assistance from AISP will greatly help the State to develop a more robust data sharing plan and system. OPM asks that the legislature allow us to continue this work over the next year to formulate a more detailed plan that integrates these key steps.

With respect to Public Act No. 19-153's focus on the "legal obstacles to the sharing of high-value data of executive branch agencies," as detailed in Appendix A, a frequent barrier to the development of integrated and shared data systems are the many overlapping federal and state confidentiality and privacy laws governing the collection, use, and disclosure of administrative data. Written to address real risks to individual privacy, these laws were nevertheless developed for different agencies to address diverse concerns, mostly before the advent of electronic records. When applied to data integration, these laws interact in ways that are often inconsistent or unclear, making the development of the sharing documents (e.g. memorandums of understanding) a difficult and prolonged process.

Many statewide longitudinal data systems are authorized through state law, for example, explicitly permitting the collection of K-12, higher education, and workforce development data, with clear provisions for oversight and governance.[13] States like Washington have passed similar measures authorizing the exchange of child welfare, justice, and other data.[14] At the behest of integrated data system advocates, legislators in states like New Jersey and California have introduced narrower laws praising or authorizing specific integrated data system initiatives.[15] OPM believes it can continue to make progress over the next year through an interagency, collaborative process, without new legislation

[12] This report does not cover issues of consent, but this is a potential area for future attention. Many jurisdictions are now using what may be called a Universal Consent, in addition to the legal documents described previously. As an example, three different systems wish to share data to determine the "heavy users" of services and possibly a different way of providing services to result in better outcomes. Instead of a client or patient having to sign three different consents or authorizations or releases of information, one document is drafted that meets the legal requirements of each of the three systems, is written in plain English, and the system representative with the best and closest relationship with the client would explain the release and ask the client to sign it. This is efficient from a systemic viewpoint and avoids the client from having to sign three documents.

[13] The best research on this is available through Data Quality Campaign. See, for example, their profile on Maryland's statewide longitudinal data system law: *Maryland Using Data to Ensure Student Success in College and Careers.*

[14] Washington's HB 1541 (2016) links different agencies through data sharing and research agreements to determine educational and workforce outcomes related to juveniles in the justice system. The agencies mentioned include courts, the department of social and health services, and the superintendent of public instruction.

[15] New Jersey's S3220 (2016) established a process to integrate health and other data from publicly supported programs for population health research to create a statewide Integrated Population Health Database. California's AB 120 (2016) to "support the development of safe and secure data sharing between public education, social service, and research entities through the Silicon Valley Regional Data Trust as it pertains specifically to at-risk, foster, homeless, and justice-involved children and youth and their families, in order to better serve, protect, and improve the futures of these Californians."

at this time. Through its work with AISP and the groundwork laid by this report, Connecticut is on its way to developing a more streamlined process to navigate the legal limitations of data sharing, while upholding the principles of privacy and safety.

The Lamont Administration strongly supports improving data integration and use to improve government programs and services, oversight, and accountability. Through our work with AISP, OPM's data team, under the leadership of the Chief Data Officer, will be working with key experts and stakeholders to identify the best path forward for Connecticut to improve its data sharing processes and infrastructure. We look forward to updating the legislature with the results of this ongoing work through this annual report.

Appendix A: Federal and State Laws Impacting Data Sharing[16]

The following sections review key federal and state laws regarding data sharing. The review in each section is not exhaustive, but is intended to evolve over time as laws and regulations change and more information becomes available. The sections should serve as a reference to anyone interested in entering into interagency data sharing agreements. The reviews document not only the restrictions on data sharing from state and federal law, but also the multiple instances in which data sharing is encouraged or even mandated by the law.

The sections were identified based on areas that were either the focus of existing data sharing agreements, or based on the 'use cases' described earlier in the report.[17] In most cases, the identification of federal and state laws also drew on the agency responses to the survey summarized earlier in this report. The sections are organized around issue areas or types of services, and do not map one-to-one onto Connecticut executive branch agencies.

Social Services

Federal Laws

Title XIX of the Social Security Act
42 U.S.C. §§1396-1396v
42 CFR Subchapter C

51 U.S.C. §2011 et seq.
7 CFR §210 et seq.

Title IV-A of the Social Security Act
42 U.S.C. §601 et seq.
45 CFR §201 et seq.

42 U.S.C. §651 et seq.
45 CFR §301 et seq.

Medicaid

Title XIX of the Social Security Act established regulations for the Medicaid program[18], which provides funding for medical and health-related services for persons with limited income. Title XIX contains a number of provisions governing the acquisition, use, and disclosure of Medicaid enrollees' health information.

State participation in Medicaid is voluntary; each state designs and administers its own Medicaid program, funded jointly by the state and the federal government. Despite a state's relative autonomy to develop its own Medicaid program plan, Title XIX predicates federal approval of state plans on the

[16] This Appendix was prepared by OPM's consultant, Richard Gold.
[17] The Appendix does not review laws and regulations for data sharing in other areas – such as financial services – which could be considered for future reports.
[18] 42 U.S.C. §§1396-1396v

inclusion of certain provisions, and conditions federal financing of the program on the satisfaction of certain requirements.

The use and disclosure of health information must be restricted to purposes directly connected with the plan administration.[19] Medicaid program administration includes: 1) establishing eligibility; 2) determining the amount of Medical Assistance; 3) providing services for recipients; and 4) conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.[20]

The single state agency that administers the Medicaid program must have criteria specifying the conditions for release and use of information about applicants and recipients. The information for which the agency must have criteria to safeguard must include:

1. Names and addresses,
2. Medical services provided,
3. Social and economic conditions,
4. Agency evaluation of personal information,
5. Medical data, including diagnosis and past history of disease or disability, and
6. Any information received for verifying income eligibility and amount of medical assistance payments, of which information received from the Internal Revenue Service (IRS) or Social Security Administration (SSA) must be safeguarded pursuant to the requirements of those agencies.[21]

These criteria apply to all requests for information from outside sources, including governmental bodies, the courts, or law enforcement officials. Access to information concerning applicants or recipients must be restricted to persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the single state agency. The agency is prohibited from publishing names of applicants or recipients. Furthermore, whenever possible, the agency must obtain permission from the individual (or family under certain circumstances) before responding to a request for information from an outside source, unless the information is to be used to verify income, eligibility, and the amount of medical assistance payments.

Before information is requested from or released to another bureau or agency (not part of Medicaid program administration) to verify income, eligibility, and the amount of assistance, the Department must execute data sharing agreements with those agencies. Data sharing agreements are also required before the department may request information from or release information to other agencies to identify third-party resources. If an emergency situation prevents the agency from obtaining recipient consent prior to release, the agency must notify the individual or family immediately after supplying the information. Where a court issues a subpoena for a case record or for any agency representative to testify concerning an applicant or recipient, the agency must inform the court of the applicable statutory provisions, policies, and regulations restriction disclosure of information.

[19] 42 U.S.C. §1902(a)(7)(A); 42 U.S.C. §1396a(a)(7)(A)
[20] 42 CFR §431.302
[21] 42 CFR §431.306

Additionally, every provider enrolled in the Medicaid program must agree to keep complete records of the services furnished to Medicaid enrollees and to provide such information to the state upon request.[22] With regard to the transmission of data, states are required to operate an information retrieval system to electronically transmit data (including individual enrollee encounter data)[23] which must be capable of developing patient and provider profiles that provide information about the use of covered service and items.[24]

There must be a plan to evaluate the quality and appropriateness of the care and services furnished to Medicaid enrollee.[25] The state must implement pre- and post-payment claims review procedures that include review of patient data and the nature of the provided service.[26] The state must establish procedures for unnecessary utilization of services and ensuring that payments are consistent with efficiency, economy, and quality of care.[27] These procedures must include a screen and review process[28] for every inpatient admission[29] and a requirement that provider hospitals maintain a utilization program[30] that evaluates the medical necessity of all admissions.[31] If the state covers health home services, the plan must include methods for tracking avoidable hospital readmissions and calculating savings that result from improved care coordination and management.[32]

The State has flexibility in what it includes in its State plan dealing with improvements to care, care coordination and management, including but not limited to the interaction between traditional health care and services related to the "social determinants of health" (e.g. housing, food, etc.) in order to assess and minimize the unnecessary provision of Medicaid services.

Supplemental Nutrition Assistance Program (SNAP)

Often referred to as the Food Stamp law or as SNAP, the Supplemental Nutrition Assistance Program federal law safeguards the personally-identifiable information provided by applicants for, and recipients of, SNAP benefits. It does not, however, present any undue barriers to information sharing with other state human services systems and specifically gives an exception to the safeguards with Federal assistance programs and Federally-assisted state programs.[33]

By law, there is a close working relationship between the SNAP and Child Support Enforcement agencies because a custodial parent of a minor child is required to cooperate with all paternity and support matters to receive SNAP benefits, and a non-custodial parent is required to cooperate with the child support enforcement state agency to receive SNAP benefits.[34]

---

[22] 42 U.S.C. §1902(a)(27); 42 U.S.C. §1396a(27)
[23] 42 U.S.C. §1903(r)(1); 42 U.S.C. §1396b(r)(1)
[24] 42 U.S.C. §1903(r)(2)(A); 42 U.S.C. §1396b(r)(2)(A)
[25] 42 U.S.C. §1902(a)(33)(A); 42 U.S.C. §1396a(a)(33)(A)
[26] 42 U.S.C. §1902(a)(37)(B); 42 U.S.C. §1396a(a)(37)(B)
[27] 42 U.S.C. §1902(a)(30)(A); 42 U.S.C. §1396a(a)(30)(A)
[28] Note: The screen and review process must be based on criteria established by independent medical professions. 42 U.S.C. §1902(a)(30)(B)(i); 42 U.S.C. §1396a(a)(30)(B)(i)
[29] 42 U.S.C. §1902(a)(30)(B)(i); 42 U.S.C. §1396a(a)(30)(B)(i)
[30] 42 U.S.C. §1903(i)(4); 42 U.S.C. §1396b(i)(4)
[31] 42 U.S.C. §1861(k)(1); 42 U.S.C. §1395x(k)(l)
[32] 42 U.S.C. §1396n; 42 U.S.C. §1396n
[33] 51 U.S.C. §2020(e)(8)
[34] 51 U.S.C. §§2015(l)(i) and (m)(1)

Even if information from SNAP is permitted to be shared with other Federal assistance programs and Federally-assisted, means-tested programs for low-income individuals and families, notice must be given to food stamp applicants that information may be provided to other systems and its use by those other systems of the information.

Key components of the SNAP law and federal regulations regarding information sharing include:

- State SNAP agency must execute data exchange agreement with other agencies, specifying information to be exchanged and procedures used for the exchange.[35]
- Privacy statement required for all SNAP applications and re-certifications that information will be verified through computer matching programs and that information may be disclosed to other Federal and state agencies.[36]
- Privacy statement also must contain statement that the collection of information, including Social Security Number, of each household member is authorized by law and information will be used to determine eligibility through computer matching programs.[37]
- Allows for SNAP obtaining current support information directly from state agency in lieu of obtaining information from household.[38]
- State SNAP agencies must provide information to Child Support and SSI programs.[39]
- Use or disclosure of information obtained from food stamp program includes persons directly connected with the administration or enforcement of the programs which are required to participate in the state income and eligibility verification system (IEVS) to the extent the food stamp information is useful in establishing or verifying eligibility or benefit amount under those programs.[40]
- SNAP state agencies may exchange with state agencies administering other programs in IEVS information about food stamp households' circumstances which may be of use in establishing or verifying eligibility or benefits amounts under Food Stamps Program and those programs.[41]
- SNAP agencies may exchange IEVS information with these agencies in other states when determined that same objectives are to be met and these programs are TANF, Food Stamps, Medicaid, Unemployment Compensation, and any state program administered under Titles I, X, XIV (adult categories), or VVI (SSI) of the Social Security Act.[42]
- SNAP State agencies verify Social Security Numbers by submitting to SSA for verification.[43]

Thus, the SNAP federal statutory framework presents a balance of protecting the confidentiality of the information provided to the SNAP for eligibility or recertification purposes with the ability to provide the information to other Federal Assistance Programs and federally-assisted programs for low-income persons.

---

[35] 7 CFR §272.8(a)(4)
[36] 7 CFR §273.2(b)(4)
[37] 7 CFR §273.2(b)(4)(i)
[38] 7 CFR §272.8(a)(1)
[39] 7 CFR §272.8(a)(3)
[40] 7 CFR §272.8(a)(2)
[41] Id.
[42] Id.
[43] 7 CFR §273.2(f)(1)(v)

Temporary Aid to Needy Families (TANF)

Regarding the sharing of information between governmental agencies, TANF is an essential partner with other systems including but not limited to child support enforcement, the Food Stamp Program, employment assistance, child protective services, Medicaid, and Unemployment Compensation.[44] By sharing information about individuals' histories and experience between TANF and other systems, the state can measure its own success.

A key provision of the TANF program is state flexibility.[45] The state is independent of federal control and direction as to the operation of the TANF program except in the areas specifically mentioned in federal statute.[46] For example, the statute prescribes the requirement for work participation and with maximum time for assistance. The statute does not address information sharing by TANF with other state systems. Thus, the information that the state TANF program collects, how the state TANF program conducts its operations and program, and how the state TANF program shares information with other federally-funded and assisted state programs, is given great latitude under this federal law under the general requirements of The Privacy Act of 1974. (TANF may receive information from other systems that have their own confidentiality requirements and such requirements must be met regarding the specific data.)

Under TANF, there is the mandate to reach out to and share information with other systems. The law specifically discusses the TANF system developing relationships and information sharing processes with domestic violence programs, child support, law enforcement, Medicaid, Social Security, child care and foster care maintenance.[47] At the same time, it must take reasonable steps to restrict the use and disclosure of information about individuals and families applying for and/or receiving TANF benefits.[48]

> *A United States Governmental Accountability Office (GAO) report recommends increased data sharing with child welfare programs to improve access to benefits and services. Relative caregivers were of specific concern in the findings, recommending coordination efforts including collocating TANF and child welfare services and having staff from each agency work together to help relative caregivers' access services. The GAO reports that, although it would be beneficial, information and data sharing between TANF and child welfare does not occur consistently, hindering the relatives' access to available benefits. Half of the states reported obstacles to sharing data including but not limited to confidentiality and privacy concerns.*[49]

From the standpoint of federal barriers or prohibitions to information sharing of individual information, TANF is capable of collaborating with other state programs to determine the information to be shared, the legitimate governmental purpose for sharing, with whom and when to share the information, and the mechanism for protecting the information once shared.

Key components of the TANF law regarding information sharing include:

---

[44] 45 CFR §205.50(a)(1)(i)(A)
[45] 42 U.S.C. §602(a)(1)(A)(iv)
[46] 45 CFR §205.55(a)(5)
[47] 42 U.S.C. §602(a)(1)(A)(vi)
[48] 42 U.S.C. §602(a)(7)(A)(i)
[49] GAO, *TANF and Child Welfare Programs: Increased Data Sharing Could Improve Access to Benefits and Services,* GAO-12-2 (Washington, D.C.: Oct. 7, 2011)

- Permits the design of the TANF program to reach out to and work in partnership with other state systems, including but not limited to education, domestic violence and rape programs, child abuse and neglect, and teenage pregnancy prevention programs.[50]
- Permits aligning closely with the state's system that establishes paternity and child support systems as a condition for individuals to be eligible to receive TANF benefits (with certain exceptions).[51]
- To collaborate with the state's Medicaid system.[52]
- To provide information to Federal, state, or local law enforcement upon written request and, if provided specific information of a possible TANF recipient being a fugitive felon or probation or parole violator, to perform the official duties in locating or apprehending an individual.[53]
- To create and maintain individual responsibility plans and require recipients to perform appropriate functions, including but not limited to insuring that school-age children attend school, maintain certain grades and attendance, immunizations, attending parenting and money management classes, employment related activities, and/or undergo appropriate substance abuse treatment.[54]
- Provide quarterly disaggregated reports on families receiving TANF and SSI benefits.
- Provide quarterly disaggregated reports on families receiving TANF and subsidized housing, Medicaid, SNAP, or subsidized child care.
- Take reasonable steps to restrict the use and disclosure of information about individuals and families receiving TANF benefits.

Thus, the statutory framework presents a balance of protecting the information provided to the TANF program versus providing an efficient, effective and coordinated process yielding the maximum benefits to individuals. States must make decisions, based on its own laws, regarding when, why, with whom, and how to share TANF information with other federally-funded and assisted systems. Many states link data and information sharing within TANF, Food Stamp Program, and Medicaid, and also link TANF data to job opportunities, child care and basic skills, Unemployment Insurance benefits, and child support enforcement.

Child Support

Unless otherwise specifically authorized in Title IV-D of the Social Security Act[55], the personal information that the system collects is confidential and cannot be shared. One reason for this legislative mandate is the child support system's access to very sensitive and statutorily protected information, including but not limited to data from the Internal Revenue Service (IRS). The system requires strict security requirements. At the same time, the law provides interface requirement in its management system, for example, the state's plan for child support must include certain information sharing with TANF, Medicaid, SNAP, public housing, higher education (for unpaid student loans), the unemployment compensation system, and the foster care system.

States are also required to maintain statewide automated data processing and information retrieval systems.[56] Such automated data systems must be used for information comparison activities that shall include:

[50] 45 CFR §205.50(a)(1)(i)(A)
[51] 45 CFR §205.50(a)(1)(i)(A)
[52] 45 CFR §205.55(a)(5)
[53] 42 U.S.C. §608(a)(9)(A)(i) & (ii)
[54] 42 U.S.C. §608(b)(2)(A)(ii) &(v)
[55] 42 U.S.C §§651 et seq.
[56] 42 U.S. C. §454A

> Exchanging information with state agencies (of the State and other States) administering programs funder under part A (TANF) programs operated under a State plan approved under Title XIX (Medicaid), and other programs designated by the Secretary (of HHS) as necessary to perform State agency responsibilities under this part and under such programs.[57]

Subject to safeguards on privacy and information sharing, there can be access to records of other State and local government agencies **by** the child support system, including vital statistics, tax and revenue records, real and titled personal property, occupational and professional licenses, ownership and control of corporations, partnerships, and other business entities, employment security records, public assistance programs, motor vehicle department, and corrections.[58] The personally identifiable information is provided by other systems to the child support system, but the data exchange is not reciprocal. The information provided back from the child support system is not identifiable. The information is then safeguarded and maintained solely by the child support system unless separately verified from other, less secure systems or methods.

The Office of Child Support Enforcement (OCSE) with the U.S. Department of Health and Human Services maintains the Federal Parent Locator Service (FPLS), which includes the National Directory of New Hires (NDNH) located at the Social Security Administration's (SSA) National Computing Center (NCC) and information from the State Directory of New Hires (SDNH), as well as the Federal Case Registry (FCR). The Office of Child Support Enforcement enters into Memorandums of Understanding (MOU)/Computer Matching Agreements (CMA) with federal or state agency that is authorized to receive FPLS information, including data from the NDNH. Authorized data users are primarily state child support agencies and those federal and state needs-based programs specified by statute. The MOU/CMA specifies the purpose for sharing information, the legal authority, the permitted purposes, the information that will be compared, the specific data elements that will be disclosed, the security safeguards required for the recipient agency to store and process NDNH data, and the expected results of the match. The NDNH also contains information from the Multistate Financial Institution Data Match (MSFIDM) and the State Financial Institution Data Match (FIDM), both of which contains highly confidential, personal information.

> *"Our most vulnerable children, those in the child welfare system, need an extra hand to help them thrive in the face of difficult circumstances. Perhaps surprisingly to some, that extra helping hand can come from the child support community. When a new home, temporary or permanent, is needed for a child, one of the first places child welfare workers look is to other family members who might be able to care for the child. Child support can be a tremendous resource for locating the child's other parent, usually the father, whose contact information may not be available from the child's mother. If the child's family has a current or former welfare case, if the parents have been divorced, if paternity has been established or if the child is on Medicaid, the child support program probably has information about the child's other parent. It is worth the time and effort for child welfare and child support agencies to build relationships and develop procedures to make sure that, when appropriate, fathers and other paternal kin have the opportunity to take responsibility for their children in need."*[59]

---

[57] 42 U.S.C. §654a(f)(3)

[58] 42 U.S.C. §666(c)(1)(D)(i)

[59] Vicki Turetsky, Commissioner, Office of Child Support Enforcement, Administration for Children and Families, U.S. Department of Health and Human Services, QIC News, National Quality Improvement Center on Non-Resident Fathers and the Child Welfare System, Quarterly Newsletter, Summer 2009, page 1.

State Laws

C.G.S. §17b-90

State law basically mirrors the federal laws in that it also prohibits any person to "solicit, disclose, receive or make use of, or authorize, knowingly permit, participate in or acquiesce in the use of, any list of the names of, or any information concerning, persons applying for or receiving assistance from the Department of Social Services or persons participating in a program administered by said department…"[60]

Child Welfare

Federal Laws

Title IV-E of the Social Security Act, as amended
42 U.S.C. §670 et seq.

Family First Prevention Services Act
Bipartisan Budget Act of 2018 (H.R. 1892)

Title IV-B of the Social Security Act, as amended
42 U.S.C. §401 et seq.; 45 CFR §1357

Child and Family Services Improvement and Innovation Act
42 U.S.C. §1305 et seq.

Fostering Connections to Success and Increasing Adoptions Act of 2008
42 U.S.C. §627 et seq.

Comprehensive Child Welfare Information System (CCWIS)
45 CFR §§1350-1355.59

Today, the child welfare system must be operated as a data-driven approach to services and supports. In 2018, the Children's Bureau published a guide to child welfare systems on how to achieve this goal.[61] In this guide, the argument is made that when multiple service systems are working with the same family, the agencies, systems, and organizations should work together to coordinate systems to be holistic and family-centric and to be more efficient and effective in working with the family. This is true at all stages of the child welfare continuum, from stabilization of an intact family, to the child, the child's family, and the resource family if a child is taken into custody, to reunification or to another permanency goal, and to a teen or young adult transitioning out of foster care into adulthood.[62] The guide further lists the necessary services, which include education, health, behavioral health, mental health, and substance use disorder treatment services.[63]

[60] C.G.S. §17b-90
[61] Capacity Building Center for States. (2018). *A Data-driven approach to service array guide.* Washington, DC: Children's Bureau, Administration for Children and Families, U.S. Department of Health and Human Services.
[62] Id. at 4.
[63] Id. at 5.

The Child and Family Services Improvement and Innovation Act of 2006, as amended in 2011,[64] amends both title IV-B and IV-E of the Social Security Act to enable information sharing between the child welfare system and other health and human systems. In conjunction with the Fostering Connections to Success and Increasing Adoptions Act of 2008[65], also amending title IV-E, these two laws made clear that the child welfare system must work in partnership with other systems and share data and information with the educational, health, early childhood, and behavioral health systems.

The laws required the child welfare systems to develop protocols for the appropriate use and monitoring of psychotropic medications and a plan for ongoing oversight and coordination of health care services for children in foster care, including but not limited to mental health services. The child welfare system had to work with the State Medicaid agency, pediatricians, other health care and child welfare experts to develop the plan and the monitoring process, which had to include the oversight of prescription drugs for children and youth in foster care, and how the child welfare agency will consult and involve physicians and other professionals in assessing the health and well-being of children in foster care in determining appropriate medical treatment.[66] Furthermore, the child welfare system was mandated to address the developmental needs of children in foster care who have not attained 5 years of age.[67]

Additionally, the Fostering Connections Act mandated that the child welfare system develop with the Medicaid system, and in consultation with pediatricians, and other health care and child welfare experts, a plan for the oversight and coordination of all health care services for any child in foster care placement, including a coordinated strategy to identify and respond to the health care needs of these children and youth, including but not limited to their mental health and dental needs. In addition to the continuing oversight of psychotropic medication for children in foster care, the plan had to outline the following:

- Schedule of initial and follow-up health screenings that meet reasonable standard of medical practice;
- How health needs identified through screenings are monitored and treated;
- How medical information is updated and appropriately shared;
- Steps to ensure continuity of health care services, including the establishment of a medical home for every child in foster care; and
- How the child welfare system consults with and involves physicians or other appropriate medical or non-medical professionals in assessing the health and well-being of children in foster care and in determining appropriate medical treatment.[68]

Regarding the educational needs of children in foster care and data sharing between the child welfare and education systems, this federal law required a written educational stability plan for each child in foster care to assure that the foster care placement takes into account the appropriateness of the current educational setting and proximity to the school where the child is enrolled at the time of placement. The child welfare agency needed to coordinate with the appropriate local educational

[64] 42 U.S.C. §§621 et seq.
[65] 42 U.S.C. §§621 et seq.
[66] 42 U.S.C. §622(b)(15)
[67] 42 U.S.C. §622(b)(18)
[68] 42 U.S.C. §622(b)(15)(A)

agencies to ensure that a child can remain in the school in which she/he is enrolled at the time of placement unless contrary to the child's best interests. If a child in foster care had to change schools due to the placement, the child must be provided immediate and appropriate enrollment in the new school with all educational records supplied to the new school. The law made clear that educational stability applied to each child's initial placement in foster care as well as any subsequent placements during the child's stay in foster care.[69]

Last, the Child and Family Services Improvement and Innovation Act mandated that data must be interoperable between the systems and incorporate interoperable standards developed and maintained by intergovernmental partnerships, such as the National Information Exchange Model (NIEM).[70]

The last set of child welfare laws to be discussed is the recent child welfare legislation of both the Comprehensive Child Welfare Information System (CCWIS)[71] final rule and the Family First Prevention Services Act,[72] both reflect the need and promotion of data sharing with other agencies and systems. The CCWIS final rule (optional to states) requires, if practicable, title IV-E agencies to exchange data with other human services and health agencies, education systems, and child welfare courts. This is a change from the previous Statewide and Tribal Automated Child Welfare Information Systems (S/TACWIS), reflecting that the child welfare practice and technology have changed considerably. Data exchanges will help coordinate services, be more efficient by reducing or eliminating redundancies, improve client outcomes, and improve data quality. Taking even a more drastic step, the Family First Prevention Services Act permits states and territories to use title IV-E funds (previously limited to help with the costs of foster care maintenance for eligible children and other related placement costs) for prevention services, including evidence-based mental health programs, substance use disorder prevention and treatment, and in-home parent skill-based programs. Both of these legislative and regulatory changes reinforce the need for child welfare services to work with and to share data with other serving systems and agencies.

State Laws

C.G.S.A. § 17a-101a-114b
C.G.S.A. § 45a-743-757
C.G.S.A. § 813a
C.G.S.A. § 46b-124
C.G.S.A. § 17a-28

Connecticut's child welfare laws generally state that all information is confidential. This includes case records of individuals, families that are served by the Department and foster parents or other individuals who receive services such as those who are subject of investigations and administrative proceedings.[73] Sharing of data is only permitted when the subject involves another agency. For example, the Commissioner of Children and Families, or the commissioner's designee, must notify the State's Attorney when a mandatory reporter fails to make a report[74] or a person makes a false report.[75]

[69] 42 U.S.C. §675(1)(G)
[70] 42 U.S.C. §629m(b)(2)
[71] Social Security Act §§474(a)(3)(C) & (D); 474(c)
[72] Public Law (P.L.) 115-123
[73] C.G.S.A. § 17a-28
[74] C.G.S.A. § 17a-101a(c)
[75] C.G.S.A. § 17a-101e; C.G.S.A. § 17a-103

Pursuant to the federal Child and Family Services Improvement and Innovation Act and the federal Preventing Sex Trafficking and Strengthening Families Act, the Commissioner must also report to the State's Attorney when there is evidence of identity theft of a child in the custody of the state's child welfare system.[76] Similarly, child welfare shares information with law enforcement when a report of child abuse involves an allegation of sexual abuse or serious physical abuse, including but not limited to a report that a child has died, been sexually assaulted, suffered brain damage or loss or serious impairment of a bodily function or organ, been sexually exploited, or has suffered serious non-accidental physical injury.[77] When a report concerns a school employee, the report is shared with the Department of Education and the state licensing agency (if person is licensed).[78]

Child welfare shares information when it coordinates its investigation of reports of child abuse and child neglect in order to minimize the number of interviews of any child[79] or as part of a multidisciplinary team[80]; and when it works with other agencies to prevent, identify, and investigate child abuse and neglect, including but not limited to law enforcement, courts, schools and other state agencies providing human services.[81] If a child exhibits developmental or social-economic delays pursuant to screenings of children from birth to three years old to the Help Me Grow prevention program under the Office of Early Childhood.[82]

There are also state laws regarding the availability and confidentiality of adoption records. These laws set forth the procedure regarding the sharing of information with the parties involved in such proceedings, but not to other persons or agencies.[83]

Court records of cases of juvenile matters are confidential and for the use of the court, but are open to inspection or disclosure to any third party, including researchers commissioned by a state agency, upon an order of the appropriate court.[84] These records are available without a court order to the parties in the proceedings, including the attorneys of the parties, as well as the Department of Children and Families. Court records of juvenile matters involving delinquency proceedings may be disclosed upon a court order to any person with a legitimate interest in the information; such information shall not be further disclosed except as authorized by a subsequent court order.[85]

Child Abuse

Federal Laws

Child Abuse Prevention and Treatment Act
42 U.S.C. 5101, et seq.

In general, the Child Abuse Prevention and Treatment Act (CAPTA) requires a State to preserve the confidentiality of all child abuse and neglect reports and records in order to protect the rights of the

[76] C.G.S.A. § 17a-114b
[77] C.G.S.A. § 17a-101b
[78] C.G.S.A. § 17a-101c; C.G.S.A. § 17a-101g(a); C.G.S.A. § 17a-101i; C.G.S.A. § 17a-101p
[79] C.G.S.A. § 17a-101h
[80] C.G.S.A. § 17a-106(a). The State's Child Advocate also has access to any information necessary to carry out its office's responsibilities. In fact, the Child Advocate has subpoena power to access such information
[81] C.G.S.A. § 17a-106
[82] C.G.S.A. § 17a-106(e)(b)
[83] C.G.S.A. § 45a-743
[84] C.G.S.A. § 46b-124(b)
[85] C.G.S.A. § 46b-124(e)

child and the child's parents or guardians.[86] However, CAPTA allows the State to release information to certain individuals and entities.

The State may share confidential child abuse and neglect reports and records that are made and maintained with any of the following:

1. Individuals who are the subject of a report;[87]
2. Grand jury or court, when necessary to determine an issue before the court or grand jury[88]; and
3. Other entities or classes of individuals who are authorized by statute to receive information pursuant to a legitimate state purpose.[89]

Additionally, States have the option to allow public access to court proceedings that determine child abuse and neglect cases, so long as the State, at a minimum, can ensure the safety and well-being of the child, parents and families.[90]

The State must provide certain otherwise confidential child abuse and neglect information to the following:

1. Any Federal, State, or local government entity, or any agent of such entity, that has a need for such information in order to carry out its responsibilities under the law to protect children from abuse and neglect;[91]
2. Child abuse citizen review panels, if such panels are established to comply with this law;[92]
3. Public disclosure of the findings or information about the case of child abuse or neglect that results in a child fatality or near fatality;[93] and
4. Child fatality review panels.[94]

Authorized recipients of confidential child abuse and neglect information are bound by the same confidentiality restrictions as the child protective services agency. Thus, recipients of such information must use the information only for activities related to the prevention and treatment of child abuse and neglect. Further disclosure is permitted only in accordance with this law.

States do have the authority to release otherwise confidential child abuse and neglect information to researchers for the purpose of child abuse and neglect research in either of two ways:

1. The child protective services agency may contract with a researcher, thereby making the researcher its "agent"; or
2. States may statutorily authorize release of such information to researchers as a legitimate State purpose, since research involving data in child protective services records can provide

[86] 42 U.S.C. 5106(b)(2)(B)(viii)
[87] 42 U.S.C. 5106(b)(2)(B)(viii)(I)
[88] 42 U.S.C. 5106(b)(2)(B)(viii)(V)
[89] 42 U.S.C. 5106(b)(2)(B)(viii)(VI)
[90] 42 U.S.C. 5106(b)(2)
[91] 42 U.S.C. 5106(b)(2)(B)(ix)
[92] 42 U.S.C. 5106(c)(5)(A)
[93] 42 U.S.C. 5106(b)(2)(B)(x)
[94] 42 U.S.C. 5106(b)(2)(B)(x)

important information that will help government officials plan programs for abused and neglected children and develop future policy directions.

Mental Health

Federal Laws

42 U.S.C. §1320d

45 CFR Part 160 and Subparts A and E of Part 164

There are no specific federal laws dealing with mental health. Instead, we again turn to the Health Insurance Portability and Accountability Act (HIPAA),[95] which mandates privacy and security safeguards for medical information about a person's health status, care, or payment for care, all of which are considered "protected health information" (PHI).[96] The law applies to all covered entities and defines a "covered entity" as individuals or entities that transmit protected health information for transactions for which the federal government has adopted standards [97] Transactions include transmission of healthcare claims, payment and remittance advice, healthcare status, coordination of benefits, enrollment and disenrollment, eligibility checks, healthcare electronic fund transfers, and referral certification and authorization. Covered entities include health plans, healthcare providers, and healthcare clearinghouses. Health plans include government programs that pay for health care, such as Medicaid and Medicare, and the military and veterans' health care programs.

Protected health information (PHI) is health data created, received, stored, or transmitted by a covered entity and their business associates in relation to the provision of healthcare, healthcare operations, and payment for healthcare services.[98] Such information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to the individual, or the payment for the provision of health care to an individual that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium.

PHI includes all "individually identifiable health information", including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or to provide healthcare services or coverage.

HIPAA also provides regulations describing the circumstances that covered entities are permitted, but not required, to use and disclose PHI for certain activities without first obtaining the patient's authorization. Such activities include payment, treatment, and health care operations.[99] "Treatment" generally means the provision, coordination, or management of health care and related services among health care providers. "Health care operations" include certain administrative and quality improvement activities of the covered entity that are necessary to operate a business and to support the core functions of treatment. Case management and care coordination are noted as health care operations.

---

[95] 45 CFP Part 160 and Subparts A and E of Part 164.
[96] 45 CFR §160.103
[97] 45 CFR §160.130
[98] 45 CFR §160.103
[99] 45 CFR §164.501

A covered entity could be the entire organization or a hybrid entity. A hybrid entity under HIPAA is a single legal entity that is a covered entity whose business activities include both covered and non-covered functions and that designates certain units as health care components and therefore covered by HIPAA. Normally, if any activities performed by an organization are covered by HIPAA, then the entire organization must comply with HIPAA regulations as to privacy[100] and security. [101] A properly drafted and enforced hybrid entity policy can help an organization avoid the global application of the HIPAA rules. Instead, the organization draws "invisible" lines throughout the organization. Only the designated components will be covered under HIPAA and only such components have the right to use, maintain, access or transmit PHI. Therefore, the hybrid HIPAA organization limits the application of the HIPAA-required divisions, including but not limited to sharing data when necessary.

The HIPAA Privacy Rule permits the covered entity to disclose protected health information without individual authorizations within the entity for its own health care operations purposes. If the disclosure is for health care operations, the Privacy Rule requires that: (i) each entity (or part of the entity in this situation) has or had a relationship with the individual whose PHI is involved; (ii) the PHI pertains to that relationship; and (iii) the disclosure is for specific activities within the definition of health care operation.[102] Case management and care coordination are among the specific listed activities.[103] As for mental health services, generally, HIPAA treats mental health information the same as other health information. Some examples of the types of mental health information that may be shared are medication prescription and monitoring, modalities and frequencies of treatment furnishes, and summaries of diagnosis, functional status, treatment plans, symptoms, prognosis, and progress to date. An exception to sharing mental health information for health care operations purposes or treatment purposes without obtaining an individual's authorization deals with psychotherapy session notes.[104] For the disclosure of psychotherapy session notes, HIPAA requires the patient to sign an authorization, whether for treatment, case management, care coordination or any other purpose.[105]

State Laws

C.G.S.A. § 52-146

Under C.G.S. § 52-146e(a), all mental health communications and records shall be confidential. No person may disclose or transmit any communications and records or the substance or any part or any resume thereof which identifies a patient to any person, corporation, or governmental agency without the consent of the patient or his authorized representative.[106] For example, "A person must receive consent from a patient in order to transmit any portion of communications and records to any person, corporation, or government agency." Any consent given to waive the confidentiality shall specify to what person or agency the information is to be disclosed and to what use it will be put. Each patient shall be informed that his refusal to grant consent will not jeopardize his right to obtain present or future treatment, except where disclosure of the communications and records is necessary for the treatment.[107] The patient may withdraw any consent at any time in writing addressed to the person or

[100] 45 CFR Part 160 and Subparts A and E of Part 164
[101] 45 CFR Part 160 and Subparts A and C of Part 164
[102] 45 CFR §§164.502(a)(1)(ii); 164.506(c)(4)
[103] 45 CFR §164.501
[104] 45 CFR §164.501
[105] 45 CFR §164.508
[106] C.G.S.A. § 52-146e(a)
[107] C.G.S.A. § 52-146e(b)

office in which the original consent was filed. Withdrawal of consent shall not affect communications or records disclosed prior to the notice of the withdrawal.[108]

Consent is not required for disclosure of mental health information in the following situations:

1. For diagnosis and treatment;[109]
2. For involuntary commitment;[110]
3. For collection of fees for psychiatric services;[111]
4. To court when made in the course of a psychiatric examination ordered by court;[112]
5. To civil court when patient introduces his mental condition as an element of his claim or defense;[113]
6. To Commissioner of Public Health in connection with any inspection, investigation, or examination of an institution or the Commissioner of Mental Health and Addiction Services in connection with any inspection, investigation or examination of an institution;[114]
7. To the family member of a homicide victim if the patient was found not guilty by reason of insanity for the crime;[115] or
8. If provider of behavioral health services that contracts with the Department of Mental Health and Addiction Services requests payment.[116]

A person engaged in research may have access to mental health communications and records which identify patients where needed for such research, if the person's research plan is first submitted to and approved by the director of the mental health facility or his designee.[117] The communications and records shall not be removed from the mental health facility. Coded data or de-identified data may be removed from a mental health facility, provided the key to the code shall remain on the premises of the facility.[118] The mental health facility and the person doing the research shall be responsible for the preservation of the anonymity of the patients of the patients and shall not disseminate identified data.[119]

All written communications of records disclosed to another person or agency shall contain the following statement:

> The confidentiality of this record is required under chapter 899 of the Connecticut general statutes. This material shall not be transmitted to anyone without written consent or other authorization as provided in the aforementioned statutes.

A copy of the consent form specifying to whom and for what specific use the communication or record is transmitted or a statement setting forth any other statutory authorization for transmittal and the

[108] C.G.S.A. § 52-146e(c)
[109] C.G.S.A. § 52-146f(1)
[110] C.G.S.A. § 52-146f(2)
[111] C.G.S.A. § 52-146f(3)
[112] C.G.S.A. § 52-146f(4)
[113] C.G.S.A. § 52-146f(5)
[114] C.G.S.A. § 52-146f(6)
[115] C.G.S.A. § 52-146f(7)
[116] C.G.S.A. § 52-146f(8)
[117] C.G.S.A. § 52-146g(a)
[118] C.G.S.A. § 52-146g(g)
[119] C.G.S.A. § 52-146g(c)

limitations imposed thereon shall accompany such communication or record. In cases where the disclosure is made orally, the person disclosing the information shall inform the recipient that such information is governed by the provisions of this statute.

In addition, state law requires that the Commissioner of Mental Health and Addiction Services is responsible for the coordination of all activities in the state relating to substance use disorders and treatment, including activities of the Departments of Children and Families, Correction, Public Health, Social Services and Veterans' Affairs, the Judicial Branch and any other department or entity providing services to persons with substance use disorders.[120]

Drug and Alcohol Use Disorders

Federal Laws

42 U.S.C. §290dd-2

42 CFR Part 2

The overall purpose of the strict Confidentiality of Substance Use Disorder Patient Records Act[121] is to remove the fear that privacy and confidentiality will be compromised by reason of the availability of the patient's records and therefore the patient does not seek treatment.[122] Thus, the confidentiality rules apply to records of the identity, diagnosis, prognosis, or treatment of any patient maintained in the performance or activity relating to substance abuse education, prevention, treatment, training, rehabilitation or research and in the performance of any program or activity relating to alcoholism or alcohol abuse education, training, treatment, rehabilitation, or research conducted, regulated, assisted, or funded directly or indirectly by the federal government.[123] Even if the patient authorizes the release of information with a written consent, meeting the requirements listed below, it is not mandatory for the facility to comply; instead, the language is permissive in nature and not mandatory.[124]

If a patient consents in writing that information about her/his substance use disorder be shared, the federal regulations make clear what the consent must include, that being:

1. Name of Patient;
2. Specific name(s) or general designation(s) of the part 2 program(s), entity(ies), or individual(s) permitted to make disclosure;
3. How much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed;
4. Name(s) of the individual(s) to whom a disclosure is to be made; or entities with a treating provider relationship with patient; or entities without a treating provider relationship with patient;
5. Purpose of disclosure (with limitation that information is what is necessary to carry out the stated purpose);

[120] C.G.S.A. § 17a-451
[121] 42 U.S.C. §290dd-2
[122] 42 CFR §2.2(B)(2)
[123] 42 U.S.C. §290dd-(3)(a) and §290ee-(3)(a)
[124] 42 CFR §2.13(a)

6. Statement that consent is subject to revocation at any time except to the extent that the part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it;
7. Date, event, or condition upon which the consent will expire if not revoked before (and such is no longer than reasonably necessary to serve the purpose for which it is provided);
8. Signature of patient/person authorized to given consent (e.g. minor; incompetent; deceased);
9. Date on which consent is signed;[125] and
10. One of the following written statements:

    a. This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whom information is being disclosed or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with substance use disorder; or
    b. 42 CRF prohibits unauthorized disclosure of these records.

Again, it must be stated that even with a written consent meeting all of the above requirements, the 42 CFR part 2 provide "may" disclose, not "shall" disclose, in accordance with the consent.[126] With a properly written and signed consent, the substance use disorder provider may provide information to prevent multiple enrollments (with conditions)[127] and to elements of the criminal justice system which have referred patients.[128]

The exceptions to disclosing substance use disorder information is much more limiting than in other federal legislation.

1. For medical emergencies. Immediately following disclosure, the part 2 program must document in the record the name and affiliation of the medical personnel to whom disclosure was made, name of the person making the disclosure, date and time of the disclosure, and nature of the emergency.[129]

2. Research. Patient identifying information may be disclosed for the purpose of conducting scientific research if the director or designee makes a determination that the recipient of the patient identifying information:

    a. If a HIPAA-covered entity, has obtained and documented authorization from patient or a waiver or alteration of authorization consistent with HIPAA (45 CFR 164.508 or 164.512(i), as applicable; or

[125] 42 CFR §2.31(a)(1)-(9)
[126] 42 CFR §2.33(a)
[127] 42 CFR §2.34
[128] 42 CFR §2.35
[129] 42 CFR §2.51

b. If subject to U.S. Department of Health and Human Services regulations regarding the protection of human subjects (45 CFR part 46), either provides documentation that the researcher is in compliance with the requirements of the HHS regulations (including informed consent or waiver of consent (45 CFR 46.111 and 46.116) or that research qualifies for exemption under HHS regulations (45 CFR 46.101(b)); or
c. If both a HIPAA-covered entity and subject to HHS regulations, it has met one or the other; and
d. If neither HIPAA-covered entity nor subject to HHS regulations regarding the protection of human subjects, this section does not apply.

State Laws

C.G.S.A. § 17a-688

All substance abuse treatment records are confidential and privileged to the patient and may only be disclosed according to this statute and 42 CFR part 2.[130] No person, hospital or treatment facility may disclose or permit the disclosure of, nor may the department disclose or permit the disclosure of, the identity, diagnosis, prognosis or treatment of any such patient that would constitute a violation of federal statutes concerning confidentiality of alcohol or drug patient records.[131] Substance use disorder treatment information may be used or disclosed by the Commissioner of Mental Health and Addiction Services for research, audit, or program evaluation purposes, provided that the information is not used in a way that discloses patient identity.[132] Last, disclosure is permitted by court order if a court holds a hearing and determines that there is cause for disclosure.[133]

Education

Federal Laws

20 U.S.C. §1232g
34 CFR §99

The confidentiality requirements regarding education data are contained in Section 444 of the General Education Provisions Act commonly referred to as the Family Educational Rights and Privacy Act (FERPA),[134] and its implementing regulations.[135] FERPA sets out requirements for the protection of students' education records and provides parents and eligible students[136] (a student who reaches the age of 18 years or attends a school beyond the high school level) certain rights with respect to the student's education records, including the right to maintain the confidentiality of the education information. This law applies to an educational agency or institution to which funds have been made available under any federally-administered Department of Education program if: (1) the educational institution provides educational services or instruction, or both, to students; or (2) the educational agency is authorized to direct and control public elementary or secondary, or post-secondary

[130] C.G.S.A. § 17a-688(a) & (c)
[131] C.G.S.A. § 17a-688(a) & (c)
[132] C.G.S.A. § 17a-688
[133] C.G.S.A. § 17a-688
[134] 20 U.S.C. 1232g
[135] 34 CFR Part 99.
[136] An eligible student is one to whom the rights accorded to parents under FERPA are transferred. 34 CFR §99.5(a)(1). An eligible student is 18 years of age or older or attends a postsecondary education institution. 34 CFR §99.3.

educational institutions.[137] ("Educational agencies or institutions" that receive funds from programs administered by the U.S. Department of Education generally include public schools, school districts (or "local education agencies (LEAs)), and postsecondary institutions, such as colleges and universities. They can also include pre-K programs if the program receives federal Department of Education funds. If private and parochial schools receive such funding, they are also subject to FERPA.)

FERPA requires that all "personally identifiable information" (PII) remain confidential unless the disclosure is pursuant to one of the enumerated exceptions to the rule. PII includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.[138] "Disclosure" is defined as permitting "access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record."[139] On an annual basis, the educational agency or institution must establish criteria of FERPA rights and disclosure conditions and provide such written notice to all parents and eligible children.[140]

Basically, FERPA states that personally identifiable information (PII) contained in education records cannot be disclosed without the consent of the child's parent or eligible student. The requirements of a consent must include the following:

1. Name of student,
2. Specify the records that may be disclosed,
3. State the educational agency or institution disclosing the information,
4. Identify the party or class of parties to whom the disclosure may be made,
5. Purpose of the disclosure,
6. Signature of parent or individual with authority to consent (electronic signature must identify and authenticate a particular person as the source of the electronic consent and indicate approval of the electronic consent), and
7. Date of signature.[141]

When a disclosure is made by the school or educational institution pursuant to a consent, if a parent or student who is 18 years old or in a post-secondary education program, the educational agency or institution shall provide such person with a copy of the disclosed records.[142]

There are a number of exceptions to the FERPA rule of confidentiality requiring an individual consent from the parent or eligible student. An exception to the FERPA confidentiality rule requiring consent is the disclosure of "Directory Information."[143] An educational agency or institution must have a written policy of the information designating the data contained in the directory information and such information may only include PII that is generally not considered harmful or an invasion of privacy if disclosed. The policy must clearly detail the categories of PII that have been designated as directory information, the parent's or eligible student's right to refuse to let any or all of these types of PII be

[137] 34 CFR §99.1
[138] 34 CFR §99.3
[139] 34 CFR §99.3
[140] 34 CFR §99.7(a)(2) and (a)(3)
[141] 34 CFR §§99.30(a) and (b); 99.33
[142] 34 CFR §99.30(c)
[143] 34 CFR §99.3

designated as directory information, and the period of time that the parent or eligible student has to "opt out" of such a disclosure of directory information.

Typically, "directory information" includes but is not limited to, student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, grade level, enrollment status (e.g., full-time or part-time, undergraduate or graduate), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, most recent educational agency or institution attended, and dates of attendance.[144] An educational agency or institution must give prior public notice to parents of attending students prior to disclosing directory information. But the school does not have to notify a parent or eligible student individually.[145] And there are a number of conditions where parents or eligible students do not have the right to "opt out" of the disclosure of directory information.[146] Last, FERPA does not require educational agencies or institutions to record disclosures of appropriately designated directory information.[147]

Another exception under FERPA is disclosure of confidential education information to a school official[148], including but not limited to teachers within the educational agency or institution, whom the agency or institution has determined to have legitimate educational interests.[149] School officials with legitimate educational interests may also include a contractor, consultant, volunteer, or other party to whom an educational agency or institution has outsourced services or functions, provided the outside party:

1. Performs an institutional service or function for which the educational agency or institution would otherwise use employees;
2. Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
3. Complies with the requirements of FERPA governing the use, maintenance, and re-disclosure of PII from education records.[150]

If an educational agency or institution has a policy of disclosing education records to school officials, the educational agency or institution must include in its annual notification of FERPA rights the criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.[151] An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those educational records in which they have legitimate educational interests. Additionally, an educational agency or institution that does not use physical or technological access controls must ensure that it has an effective administrative control for access to the education records and that it remains in compliance with the legitimate educational interest requirement.[152] Finally, FERPA does not require educational agencies and institutions to record re-disclosures of PII from education records to school officials.[153]

[144] 34 CFR §99.3
[145] 34 CRR §99.37
[146] 34 CFR §§99.31(a)(11); 99.37
[147] 34 CFR §99.32(d)(4)
[148] 34 CFR §99.31(a)(1)
[149] 34 CFR §99.31(a)(1)(i)(A)
[150] 34 CRF §99.31(a)(1)(i)(B)
[151] 34 CFR §99.7(a)(3)(iii)
[152] 34 CFR §99.31(a)(1)(ii)
[153] 34 CFR §99.31(a)(1)

For research purposes, there is a studies exception requiring individual consents to share education information. FERPA permits the disclosure of PII to organizations conducting studies for, or on behalf of, educational agencies or institutions to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction.[154] The educational agency or institution may disclose PII if the disclosing educational entity enters into a required written agreement[155] (including but not limited to a memorandum of understanding or data sharing) with the organization conducting the study, the study does not permit identification of individual parents and students by anyone other than representatives of the organization with legitimate interests in the information, and the information is destroyed when no longer needed for the study.[156]

In addition to the above, another exception is for audit or evaluation purposes. The disclosure from education records must be to: (a) audit or evaluate a Federal or State-supported education program; or (b) enforce or comply with Federal legal requirements related to the program. The receiving entity must be a State or local educational authority or other FERPA-permitted entity or must be an authorized representative of a State or local educational authority or other FERPA-permitted entity. The party disclosing the personally identifiable information (PII) from education records must enter into a written agreement to designate anyone other than its employee or its authorized representative (each new audit, evaluation, or enforcement effort requires an agreement) and is responsible for using reasonable methods to ensure to the greatest extent practicable that the authorized representative: (1) uses the PII only for the authorized purpose; (2) protected the PII from further unauthorized disclosures or other uses; and destroys the PII when no longer needed for the authorized purpose and in accordance with any specified time period set forth in the written agreement.[157]

In addition to the above, there are a number of exceptions where education record information may be disclosed without prior consent, including:

1. Other school officials within the agency/institution whom the agency/institution has determined to have legitimate educational interests;
2. Contractor, consultant, volunteer, or other party whom an agency/institution has outsourced institutional services or functions may be considered a school official;
3. Educational agency/institution where student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for the purposes related to the student's enrollment or transfer;
4. Particular authorized government officials;
5. In connection with financial aid;
6. Juvenile justice system and the system's ability to effectively serve the student whose records are released;
7. Organizations conducting studies for, or on behalf of, educational agencies/institutions to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (improve instruction);
8. Accrediting organizations to carry out their accrediting functions;
9. Parents of a dependent child or a student who is not an eligible student;

[154] 34 CFR §99.31(a)(6)
[155] 34 CFR §99.31(a)(6)
[156] 34 CFR §99.31(a)(6)(iii)(C)
[157] 34 CFR §99.35

10. Comply with a judicial order or lawfully submitted subpoena;
11. Health of safety emergency;
12. To victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense; and
13. De-identified records and information (removal of all personally identifiable information).[158]

On January 14, 2013, the Uninterrupted Scholars Act (USA), Pub. L. No 112-278, was signed into law creating another FERPA exception to general requirement of individual consent and permitting the educational agency or institution to disclose education records of students to a state or local child welfare agency or tribal organization (child welfare agency) authorized to access a student's case plan when such child welfare agency is legally responsible for the care and protection of the student. There were many studies issued and convenings held to discuss the educational outcomes for children in foster care, resulting in the passage of this federal legislation amending FERPA and adding another exception. While not mandatory, this FERPA exception was enacted to permit, encourage and assist educational agencies or institutions to share PII education information and work together with child welfare agencies to improve the educational outcomes of children in foster care.

The USA exception also amended a notice requirement that generally applies when a disclosure is made pursuant to a lawfully issued subpoena or judicial order. Specifically, when an educational agency or institution must provide written notice to a parent or eligible student before complying with the subpoena or judicial order, such notice requirement is not applicable when the parent is a party to a state court proceeding regarding child abuse and neglect (as defined in the Child Abuse Prevention and Treatment Act (CAPTA)[159]) or dependency matters and the judicial order or subpoena is issued in the context of such proceeding. With the passage of the USA, in conjunction with the FERPA studies exception, jurisdictions throughout the county now have the legal ability to share educational information with child welfare agencies.

State Laws

C.G.S.A. § 10-15b
C.G.S.A. § 10-234bb
C.G.S.A. § 10-234cc
C.S.G.A. § 10-234dd
C.S.G.A. § 10-10a(b)
C.S.G.A. § 19a-581
C.S.G.A. § 10-154a
C.S.G.A. § 1-210(b)(17)

Any exchange of student information, student records, or student-generated content between a local or regional board of education and a contractor requires a written agreement. The law requires that the contract contain elements including a statement that the student data is not the property of or under the control of the contractor, a provision where the board of education may request the deletion of data in the contractor's possession, procedures by which a student or parent could correct any erroneous information, the contractor must ensure the security and confidentiality of data, procedures by which the contractor must notify the board of any unauthorized release, disclosure or acquisition of data, and that the contractor must abide by the Family Educational Rights and Privacy Act.[160] Contractors are also

[158] 34 CFR §99.31
[159] 42 U.S.C. §§5101, section 3
[160] C.G.S.A. § 10-234bb

required to implement and maintain certain security protocols, practices and technical safeguards to protect student data consistent with federal guidance related to protected health information.

In addition to education and school records, state law discussed other types of information obtained by schools and teachers. HIV information is strictly confidential and imposes significant responsibilities on school districts. When school officials become aware of a student's HIV status, they may not share that information with other school personnel as they do with other educational records.[161] Communications concerning drug or alcohol abuse or problem made in confidence by a student to a school professional (e.g. teacher, nurse) need not be disclosed by the professional employee.[162] Any document that is confidential under FERPA is not subject to the Freedom of Information Act.[163]

Early Childhood

Federal Laws

42 U.S.C. §658, et seq.
45 CFR §§98 and 99 et seq.

For the past 20 years, the Federal government and states have ensured that child care was available as a critical support for eligible low-income working families, especially those making the transition from TANF cash assistance to work and for children and families involved with the state child welfare agencies. As a result, there is important information contained in the eligibility records maintained by the state agencies administering child care programs.[164] In many states, the enrollment for child care assistance is closely linked to other human services benefits programs, such as TANF, SNAP, Medicaid, and Low-Income Home Energy Program (LIHEAP).

Key components of the Child Care and Development Block Grant law and federal implementing regulations include:

- Lead state child care agency coordinates the provision of child care services with other Federal, state, and local child care and early childhood development programs.[165]
- State must demonstrate how it will meet the specific child care needs of families receiving TANF or at risk of receiving TANF and who, through employment activities, will transition from TANF.[166]
- Lead child care agency gives priority to children of families with very low family income and children with special needs.[167]
- State agency accumulates specific case level individual recipient reports and provides quarterly case-level reports to the Department including sources of income (including TANF, SNAP, housing assistance, etc.).[168]

Unlike some other specific federal human services laws and regulations, the issues of confidentiality and information sharing are absent in the laws and regulations creating and regulating child care. States

[161] C.S.G.A. § 19a-581
[162] C.S.G.A. § 10-154a
[163] C.S.G.A. § 1-210(b)(17)
[164] Child Care and Development Block Grant Program of 1990 as amended. 42 U.S.C. §658
[165] 42 U.S.C. §658D(b)(1)(D); 45 CFR §§98.14(a)(1)(A) & (D)
[166] 42 U.S.C. §658E(c)(2)(H)
[167] 45 CFR §§98.44
[168] 45 CFR §§98.72(a)(6)

decide how case information, eligibility information, and other types of case matching can be shared with other governmental units. The Administration for Children and Family of the U.S. Department of Health and Human Services has encouraged states to align child care eligibility policies with other programs serving low-income families. In particular, states may establish longer eligibility to align with other programs, such as Head Start, Early Head Start, SNAP, Medicaid, and the Children's Health Insurance Program (CHIP). States may also match records across programs to streamline the application process for families and to promote program integrity (e.g. through verifying or documenting eligibility information).

With the absence of information sharing direction provided by the child care law and regulations, the State's federal limitations are found in The Privacy Act of 1974, as amended.[169] The Privacy Act generally only binds federal agencies, and is not applicable to States, with some exceptions (matching of individual data between different governmental agencies is permitted with prior written consent of the individual to whom the information pertains[170], or unless pursuant to a court order whereupon advance written consent is not required).[171]

State Laws

19a-79-1

The only specific reference regarding confidentiality is found in the Family Day Care Homes regulations. Specifically, this set of regulations states that the provider and staff cannot release any records regarding the child or family without the written of the parent. The only exceptions listed were for emergencies or upon the request of the Office of Early Childhood, the police, or the Department of Children and Families.[172] There was not a similar provision in the Child Day Care Centers and Group Day Care Homes regulations.[173]

Health

Federal Laws

45 CFR 160, 164, as amended, and Subparts A & E

Since it is a national mandate to improve health care and efficiency while reducing costs, and to use technology (through Electronic Medical Records (EMR), Electronic Health Records (EHR) and Health Information Exchanges (HIE)), to its utmost to reach these goals, it is essential for all systems to work together. That means sharing appropriate information to avoid redundancies and to think differently how the human services and health systems can help each other. One hypothesis is that if the systems are in tandem, the health system can decrease the reliance on high-cost medical care and procedures, including emergency room care. It has been shown that families with problems paying their rent and housing-related expenses experience higher rates of emergency hospitalizations than other families.[174] Social needs (including but not limited to shelter, food, utilities) are directly leading to worse health, and the social needs are as important to address as the medical conditions. The medical field and

[169] 5 U.S.C. §552a
[170] 5 U.S.C.§552a(b)
[171] 5 U.S.C. §552a(b)(11)
[172] C.G.S.A. § 19a-87b-10(5)
[173] C.G.S.A. § 19a-79
[174] Bushel, Gupta, Gee and Haas. *Housing Instability and Food Insecurity as Barriers to Health Care Among Low-Income Americans*, Journal of General Internal Medicine, 2006.

practitioners are not capable to address the patient's social needs, which is why the systems must work together. If a person does not have food to eat, they are more likely to be in poor health. Conversely, a person's health improves and the person's health needs and costs decrease if they have nutritious food, adequate and affordable housing, transportation assistance and gainful employment.[175] Health and human services must work together to achieve affordable health care and wellness for our citizens.

Volumes have been written about the Health Insurance Portability and Accountability Act (HIPAA) but in a nutshell, there are 3 purposes for this federal law:

1. It was the beginning of the creation of a uniform standard for processing electronic health care claims in the United States. The HITECH amendment to ARRA built on this processing standard by providing financial incentives for the creation of electronic health records. This was the "portability" purpose so that if a patient moved, the new medical provider would understand and use the same uniform standard.
2. It established a minimum set of privacy rules that all health care providers (as well as health plans and clearinghouses) must follow when handling patient information, giving patients greater control over how their individual health information is used. This was the first part of "accountability". This was to encourage people to truthfully share information with their medical providers without fear that the information will be broadly distributed to other persons.
3. It established new standards for protecting the security of patient information, or the second part of "accountability".

Cross-system information sharing can make all the systems be more effective and efficient in performance, cost savings and revenue reductions. Whether it is the SNAP program and the determination of whether the applicant is an "able bodied adult without dependents" and is capable of working; or the Medicaid system, greatly expanded in enrollment under the Patient Protection and Affordable Care Act, it is essential for the health and public service system to share information when permissible by law. When a child is placed into the foster care system, the state becomes the responsible party for that child and it is essential for the child welfare system to have both basic and complete health and treatment information regarding the child to prevent a health emergency or tragedy and to prevent the inefficient retesting and re-examinations, and even sometimes re-immunizations, which take up caseworker time to arrange and cause expends unnecessary fund expenditures. The corrections system is another example of where readily available and timely health and treatment information can provide better, continuous care for inmates in the state's care and save money by avoiding repetitive and unnecessary costs.

The following outlines the Health and Insurance Portability and Accountability Act (HIPAA) of 1996 and how it is supportive of information sharing with other systems:

- The federal protections are not to interfere with patient access to or the quality of health care delivery[176]

[175] *Health Care's Blind Side: The Overlooked Connection between Social Needs and Good Health*, Robert Wood Johnson Foundation, December 2011.
[176] HHS/OCR guidance

- It is carefully balanced to avoid creating unnecessary barriers to the delivery of quality health care[177]
- Sharing is encouraged if the prohibition would result in unnecessary interference with access to quality health care or certain other important public health benefits of national priorities[178]
- Permitted to share to the individual or designee of individual[179]
- Permitted to share for treatment, payment or health care operations[180]
- Treatment includes the provision, coordination or management of health care and related services among health care providers regarding the individual[181]
- Lengthy list of exceptions to the privacy protections and the requirement for a written authorization
    - Permission to share if required by state law, including to human services entities and the courts[182]
    - An exception for a court order or subpoena with prior notice to the individual[183]
    - Clear description of the elements of and required statements in an appropriate authorization[184]
- Encourages policies and procedures on how protected health information is used, disclosed, and requested for specific purposes[185]
- Encourages policies and procedures to develop reasonable criteria for determining what is the "minimum necessary" protected health information to accomplish purpose of request[186]
- Policies and procedures should identify persons/classes of persons who need access to information to carry out job duties, categories or types of protected health information needed, and conditions appropriate to such access.[187]

A governmental entity that administers the Medicaid and other benefit programs (e.g. healthcare coverage including but not limited to coverage for physical health, mental health, and drug use disorders; TANF; SNAP, etc.) and other human services (e.g. housing, employment, child welfare, mental health, etc.) could decide that the entire entity should be designated as the covered entity under HIPAA, so that information can be shared between different individuals within the organization providing services to the same person, on a need-to-know basis and only the minimally necessary information.[188] This type of integrated, multi-service public agency is the legal entity, with one director, various disciplines, and a centralized administrative unit. The agency needs to have one set of policies and procedures and provides integrated services. The agency's confidentiality notice, provided to all clients as soon as possible, is shared within the integrated, multi-service public agency. Clients or patients could be provided an opportunity to "opt out" and restrict information sharing by designating a particular type of service information not to be shared with other systems. In addition, the agency provides a specific authorization for certain information to be shared, including the protection of the

[177] 45 CFR §160
[178] HHS/OCR guidance
[179] 45 CFR §164.502(a)
[180] 45 CFR §164.506
[181] 45 CFR §164.501
[182] 45 CFR §164.512(a)
[183] 45 CFR §164.512(e)
[184] 45 CFR §164.508(c)(1) & (2)
[185] 45 CFR §164.502(b)(1)
[186] 45 CFR §§164.502(b)(1); 164.514(d)(4)
[187] HHS/OCR guidance
[188] HHS/OCR guidance

location of an abused person, domestic violence, HIV and AIDS information, and alcohol and drug use disorder treatment services.

In this situation, HIPAA permits the sharing of protected health information within the agency without requiring specific and separate authorizations under all of the applicable federal laws for the purposes of treatment and other related health services. The HIPAA definition of treatment permits a provider to offer or coordinate social, rehabilitative, or other services as long as they are associated with and related to the provision of health care.[189]

As for barriers to information sharing, HIPAA was enacted to make it easier for individuals to share health information electronically and thus the word "Portability" in its title. It is interesting to note that the law in many ways has stopped the sharing of information with practitioners of health services and practitioners working with an individual in other fields and systems. Instead of seeing the protections as a part of the treatment process and the multi-disciplinary practice, HIPAA has become the "Red Light" of information sharing, even though the law does not prohibit information from being shared. Instead, policy makers must work together to protect the confidentiality rights of the individual and make the information sharing easier among the people working with a particular individual to provide services to that person.

The following outlines what are commonly viewed as barriers that HIPAA presents to the efforts of sharing health information with other systems:

- Federally-mandated foundation for the protection of personal health information, and the confidentiality and privacy of such information
- Strong privacy protections regarding the sharing of protected health information unless authorized by the individual
- No uniform authorization for an individual; instead, each covered entity has its own and separate authorization for an individual to sign
- Fear of violation of the federal law and disclosing protected health information inappropriately but for positive intentions
- Does not make clear that "treatment" for many federally-funded recipients in multi-systems may involve services from these other systems to meet the "social determinants of health"
- Does not make clear what is the "minimum necessary" protected health information to fulfill a request since it is based on the circumstances of the particular request and the individual's situation

But there is no language in the HIPAA laws, regulations or official clarifications by the Department of Health and Human Services Office of Civil Rights that states that personal health information can never be shared. Instead, it is a process to determine if the information is protected by HIPAA; if protected, can it be shared under the Privacy Rule or do you need a signed authorization by the patient to share the information; how to share the minimally necessary information, and then how to keep the information secure once shared.

So, the first question is what health information is protected by HIPAA. First, it must be information that could be used to identify the individual patient, or protected health information. Such "individually

[189] Federal Register, Volume 65, No. 250, December 28, 2000/Rules and Regulations at 82628

identifiable health information"[190] includes both the demographic information about a patient (name, address, employer, etc.) and the medically related information (diagnosis, treatment, condition, medications prescribed, etc.). It includes past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

As a general rule, all individually-identifiable health information is confidential and protected. The next question is when can protected health information under HIPAA be disclosed and shared? There are 3 general circumstances when such information can be shared:

1. For treatment, payment and health care operations—this circumstance is important when dealing with individual case information, especially when looking at "treatment."[191]

   Examples of "treatment" include the provision, coordination, or management of health care and related services for an individual by one or more health care providers (between doctors, nurses, medical technicians, hospital social workers, hospice workers), including consultation between providers regarding a patient and referral of a patient by one provider to another.[192]

   Examples of "payment" activities include such things as billing and collections, utilization review, reviewing health care services for medical necessity determinations, coverage, justification of charges, and determining eligibility and coverage.[193]

   Examples of "health care operations" include quality assessment and improvement, credentialing and peer review, compliance, auditing services, business planning and development, legal services, training health care and non-health care professionals, accreditation, certification and licensing.[194]

2. For other purposes if the patient has authorized the disclosure—this circumstance is also important when working with an individual in different systems. If there is a trust relationship between the individual and the caseworkers in the different systems to work together for the benefit of the individual, it will be much easier to obtain the authorization.[195]

3. For certain public and research purposes, even if the patient has not authorized the disclosures. This circumstance is basically for research, planning and program effectiveness and not case-specific situations.[196]

And then there are the additional exceptions to the rule, where protected health information can be shared without authorization:

---

[190] 45 CFR §160.103
[191] 45 CFR §160.506
[192] 45 CFR §160.506
[193] OCR/HHS Guidance
[194] OCR/HHS Guidance
[195] 45 CFR §160.506
[196] 45 CFR §164.514(a) & (b)

1. Victims of abuse, neglect or domestic violence[197]
2. Judicial and administrative proceedings[198]
   - Court or administrative tribunal order
   - Subpoena if certain assurances regarding notice to individual and ability to request a protective order is provided
3. Law enforcement purposes[199]
   - Required by law (court orders, court-ordered warrants, subpoenas)
   - To identify or locate a suspect, fugitive, material witness or missing person
   - In response to request for information about victim or suspected victim of a crime
   - To alert law enforcement of a person's death if there is a suspicion that criminal activity caused the death
   - When health care provider believes that protected health information is evidence of a crime that occurred on its premises
   - When health care provider is providing care for a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victim, and the perpetrator of the crime.
4. Required by law[200]
5. Public health activities[201]

   Examples include:

   -Public health authorities for prevention and controlling disease, injury or disability

   -Government authorities authorized to receive reports of child abuse and neglect

   -Entities, products and activities subject to the Food and Drug Association (FDA)

   -Individuals who may have contracted or been exposes to communicable disease when notice is authorized by law

   -Employers in compliance with Occupational Safety and Health Administration or similar State law
6. Public health activities[202]
7. Decedents (funeral directors, coroners, medical examiners)[203]
8. Cadaveric organ, eye or tissue donation[204]
9. Serious threat to health or safety[205]
10. Specialized government functions[206]
11. Workers' compensation[207]
12. Research (under a number of stringent circumstances)[208]

[197] 45 CFR §164.512(c) & (f)
[198] 45 CFR §164.512(e)
[199]45 CFR §164.512(f)
[200] 45 CFR §164.512(a)
[201] 45 CFR §164.512(b)
[202] 45 CFR §164.512(f)
[203] 45 CFR §164.512(g)
[204] 45 CFR §164.512(h)
[205] 45 CFR §164.512(j)
[206] 45 CFR §164.512(k)
[207] 45 CFR §164.512(l)
[208] 45 CFR §164.512(i)

Whether the information can be shared under one of the 3 general circumstances of the HIPAA Privacy Rule or under one of the 12 exceptions, the information should be provided only to a person who has a "need to know" the information for legitimate purposes and to the minimum extent necessary. In addition to the "need to know" rule, and when providing the information outside of the traditional "treatment" circumstances (for example physicians, nurses, and other health practitioners); the information shared should be limited to the" minimum necessary". Therefore, there must be careful thought as to what information is needed and why the information is needed (and only for legitimate purposes).[209]

State Laws

CGSA § 19A-25 and 19a-25-1 et seq.

State law requires the confidentiality of records procured by the Department of Public Health or directors of health of towns, cities or boroughs.[210] This includes all information, records of interviews, written reports, statements, notes, memoranda or other data, including personal data. This also includes information obtained and collected by staff committees regarding issues including but not limited to morbidity and mortality, maternal mortality, disease prevention and control, etc.

The Department of Public Health cannot disclose identifiable health data, except as minimally necessary, to the following: (1) to healthcare providers in a medical emergency to protect the health, life, or well-being 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 or mortality; and (3) for medical and scientific research. The disclosure can only take place upon the execution of a written agreement, which provides for the protection of the data, among other things.

Workforce Development

Federal Laws

42 U.S.C. § 503 et seq.
20 CFR § 603 et seq.

The Unemployment Compensation wage and benefit information held by a state's labor department is always desired by other governmental agencies, since the data is generally up-to-date and rich with personal information. Agencies administering programs, including TANF, SNAP, child support, child welfare, and others, are anxious to enter data sharing agreements with the Department of Labor to help ensure that these other systems are operating with the best and most current information.

By federal and state law, the information obtained for purposes of administering the unemployment compensation law must be maintained in a confidential manner, including the name or any identifying information about an individual or any past or present employer or employing unit, or which if combined with publicly-available information could reveal such information.[211] Similar to other federal

[209] HIPAA is a federally-mandated minimum standard. If a federal or state law is applicable to the information and requires a more stringent standard of confidentiality and conditions and requirements to share information, then the higher standard must be met.
[210] CGSA § 19A-25
[211] 20 CFR § 603.4(b)

laws, along with this broad statement of confidentiality, there are a number of permissible disclosure exceptions to the rule, none of which may interfere with the administration of the unemployment compensation system:

- If the information is in public domain[212]
- Unemployment compensation appeals records (except that all social security account numbers and employer registration numbers must be removed)[213]
- Information to the individual about the individual and information to the employer about the employer[214]
- Release of personally-identifiable confidential unemployment compensation information upon written, informed consent of the specific individual or employer[215]
- Release or consent to a third party by individual or employer to provide information regarding the respective signing party[216]
- To a public official for use in the performance of her/his official duties, which is defined as the administration or enforcement of law or execution of the official responsibilities of a federal, state, or local elected official; includes research related to the law administered by the public official[217]
- To public official's agent or contractor[218]
- Bureau of Labor Statistics, if collected exclusively for statistical purposes under an agreement with the Bureau of Labor Statistics[219]
- Court order or official subpoena[220]
- Federal unemployment compensation program oversight or audit.[221]

The federal unemployment compensation law also requires mandatory disclosure exceptions, notwithstanding the confidentiality rule. These mandatory exceptions include:

- Disclosure to claimants, employers, the Internal Revenue Service (for purposes of UC tax administration) and the U.S. Citizen and Immigration Services (for purposes of verifying a claimant's immigration status)[222]
- Specific information to Unemployment Compensation for Federal Employees (UCFE), Unemployment Compensation for Ex-Service members (UCX), Trade Adjustment Assistance (TAA, except for confidential business information collected by States), Disaster Employment Assistance (DUA), and any Federal UC benefit extension program[223]
- To Railroad Retirement Board[224]

[212] 20 CFR § 603.5(a)
[213] 20 CFR § 603.5(b)
[214] 20 CFR § 603.5(c)
[215] 20 CFR § 603.5(d)(1)
[216] 20 CFR § 603.5(d)(2)
[217] 20 CFR § 603.5(e)
[218] 20 CFR § 603.5(f)
[219] 20 CFR § 603.5(g)
[220] 20 CFR § 603.5(h); 20 CFR § 603.7
[221] 20 CFR § 603.5(i)
[222] 20 CFR § 603.6(a)
[223] 20 CFR § 603.6(b)(1)
[224] 20 CFR § 603.6(a)(2)

- To federal and state food stamp agency specific information, including wage information, whether individual is receiving, has received, or has made application for unemployment compensation benefits, current/most recent address of person, and whether person has refused an offer of employment and details about the offer[225]
- To any State or local child support enforcement for the purposes of establishing and collecting child support obligations from, and locating, persons owing such obligation (excluding the custodial parent support obligations)[226]
- To U.S. Department of Health and Human Services for purposes of National Director of New Hires and its purposes of child support enforcement, TANF and TANF research, administration of earned income tax credit, and use by the Social Security Administration[227]
- To U.S. Department of Housing and Urban Development (HUD) and representative of a public housing agency regarding benefits under a HUD housing assistance program, including wage information and whether the individual is receiving, has received, or has made application for unemployment compensation[228]
- To TANF agency, wage information for the purposes of determining eligibility for TANF and the amount of the assistance[229]
- To comply with Work Innovation Opportunity Act (WIOA), cooperate in evaluations (including related research projects) provided by U.S. Department of Labor or U.S. Department of Education (under Title I of 29 U.S.C. 720 et seq.) by providing requested confidential information to a Federal official (or agent or contractor)[230]

The federal law specifically states that the following entities may request confidential unemployment compensation (including wage information) information from a state's Department of Labor: TANF agency; Medicaid agency; Food Stamp agency; child support enforcement agency, other Social Security Programs under Title I (education), Title II (old-age, survivors, and disability insurance benefits), Title X (service to the blind), Title XIV (totally and permanently disabled) and Title XVI (Supplemental Security Income for the Aged, Blind, and Disabled),[231] and a state agency that has entered an agreement for the purposes of the Income Eligibility Verification System (IEVS). Additionally, the federal regulations set forth the details of the contents of an appropriate data sharing agreement.[232]

Every claimant for unemployment compensation and every employer subject to the State's law must be notified that confidential and wage information may be requested and used for other governmental purposes, including but not limited to the verification of eligibility.[233]

Finally, compliance with federal law regarding confidentiality is a condition of (1) the Department's receiving federal unemployment compensation grant funds (which constitute the majority of the funds coming into the Labor Department) and (2) employers receiving FUTA tax credits (which amount to approximately $500 million per year).[234]

---

[225] 20 CFR § 603.6(a)(3)
[226] 20 CFR § 603.6(a)(4)
[227] 20 CFR § 603.6(a)(5)
[228] 20 CFR § 603.6(a)(6)
[229] 20 CFR § 603.6(a)(7)
[230] 20 CFR § 603.6(a)(8)
[231] 20 CFR § 603.21
[232] 20 CFR § 603.10
[233] 20 CFR § 603.6(a)(11)
[234] 20 CFR § 603.12

State Laws

CT Gen State § 31-254

Connecticut law implements and reflects the federal law, making clear that all of the information collected by the Department of Labor (DOL) for the administration of the unemployment compensation program is confidential. Essentially, Connecticut's law prohibits DOL from confirming or denying the existence of or providing access to unemployment compensation information, unless the recipient is a public official, the individual, or a separating or base period employer. The Connecticut law also outlines exceptions. For example, access may be provided to an entity, upon written, informed consent by the individual or employer. In addition, the law specifies that any authorized user of the CTWorks Business System shall have access to information from the Department of Labor, so long as the user enters a written agreement establishing the safeguards to protect the confidentiality of any information disclosed to such user.[235] The Regional Workforce Development Boards may have access to unemployment compensation information, so long as the information is necessary for the administration of the Workforce Innovation and Opportunity Act, Jobs First Employment Services Program, or the Trade Adjustment Act program, and only pursuant to a data sharing agreement.

The statute also references the provision of unemployment compensation information to the Department of Social Services, the Board of Regents, an agent of the United States Department of Labor, and AccessHealthCT, so long as there is an agreement between the state departments and the recipient agencies agree to the confidentiality safeguards required by the DOL.

While the statute does not mandate the provision of unemployment compensation information to any agency but the Department of Social Services, DOL has numerous data sharing memoranda of understanding (MOUs) with local, state, and federal agencies to assist such agencies with their statutory mandates.

Finally, the statute provides that the Department of Labor administers a state directory of new hires and is required to provide information obtained through that directory to the Department of Social Services and to the United States Department of Health and Human Services for inclusion in the National Directory of New Hires. The statute provides that not later than 20 days after the date of employment, an employer maintaining an office or transacting business in the state is required to report the name, address and Social Security Number of each new employee (including an employee rehired in the past sixty (60) days) employed in the state.[236] While new hires information in not unemployment compensation information, federal law requires that it be treated confidentially in the same manner.[237]

Criminal Justice

Federal

44 U.S.C. §§3541 et seq.
42 U.S.C. §3789g
28 CFR Part 22

[235] CT Gen State § 31-254(a)(2)
[236] CT Gen State § 31-254(b)
[237] 20 CFR § 617.57

Law enforcement requires timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, in 1998, the Advisory Policy Board recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure. Administered through a shared information management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and general of criminal justice information. The Federal Information Security Management Act of 2002[238] provides further legal basis for the approved management, operational, and technical security requirements mandated to protect criminal justice information and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of criminal justice information, whether at rest or in transit. The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's Advisory Policy Board's decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST).

For research purposes, the National Institute of Justice (NIJ) provides for the protection of the privacy and well-being of individuals who are participants in NIJ research studies through statutory and regulatory protection provided to private information.[239] The regulations:

1. Protect the privacy of individuals by limiting the use of private, identifiable information for research or statistical purposes.
2. Protect private information provided by individuals from use in any judicial, legal, or administrative process without the individual's prior consent.
3. Improve the scientific quality of NIJ research programs by minimizing the subject's concerns over the use of the data.
4. Clarify for researchers the limitations on the use of privately identifiable information for only research or statistical purposes.
5. Ensure that the understanding and knowledge of the broad criminal justice system will continue to advance by providing individual privacy protections.

Additionally, the regulations provide specific requirements on data access and security, limitations on the transfer of the data, and specifications for final disposition of the information.

State

C.G.S. § 18-87k
C.G.S. § 54-300
C.G.S. § 17a-513-516
C.G.S. § 4d-43

[238] 44 U.S.C. §§3541 et seq.
[239] 42 U.S.C. §3789g; 28 CFR Part 22

There are a number of state laws dealing with the exceptions to the confidentiality rules regarding offender information and data and permitting sharing of such information and data between systems for different purposes:

- The Criminal Justice Policy Advisory Commission uses data and information to develop policies, procedures, and research regarding many issues, including the impact of efforts to prevent prison overcrowding, developing reentry strategy, and identifying institution-based and community-based programs and services that effectively address offender needs including health care, transitional health care, family support, substance abuse, domestic violence, and sexual offender programs and services.[240]

- There is established a Criminal Justice Policy and Planning Division within the Office of Policy and Management. At the request of this Division, the Department of Correction, the Board of Pardons and Paroles, the Department of Mental Health and Addiction Services, the Department of Emergency Services and Public Protection, the Chief Court Administrator, the executive director of the Court Support Services Division of the Judicial Branch, the Chief State's Attorney and the Chief Public Defender shall provide the division with information and data needed to perform its division. The Division shall have access to individualized records maintained by the Judicial Branch and the other listed agencies that are necessary for research purposes. All data and information that is shared shall be pursuant to developed protocols to protect the privacy of the individualized records consistent with state and federal law and shall remain confidential while in the custody of the Division and shall not be disclosed. Additionally, individualized records shall be used for statistical analyses only and not in any other manner that would disclose the identity of individuals to whom the records pertain.

- Connecticut Sentencing Commission shall perform a number of statutory functions, including but not limited to, facilitating the development and maintenance of a statewide sentencing database in collaboration with state and local agencies, using existing state databases or resources, conducting sentencing trends analyses and studies and preparing offender profiles, and identifying potential areas of sentencing disparity related to racial, ethnic, gender and socioeconomic status. The Commission may request any office, department, board, commission or other agency of the state or any political subdivision of the state to supply records, information and assistance as may be necessary or appropriate in order for the commission to carry out its duties. Any records or information supplied to the Commission that is confidential shall remain confidential and not be disclosed.[241]

- The Office of the Governor, Lieutenant Governor, Treasurer, Attorney General, Secretary of State or Comptroller and the Commissioner of Corrections may, by interagency agreement, provide for such office (1) to receive information system and telecommunication system facilities, equipment and services pursuant to contracts, subcontracts or amendments to contracts or subcontracts, and (2) to interconnect with other state agency information systems and telecommunication systems.[242]

[240] C.G.S. § 18-87k
[241] C.G.S. § 54-300
[242] C.G.S. § 4d-43

- Sharing of data and information regarding persons in the custody of the Commissioner of Correction with a psychiatric disorder either upon entry into the corrections system or while incarcerated in prison,[243] and questions regarding the competency of a defendant to stand trial.[244]

Homelessness

Federal Laws

12 U.S.C. §5201 et seq.
24 CRF Parts 91, 576, 580, and 583

The federal government provides funding to prevent homelessness and to help states and local governments provide housing and other services to homeless persons to move them into permanent housing and productive citizens. In 2009, Congress passed the Helping Families Save Their Homes Act and the Homeless Emergency Assistance and Rapid Transition Housing Act (HEARTH),[245] amending and clarifying the Homeless Management Information System (HMIS). Housing and homeless information is confidential and personally identifiable information cannot be shared unless permitted. But it is with HMIS that state and local governments share data with other systems, which is encouraged by the U.S. Housing and Urban Development (HUD). In the HMIS Implementation Guide published by HUD, the federal government states that the benefits of an HMIS are available through interagency data sharing. To reduce duplicative client intakes and provide opportunities to improve case management and service coordination, HMIS must support interagency data sharing and the Guide states that these objectives are important to achieve permanent housing for all persons.[246]

HMIS requires universal data elements and program-specific data elements.[247] These data elements are further evidence of the need to partner with other agencies and systems to treat the client in a "total person" manner to help solve the homelessness situation.[248] The Program-Specific Data Elements that are required for federal reporting include elements that may be used by more than one federal funder program and are common across federal agencies:

- Income and Sources
- Non-Cash Benefits
- Health Insurance
- Physical Disability
- Developmental Disability
- Chronic Health Condition
- HIV/AIDS[249]
- Mental health problem

[243] C.G.S. § 17a-513-516
[244] C.G.S. § 54-56d
[245] 12 U.S.C. §5201 et seq.
[246] Center for Social Policy, Aspen Systems Corporation, U.S. Department of Housing and Urban Development. *Homeless Management Information Systems: Implementation Guide.* September 2002
[247] HMIS Data and Technical Standards, HUD Exchange. 2017.
[248] The universal data elements include name, Social Security Number, date of birth, race, ethnicity, gender, veteran status, disabling condition, project start date, project exit date, destination, relationship to head of household, client location, housing move-in date, living situation.
[249] Consent would have to include specific language required to share information regarding HIV/AIDS

- Substance Abuse[250]
- Domestic Violence
- Contact
- Date of engagement
- Bed-Night Date
- Housing Assessment Disposition

Additionally, the service array that HUD is providing for homeless projects indicate the need to work with and share information with other agencies and systems. These project services include:

1. Street outreach, reimbursing for case management, emergency health services, emergency mental health services, transportation and services for special populations (e.g. youth, persons living with HIV/AIDS, victim services)[251]
2. Emergency shelter, essential services including case management, child care, education, employment assistance and job training, outpatient health services, life skills training, mental health and substance use disorder services, and services for special populations[252]

HMIS ensures the confidentiality of identifiable personal information.[253] Protected personal information is defined as any information about a living homeless individual that identifies, either directly or indirectly, a specific individual, or can be manipulated by a reasonably foreseeable method to identify a specific individual or can be linked with other available information to identify a specific individual.[254] This is accomplished with written client consents for the data sharing. The HUD HMIS Manual provides several potential data sharing functions (without requiring specifics as to the content of the data sharing agreements or the client consent form). Those specifics include:

- Blanket sharing or flexible data sharing. A blanket sharing function discloses a complete client record to other agencies. Flexible data sharing capacity allows clients to identify which part or parts of a client's file they would like disclosed and to specify individual programs with whom to share the information.
- Real-time capacity for agencies to share client information and jointly manage services for a client.
- Capability for one agency to electronically send a client referral or client information with complete client intake information to another agency.[255]

Again, the federal regulations provide permissible HMIS uses and disclosures of protected personal information. These include the following:

- To provide or coordinate services to an individual
- For functions related to payment or reimbursement of services
- Administrative functions (e.g. legal, audit, personnel, oversight and management functions

[250] Consent would have to include specific language required by applicable federal law
[251] 24 CFR §576.101
[252] 24 CFR §576.102
[253] 24 CFR §580.35
[254] Federal Register, July 30, 2004, pg. 45928
[255] Center for Social Policy, Aspen Systems Corporation, U.S. Department of Housing and Urban Development. *Homeless Management Information Systems: Implementation Guide,* at 18. September 2002.

- For creating de-identified protected personal information (e.g. research).
- Required by law
- To avert a serious threat to health or safety
- Victims of abuse, neglect or domestic violence
- Academic research purpose
- Law enforcement purposes[256]

State Laws

SB 896 (October 1, 2013)

Connecticut's homeless person's bill of rights guarantees that the rights, privacy and property of homeless persons are adequately safeguarded and protected under the laws of the state. In the law, "homeless person" is defined as any person who does not have a fixed or regular residence and who may live on the street or outdoors, or in a homeless shelter or another temporary residence.

Each homeless person has the right to:

1. Move freely in public spaces, including on public sidewalks, in public parks, on public transportation and in public buildings without harassment or intimidation from law enforcement officers in the same manner as other persons
2. Have equal opportunities in employment
3. Receive emergency medical care
4. Register to vote and to vote
5. Have person information protected
6. Have a reasonable expectation of privacy in his or her personal property
7. Receive equal treatment by state and municipal agencies.

In addition, there are some additional provisions that are found in state law relative to the release of homeless program information related to sex offenders, domestic violence victims, and participants in the State RAP.[257]

[256] Federal Register, July 30, 2004, pp. 45918-45919,

[257] CT Gen State §138a and b