US Offices of ONC Health-It & Health and Human Services regarding HIE, HIPAA and Privacy

Fact Sheet

This fact sheet is directly copied and pasted from government and corporate websites, with the source web sites.

Red highlights are for emphasis, but the text from the websites has not been altered.

1. **The Cures Act of 2016 introduced HIE, and ways it relates to mental health, substance abuse treatment and HIPAA.**
   https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf

   EC. 4005. LEVERAGING ELECTRONIC HEALTH RECORDS TO IMPROVE PATIENT CARE.

   (a) REQUIREMENT RELATING TO REGISTRIES.—

   (1) IN GENERAL.—To be certified in accordance with title XXX of the Public Health Service Act (42 U.S.C. 300jj et seq.), electronic health records shall be capable of transmitting to, and where applicable, receiving and accepting data from, registries in accordance with standards recognized by the Office of the National Coordinator for Health Information Technology,

   including clinician-led clinical data registries, that are also certified to be technically capable of receiving and accepting from, and where applicable, transmitting data to certified electronic health record technology in accordance with such standards.

   (2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require the certification of registries beyond the technical capability to exchange data in accordance

   with applicable recognized standards.

2. **CARIN Alliance joins ONC in creating National Digital Health ID (CARIN stands for "Creating Access in Real Time Now")**

   Digital Identity and Federation in Healthcare
   https://www.carinalliance.com/wp-content/uploads/2021/03/CARIN-Alliance-Federated-Trust-Agreement-WP_3.8.21-1.pdf

   The 21st Century Cures Act, the ONC Cures Act Final Rule, and the CMS Interoperability and Patient Access rule have accelerated the ability for an individual to access their personal health information via an application of their choice by leveraging HL7® FHIR® Application Programming Interfaces or APIs. Currently, the use of SMART on FHIR® allows for an individual to use their provider or payer portal username and password to authenticate themselves and retrieve their personal health information. While the CARIN Alliance strongly endorses the current implementation of SMART on FHIR® by stakeholders in the health care ecosystem to ensure individuals have immediate access to their health information, we also want to advance a future vision for how we could as an industry digitally authenticate individuals in a trusted way without

being tied to the creation of portal accounts, and then allow an individual to use that same trusted authentication event to access their health information across multiple payers and providers. We envision an ecosystem where an individual voluntarily creates a digital identity credential1 in an application of their choice, which they own, manage, and use to access their health information from any health care payer or provider in the country. In order to realize this ecosystem, we must ensure that people are who they claim to be (often referred to as "identity proofing") before they are granted access to data, and then deploy strategies to match individuals across systems using trusted identifiers so the right information can be shared with the right person at the right time. In other words, we first need to establish a trusted digital identity credential and then we need to federate that trust.

Their proposed transition from physical ID to digital ID: (page 4)

PHYSICAL ID	**VS**	**DIGITAL ID**
Government organization, e.g. DMV		Credential service provider (issuer)
Official paper-based document, e.g. birth certificate		Identity evidence
Paper-based identity, e.g. driver's license		Digital identity credential
Accepts driver's license to confirm your identity, e.g. doctor's office		Relying party

CARIN Alliance Partners
https://www.carinalliance.com/our-membership/carin-board-participants/
Many listed, here are some big names:

- Board members include: Apple, Microsoft, ENHAC and others
- Alliance members include: Amazon, Anthem, Cigna, CVS, Google, Humana, Inovalon, United Healthcare
- Special Guests: Optum, Pfizer, Trinity Health
- Consulting Government Agencies: ONC, FTC, OCR, VHA, CMS,HHS, NIH

The Electronic Healthcare Network Accreditation Commission (EHNAC) of Simsbury, CT and CARIN Alliance announce partnership, October 3, 2022

https://www.carinalliance.com/wp-content/uploads/2022/10/EHNAC-CARIN-partnership-press-release.pdf

EHNAC and CARIN Alliance Announce New CARIN Code of Conduct Accreditation Program Partnership to advance consumer-directed exchange within the healthcare industry among health plans, providers and third-party app developers SIMSBURY, Conn. and WASHINGTON – October 3, 2022 – The Electronic Healthcare Network Accreditation Commission (EHNAC), a non-profit standards development organization and accrediting body for organizations that electronically exchange healthcare data, and The CARIN Alliance, a collaborative working to advance consumer-directed exchange of health information, today announced the creation of a new CARIN Code of Conduct Accreditation Program (CCCAP). This new offering is set to bring both the CARIN Code of Conduct and EHNAC's criteria review process to health plans, health systems, EHR vendors,

implementers of HL7® FHIR®-based application programming interfaces (APIs),
and third-party app developers in a continued effort to support additional levels of trust related to consumer access to health data.

3. **Federal and State departments have a huge agenda for collecting and exchanging healthcare data.**

https://www.healthit.gov/buzz-blog/health-it/wowzapalooza-a-post-health-datapalooza-2023-health-it-roundup

WowzaPalooza – A Post-Health Datapalooza 2023 Health IT Roundup - Steven Posnack | MARCH 9, 2023

States: In case you missed it, Health Datapalooza happened toward the end of February. The aptly named conference always invokes a bit of fun while at the same time being a high octane mix of data scientists, policy makers, health care leaders, entrepreneurs, researchers, and patient advocates.

4. **ONC Health IT has goals to establish a national digital health ID and has the specific goal to gain behavioral health data, which has stricter laws that protect private health information.**

https://www.healthit.gov/topic/health-equity#:~:text=ONC's%20Health%20IT%20Certification%20Program,a%20consistent%20and%20standardized%20way.

- Under "Using Standards & Certification of Health IT to Improve Health Equity"

States: "ONC's United States Core Data for Interoperability (USCDI) helps guide how race, ethnicity, sexual orientation, and gender identity data can be consistently recorded across the health system."

In 2022, ONC added additional health equity-supporting data elements to USCDI, including disability status, mental function, tribal affiliation, and insurance information. The July 2022 Standards Bulletin provides more details about how USCDI v3 promotes equity, reduces disparities, and supports public health data interoperability. For USCDI v4 development processes, we have prioritized behavioral health data, which has disproportionate health equity impacts**.**

- Under "Project US@"

States "Accurate patient matching has long been recognized as foundational to the interoperability of patient data across healthcare. One of the ways that patient matching could be improved is through demographic data standardization. The Office of the National Coordinator for Health Information Technology (ONC) is collaborating with standards development organizations (SDOs) including the National Council for Prescription Drug Programs (NCPDP), Health Level 7 (HL7) International, and X12, along with other interested stakeholders to create a unified, cross-standards technical specification for patient address to help improve patient matching called Project US@.

- Under FHIR at Scale Taskforce (FAST)

States: Leverage most up to date industry considerations to build on best practices and recommendations for identity matching services and KPIs, and identity assurance for an appropriate, national, standards based approach for individual identity matching.

- HL7 Implementation Guide: Improving identity assurance and patient match quality through **interoperable Digital Identity and Patient Matching** capabilities
- Under "Challenge"

States: Nationwide exchange of health information requires a fabric of trust that enables secure data transfer and identity assurance among providers, HIEs and other healthcare industry participants. A nationwide trust fabric is greatly facilitated by methods that are secure, standardized, and broadly adopted. These methods help to set and query the identity policies and attributes of standards-based digital certificates, enabling a variety of contexts for secure exchange (signing, encryption, TLS, etc.).

- Under "Purpose and Goals"

This initiative aligns with Meaningful Use and aims to enable providers to electronically exchange and protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. The preliminary focus will be on developing an analysis of the issues related to complying with digital certificate requirements for exchanging data with Federal agencies.

- Target goals for this Initiative include:

Cross-certification of Certificate Authorities (CAs) with Federal Bridge Certificate Authority (FBCAs)

Adoption of well-defined standards for certification authorities to issue interoperable digital certificates for organizations and individuals.

Minimize costs to obtain, maintain, and use digital certificates

Existence of a robust market for reliable digital certificate issuers for healthcare

- Under "Data Access for Research Phase 3"

States: "DAF (Data Access Framework) Phase 3 Policy Considerations

As part of the DAF Phase 3 activities, various policy issues need to be addressed. In order to address the various policy issues, a work group dedicated to addressing policy issues will be setup with close coordination with the ONC Office of the Chief Privacy Office (OCPO). The work group is expected to perform the following activities

Capture policy guidance required to operationalize capabilities C1 through C6 specifically in the following areas

Patient identity matching

Patient consent and data donation

Patient privacy and data disclosure

Shared or Centralized IRB approaches to facilitate data access across multiple sites for research purposes

Trust establishment and endpoint discovery

- Under ONC Standards Bulletin 2022 states:

States: ONC Standards Bulletin 2022-2 (SB22-2) discusses the development and finalization of the latest version of the United States Core Data for Interoperability (USCDI), Version 3 (USCDI v3), which was released on July 19, 2022. Stakeholders across the healthcare system benefit from the USCDI, which sets the technical foundation for the access, exchange, and use of electronic health information to support patient care. The USCDI defines the baseline set of data to inform interoperable implementations for stakeholders such as federal agencies supporting health and health care, hospitals, research organizations, clinician offices, and software developers.

5. **There are serious risks for hacking of private health information. At a time nationals concerns are raised about data collection from enemy states and introduction of the Restrict Act.**

https://www.healthit.gov/data/quickstats/breaches-unsecured-protected-health-information

- UnderONC Data on HIE hacking:

States: 2015 Number of People Effected by Electronic Medical Record Hacking Incidents: 3,948,985

https://www.reuters.com/world/us/significant-breach-potentially-exposes-us-lawmakers-personal-data-letter-2023-03-08/

- States US House of Representative DC Health link hacked, March 9, 2023
-

https://www.congress.gov/bill/118th-congress/senate-bill/686?s=1&r=15

- Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act or the RESTRICT Act

US is currently reviewing legislation regarding security risks among technology communications

6. **There is a comprehensive federal plan for healthcare data collection and exchange.**

https://www.healthit.gov/sites/default/files/page/2020-10/Federal%20Health%20IT%20Strategic%20Plan_2020_2025.pdf

- **Under "2020-2025 Federal Health IT Strategic Plan"**

States: Federal Health Principles

Put Individuals First: goals, values, culture and privacy

Build a culture of secure access to health information: Support secure health information access, exchange, and use by individuals, caregivers, healthcare providers, public health professionals and other stakeholders.

- An Outcome Driven Plan: Focused on meeting the needs of: Individuals, populations, caregivers, healthcare providers, payers, public health professionals, researchers, developers and innovators.

- Protecting Privacy of Health Information

The most sensitive information about a person is often their health information. Government agencies, healthcare providers, health IT developers, researchers, and other stakeholders have been working together to implement mechanisms for strengthening health information privacy as more data are generated and exchanged through interoperable health IT.

Despite implementation and use of robust privacy practices in healthcare as required by federal and state regulations, EHI can still be misused or inappropriately disclosed in ways that may harm consumers. Federal partners and providers play an important role in educating individuals and their caregivers on data practices and safety risks associated with uses of electronic data. They can also educate patients on how to meaningfully consent to the use of their data.

Securing Health Information

The confidentiality, integrity, and security of EHI that is created, transmitted, and stored using health IT is a priority for all stakeholders. This is especially true considering the healthcare industry's move toward cloud-based storage, where data on large populations of patients is held in one place. The strategies included throughout this Plan are predicated on implementation of robust mechanisms for securing information from ransomware and other cybersecurity risks, while ensuring that information is accessible and usable when and where it is needed. Sustain collaborative activities necessary to ensure public health surveillance, preparedness, and response.

Assess availability of health and human services data and streamline the appropriate collection, submission, and sharing of this data between federal, state, Tribal, and local systems to enable population health planning; analysis of quality and patient outcomes across settings and programs; and clinical research.

Broaden use of new technologies and analytic approaches like ML and

predictive modelling to harness the power of integrated data for improving quality and decision making.

• Increase use of health IT capabilities to conduct research and integrate into other data sources remotely or virtually, as appropriate.

• Advance research into targeted therapies through real-time data and ML intelligence informed through public health principles, data, and research.

• Identify and implement health IT capabilities that support rapid sharing of disease surveillance data.

Continue collaboration across public and private sectors to adopt and advance nationally-supported standards, implementation specifications, and certification criteria, including the United States Core Data for Interoperability (USCDI), Interoperability Standards Advisory (ISA), and FHIR®.

7. There is federal legislation to address information blocking practices taken by healthcare providers, developers of certified health IT, and HIEs

https://www.healthit.gov/sites/default/files/State%20Mental%20Health%20Laws%20Map%201%20Minimum%20Necessary%20-%20revised%202-23-17.pdf

States: Eliminate unnecessarily restrictive data sharing practices and use nationally supported standards, implementation specifications, and certification criteria to promote data liquidity.

8. There are federal plans that specifically target "capture" of behavioral health data.

https://www.healthit.gov/sites/default/files/onc_sim_resource_center_webinar032916.pdf

- Under "Behavioral Health Integration"

States: 2015 Certification Edition Ability to Capture 8 Domains of Social, Psychological, and Behavioral Health Data

Optional certification, includes the ability to record, change and access standardized questions and responses (a)(15) for:

• Financial resource strain

• Education level

• Stress

• Depression screening (PH02)

• Physical Activity

• Alcohol Use

• Social Connection and Isolation

- Under “Behavioral Health Consent Management”

States: The timely exchange of health information between behavioral health providers and physical health providers to support care coordination is a critical element of the National Quality Strategy and health reform efforts. However, privacy and confidentiality concerns are currently limiting the inclusion of behavioral health data in electronic health information exchange efforts.

Administration are piloting approaches to data segmentation and granular consent management that will help solve these issues.

- The HIEs could be used to support a community record, including data from criminal justice, housing and urban development, and other social support systems. Guidance on privacy and other policy issues related to the development of a community record would be useful.
- Behavioral health providers also noted that a field simply for progress notes was insufficient. Only the immediate provider may review that content; however, specific fields related to treatment plans, goals, and referrals may facilitate integration. Additionally**,** the inclusion of specific key words related to behavioral health in certified EHR capabilities may assist in documentation.

Some providers may be required to report duplicate patient information regarding child welfare, developmental disabilities, and HIV interventions to several federal and state health agencies as well as payers for reimbursement. This requirement is especially burdensome for small providers and significantly increases the cost of care delivery. Stakeholders urged ONC to collaborate with other federal agencies to use health IT to facilitate the streamlining and standardization of duplicate reporting. The current standards can be a launch point for standardizing data collection by federal and state agencies.

9. Federal policy establishing HIPAA allows provider release of data without consent by means of BAA and addresses providers rights to not release PHI.

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf

- Under HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment

States: INDIVIDUAL CHOICE AND THE HIPAA PRIVACY RULE page 1

The Individual Choice principle of the Privacy and Security Framework emphasizes that the

opportunity and ability of an individual to make choices with respect to the electronic exchange of their individually identifiable health information is an important aspect of building trust.

Optional Consent page 2

The Privacy Rule's optional consent provisions offer covered entities the ability to adopt use and disclosure policies that build upon the Privacy Rule's baseline requirements and reflect a covered entity's own professional ethics and best judgment.

Ultimately, the Privacy Rule allows each covered entity to tailor their consent policies and procedures, if any, according to what works best for their organization and the individuals with whom they interact.

The HIPAA Privacy Rule requires the individual's written authorization for any use or disclosure of protected health information (PHI) not otherwise expressly permitted or required by the Privacy Rule. For example, authorizations are not generally required to disclose PHI for treatment, payment, or health care operations purposes because covered entities are permitted to use and disclose PHI for such purposes, with few exceptions. Page 4.

In particular, the Privacy Rule's provisions for optional consent and the right to request restrictions can support and facilitate individual choice with respect to the electronic exchange of health information through a networked environment, depending on the purposes of the exchange. The Privacy Rule allows covered entities to obtain the individual's consent in order to use or disclose protected health information (PHI) for treatment, payment, and health care operations purposes. If a covered entity chooses to obtain consent, the Privacy Rule provides the covered entity with complete flexibility as to the content and manner of obtaining the consent. 45 C.F.R. § 164.506(b). Similarly, the Privacy Rule also provides individuals with a right to request that a covered entity restrict uses or disclosures of PHI about the individual for treatment, payment, or health care operations purposes. See 45 C.F.R. § 164.522(a). While covered entities are not required to agree to an individual's request for a restriction, they are required to have policies in place by which to accept or deny such requests. Thus, covered entities may use either the Privacy Rule's provisions for consent or right to request

restrictions to facilitate individual choice with respect to electronic health information exchange. Page 4

Does the HIPAA Privacy Rule permit a covered entity to disclose psychotherapy notes to or through a health information organization (HIO)?
A6: Yes, provided the covered entity has obtained the individual's written authorization in accordance with 45 C.F.R. § 164.508. See 45 C.F.R. § 164.501 for the definition of "psychotherapy notes." With few exceptions, the Privacy Rule requires a covered entity to obtain individual authorization prior to a disclosure of psychotherapy notes, even for a disclosure to a health care provider other than the originator of the notes, for treatment purposes. For covered entities operating in an electronic environment, the Privacy Rule does, however, allow covered entities to disclose protected health information pursuant to an electronic copy of a valid and signed authorization, as well as to obtain HIPAA authorizations electronically from individuals, provided any electronic signature is valid under applicable law. Page 5

- **https://www.healthit.gov/sites/default/files/playbook/pdf/exchange-health-care-ops.pdf**

Under: Permitted Uses and Disclosures: Exchange for Health Care Operations

45 Code of Federal Regulations (CFR) 164.506(c)(4)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities without first obtaining an individual's authorization: including for treatment and for health care operations of the disclosing CE or the recipient CE when the appropriate relationship exists. Other laws may apply. This fact sheet discusses only HIPAA. Under HIPAA, a CE can disclose (whether orally, on paper, by fax, or electronically) PHI to another CE or that CE's business associate for the following subset of health care operations activities of the recipient CE (45 CFR 164.501) without needing patient consent or authorization (45 CFR 164.506(c)(4)):

• Conducting quality assessment and improvement activities
• Developing clinical guidelines
• Conducting patient safety activities as defined in applicable regulations
• Conducting population-based activities relating to improving health or reducing health care cost
• Developing protocols

• Conducting case management and care coordination (including care planning)

• Contacting health care providers and patients with information about treatment alternatives

• Reviewing qualifications of health care professionals

• Evaluating performance of health care providers and/or health plans

• Conducting training programs or credentialing activities

• Supporting fraud and abuse detection and compliance programs

In general, before a CE can share PHI with another CE for one of the reasons noted above, the following

three requirements must also be met:

1. Both CEs must have or have had a relationship with the patient (can be a past or present

patient)

2. The PHI requested must pertain to the relationship

3. The discloser must disclose only the minimum information necessary for the health care

operation at hand page 1

As in the prior scenarios, the providers sharing PHI with the health plan's BA are not responsible under HIPAA for what the BA subsequently does with the information once information has been sent to the BA for a permissible reason and in a secure manner. Page 2

- **https://www.healthit.gov/sites/default/files/playbook/pdf/your-practice-and-the-hipaa-rules.pdf**

Under "Chapter 2: Your Practice and the HIPAA Rules"

States: The HIPAA Rules do not override such state laws that do not conflict with the

Rules and offer greater privacy protections. If a state law is less protective than the HIPAA Rules but a CE or BA could comply with both, both apply — such as when a state law permits disclosure without an authorization and the Privacy Rule requires an authorization, the entity could comply by obtaining authorization. Page 11

10. **US Department of Health and Human Services Office of Civil Rights does not address mental health and substance abuse privacy laws in it's HIPAA and HIE policy statement.**

https://www.hhs.gov/sites/default/files/hie-faqs.pdf

HIPAA, Health Information Exchanges, and Disclosures of Protected Health Information for Public Health Purposes, December, 2020

11. There are federal guidelines, resources, trainings and pilot studies dedicated to HIE

https://www.healthit.gov/sites/default/files/playbook/pdf/educational-module-Behavioral-Health-Providers.pdf

This is a good overview of the enormity of the work being done to promote HIE and national digital health ID.

12. There is federal legislation prohibiting information blocking, with 8 excemptions.

https://www.healthit.gov/topic/information-blocking?options=dc40385d-a097-4e40-acce-d3c805fead09

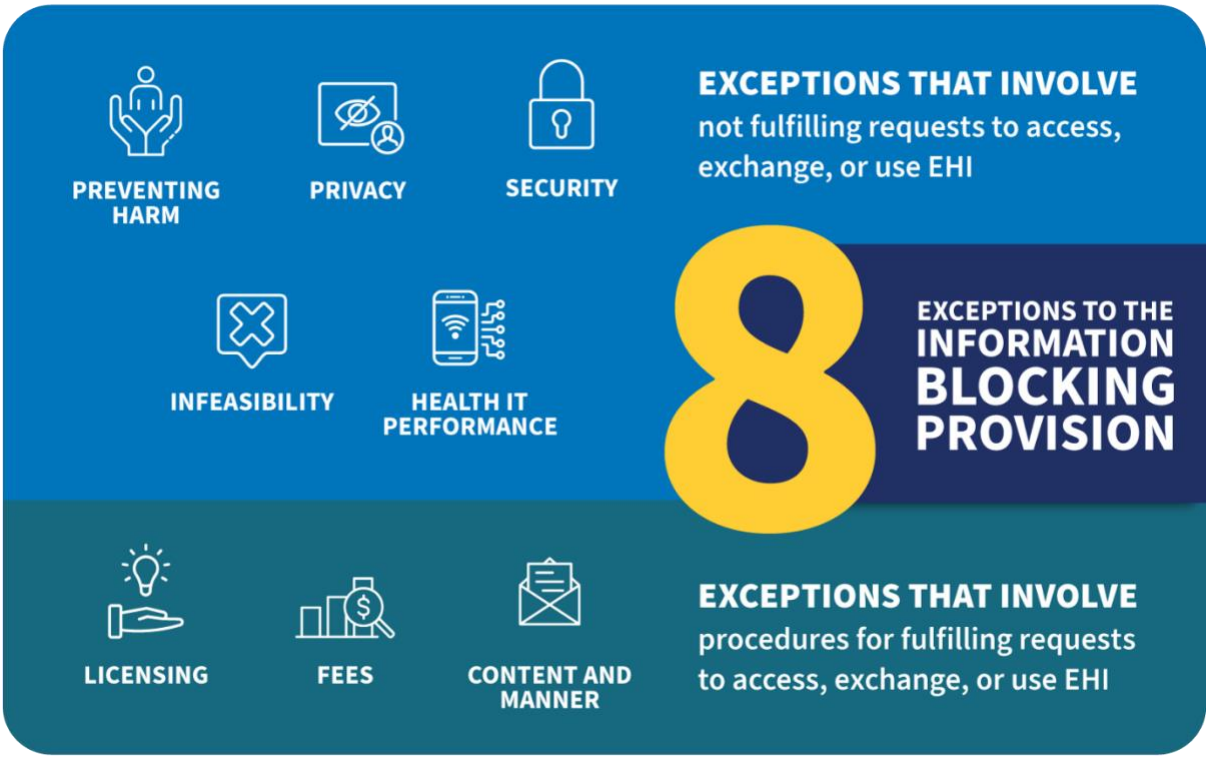
- Under "What Is Information Blocking and to Whom Does It Apply?"

States: Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception. The Cures Act applied the law to healthcare providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs).

It is also important to note that the Cures Act established two different "knowledge" standards for actors' practices within the statute's definition of "information blocking." In particular, for health IT developers of certified health IT, as well as HIEs/HINs, the law applies the standard of whether they know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI. For healthcare providers, the law applies the standard of whether they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.

Information Blocking Exceptions

Eight information blocking exceptions were established in the 2020 Cures Act Final Rule. When an actor's practice meets the condition(s) of an exception, it will not be considered information blocking.



https://www.healthit.gov/sites/default/files/page2/2020-03/InformationBlockingExceptions.pdf

- Under : Exceptions that involve not fulfilling requests to access, exchange, or use EHI

States: Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

¬Preventing Harm ¬Privacy Exception ¬Security Exception ¬Infeasibility Exception

¬Health IT Performance Exception ¬Content and Manner Exception ¬Fees Exception

Licensing Exception

13. **US Health and Human Services created privacy role regarding HIPAA and Reproductive Health Care but didn't address HIE.**

    https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hipaa-reproductive-health-fact-sheet/index.html

    - HIPAA Privacy Rule Notice of Proposed Rulemaking to Support Reproductive Health Care Privacy Fact Sheet

14. **Federal departments collect All-Payer Claims Database data from insurers submitting all claims from providers.**

https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/state-all-payer-claims-databases-advisory-committee

- Under “All-Payer Claims Databases”

States: The Agency for Healthcare Research and Quality is undertaking activities to develop an effective and feasible approach for using all-payer claims databases to advance the goal of improving health care affordability, efficiency, and cost transparency.

https://www.ahrq.gov/data/apcd/index.html

- Under “Under US Dept of health and Human Services: Overview of All-Payer Claims Databases”

States: All-payer claims databases (APCDs) are large State databases that include medical claims, pharmacy claims, dental claims, and eligibility and provider files collected from private and public payers.

APCD data are reported directly by insurers to States, usually as part of a State mandate. In terms of their capacity to produce price, resource use, and quality information for consumers, APCD data have three potential advantages over other datasets:

They include information on private insurance that many other datasets do not. They include data from most or all insurance companies operating in any particular State, in contrast to some proprietary datasets.

They include information on care for patients across care sites, rather than just hospitalizations and emergency department visits reported as part of discharge data systems maintained by most States through State governments or hospital associations. They also include large sample sizes, geographic representation, and capture of longitudinal information on a wide range of individual patients.

https://www.ahrq.gov/sites/default/files/wysiwyg/professionals/quality-patient-safety/quality-resources/apcd/apcdmeasinvrpt.pdf

Under “The high-priority areas included:”

• States: Measures that address specific high-priority conditions and services (i.e., cardiac disease,

preventive services, kidney or bladder conditions, mental health and substance abuse

diagnoses, diabetes, and gastrointestinal disorders)

https://www.ahrq.gov/data/apcd/confrpt.html

Under “Data Release”

- States: States vary in their APCD release practices. This roundtable identified several core principles of data release that should apply to APCDs:

Maintain the privacy of the patient at all times. If specified in law or regulation do not release/identify individual payers and/or providers.

Promote use of the data by data agency and researchers outside the organization for the public good.

Balance the minimum necessary release with operational overhead of cutting multiple files. Data sales can be an important source of revenue to ensure the APCD's sustainability and should be considered when drafting release policies. However, pricing considerations should factor in research and public agency applications.

https://www.dol.gov/agencies/ebsa/about-ebsa/about-us/state-all-payer-claims-databases-

Under "Advisory-Committee"

- States: The State All Payer Claims Databases Advisory Committee (SAPCDAC) was established in 2021. The SAPCDAC was established by Section 735 of ERISA (as added by section 115(b) of the No Surprises Act, enacted as part of the Consolidated Appropriations Act 2021 (Dec. 27, 2020)). The SAPCDAC will advise the Secretary of Labor on the standardized reporting format for the voluntary reporting by group health plans to State All Payer Claims Databases, as well as guidance provided to States on the process by which States may collect such data. The SAPCDAC must submit a report that includes recommendations on the establishment of the format and guidance by June 25, 2021.

15. FTC: Record Sharing, HIPAA and the FTC ACT States:

https://www.ftc.gov/business-guidance/resources/sharing-consumer-health-information-look-hipaa-ftc-act

Does your business collect and share consumer health information? When it comes to privacy, you've probably thought about the Health Insurance Portability and Accountability Act (HIPAA). But did you know that you also need to comply with the Federal Trade Commission (FTC) Act? This means if you share health information, it's not enough to simply consider the HIPAA regulations. You also must make sure your disclosure statements are not deceptive under the FTC Act.

HIPAA

Let's start with HIPAA. The HIPAA Privacy Rule requires certain entities to protect the privacy and security of health information. The Rule also provides consumers with certain rights with respect to their information. This Rule applies to you if you are a *HIPAA covered entity*— a health plan, most health care providers, or a health care clearinghouse. It also applies if you are a *business associate* – a person or company that helps a covered entity carry out its health care activities and functions. Here are some highlights of the HIPAA Privacy Rule requirements for covered entities and business associates:

- In order for you to use or disclose consumer health information for commercial activities besides treatment, payment, health care operations, or other uses and disclosures permitted or required by the Privacy Rule, the consumer must first give you written permission through a **valid HIPAA authorization**.
- HIPAA authorizations provide consumers a way to understand and control their health information. The authorization must be in **plain language**. If people can't understand it, then it isn't effective. Think about who, what, when, where and why. Explain who is disclosing and receiving the information, what they are receiving, when the disclosure permission expires, where information is being shared, and why you are sharing it.
- The authorization must include **specific terms and descriptions.** For example, if you want consumers to authorize you to share their health information, you need to tell them

specifically how it will be used – for example, by a pharmaceutical company for marketing purposes, a life insurer for coverage purposes, or an employer for screening purposes.

If you are a business associate, there's a crucial first step: **the covered entity must give you explicit permission through a HIPAA business associate contract** to use or disclose health information.This means you cannot ask a consumer to sign a HIPAA authorization if your business associate contract does not expressly permit you to do so.

FTC Act

Once you've drafted a HIPAA authorization, you can't forget the FTC Act. The FTC Act prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce. Among other things, this means that companies must not mislead consumers about what is happening with their health information.

What does that mean, in practice? You need to do more than just meet the requirements for a HIPAA-compliant authorization. Your business must consider all of your statements to consumers to make sure that, taken together, they don't create a deceptive or misleading impression. Even if you believe your authorization meets all the elements required by the HIPAA Privacy Rule, if the information surrounding the authorization is deceptive or misleading, that's a violation of the FTC Act.

What can you do to comply with the FTC Act?

- Review your entire user interface. Don't bury key facts in links to a privacy policy, terms of use, or the HIPAA authorization. For example, if you're claiming that a consumer is providing health information only to her doctor, don't require her to click on a "patient authorization" link to learn that it is also going to be viewable by the public. And don't promise to keep information confidential in large, boldface type, but then ask the consumer in a much less prominent manner to sign an authorization that says you will share it. Evaluate the size, color and graphics of all of your disclosure statements to ensure they are clear and conspicuous.
- Take into account the various devices consumers may use to view your disclosure claims. If you are sharing consumer health information in unexpected ways, design your interface so that "scrolling" is not necessary to find that out. For example, you can't promise not to share information prominently on a webpage, only to require consumers to scroll down through several lines of a HIPAA authorization to get the full scoop.
- Tell consumers the full story before asking them to make a material decision – for example, before they decide to send or post information that may be shared publicly. Review your user interface for contradictions and get rid of them.
- The same requirements apply to paper disclosure statements. Don't give consumers a stack of papers where the top page says that their health information is going to their doctor, but another page requests permission to share that health information with a pharmaceutical firm.

For additional guidance on creating effective disclosures, check out the FTC's .com Disclosures report. If you have a health app, don't forget to consult the mobile health apps interactive tool, the FTC's best practices guidance for mobile health app developers and the OCR developer portal. And when you're telling consumers about how you share consumer health information, always remember the FTC Act as well as HIPAA. October 2016

16. **https://www.hhs.gov/sites/default/files/fy2022-gdm-operating-plan.pdf**

Dept of Health and Human Services Fiscal Year 2022 Budget

Office of the National Coordinator for Health IT (ONC): $86,614,000

17. **NIH article on Ethical Issues in Patient Data Ownership**

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8178732/

Addresses the need for HIPAA revisions to protect patient privacy.

18. **Washington State passes "My Health My Data" act, April, 2023**

https://iapp.org/resources/article/washington-my-health-my-data-act-overview/

This is what CT needs to establish ASAP.

19. **NIH Data Sharing Policy**
    https://www.hhs.gov/ohrp/sachrp-committee/recommendations/august-12-2020-attachment-a-nih-data-sharing-policy/index.html
20. **ONC partners with JASON regarding AI and healthcare.**

    https://irp.fas.org/agency/dod/jason/
    https://www.healthit.gov/hitac/committees/jason-task-force

    JASON Report on AI and Healthcare on the ONC site, 2017
    https://www.healthit.gov/sites/default/files/jsr-17-task-002_aiforhealthandhealthcare12122017.pdf

Connecticut HIE, HIPAA and Privacy Facts

1. **CT statute on Privileged Communicatoin between mental health providers and patients.**
   https://www.cga.ct.gov/current/pub/chap_899.htm#sec_52-146d

- Sec. 52-146d. (Formerly Sec. 52-146a). Privileged communications between psychiatric mental health provider and patient. Definitions. As used in sections 52-146d to 52-146i, inclusive:

"Authorized representative" means (A) a person empowered by a patient to assert the confidentiality of communications or records which are privileged under sections 52-146c to 52-146i, inclusive, or (B) if a patient is deceased, his or her personal representative or next of kin, or (C) if a patient is incompetent to assert or waive his privileges hereunder, (i) a guardian or conservator who has been or is appointed to act for the patient, or (ii) for the purpose of maintaining confidentiality until a guardian or conservator is appointed, the patient's nearest relative;

(2) “Communications and records” means all oral and written communications and records thereof relating to diagnosis or treatment of a patient's mental condition between the patient and a psychiatric mental health provider, or between a member of the patient's family and a psychiatric mental health provider, or between any of such persons and a person participating under the supervision of a psychiatric mental health provider in the accomplishment of the objectives of diagnosis and treatment, wherever made, including communications and records which occur in or are prepared at a mental health facility;

(3) “Consent” means consent given in writing by the patient or his authorized representative;

(4) “Identifiable” and “identify a patient” refer to communications and records which contain (A) names or other descriptive data from which a person acquainted with the patient might reasonably recognize the patient as the person referred to, or (B) codes or numbers which are in general use outside of the mental health facility which prepared the communications and records;

(5) “Mental health facility” includes any hospital, clinic, ward, psychiatric mental health provider's office or other facility, public or private, which provides inpatient or outpatient service, in whole or in part, relating to the diagnosis or treatment of a patient's mental condition;

(6) “Patient” means a person who communicates with or is treated by a psychiatric mental health provider in diagnosis or treatment;

(7) “Psychiatric mental health provider” means a physician specializing in psychiatry and licensed under the provisions of sections 20-9 to 20-12, inclusive, an advanced practice registered nurse licensed under chapter 378 who is board certified as a psychiatric mental health provider by the American Nurses Credentialing Center, a person licensed to practice medicine who devotes a substantial portion of his or her time to the practice of psychiatry or a person reasonably believed by the patient to be so qualified.

- Sec. 52-146o. Disclosure of patient communication or information by physician, surgeon or health care provider prohibited. (a) Except as provided in sections 52-146c to 52-146j, inclusive, sections 52-146p, 52-146q and 52-146s, and subsection (b) of this section, in any civil action or any proceeding preliminary thereto or in any probate, legislative or administrative proceeding, a physician or surgeon, licensed pursuant to section 20-9, or other licensed health care provider, shall not disclose (1) any communication made to him or her by, or any information obtained by him or her from, a patient or the conservator or guardian of a patient with respect to any actual or supposed physical or mental disease or disorder, or (2) any information obtained by personal examination of a patient, unless the patient or that patient's authorized representative explicitly consents to such disclosure.

  (b) Consent of the patient or the patient's authorized representative shall not be required for the disclosure of such communication or information (1) pursuant to any statute or regulation of any state agency or the rules of court, (2) by a physician, surgeon or other licensed health care provider against whom a claim has been made, or there is a reasonable belief will be made, in such action or proceeding, to the physician's, surgeon's or other licensed health care provider's attorney or professional liability insurer or such insurer's agent for use in the defense of such action or

proceeding, (3) to the Commissioner of Public Health for records of a patient of a physician, surgeon or health care provider in connection with an investigation of a complaint, if such records are related to the complaint, or (4) if child abuse, abuse of an elderly individual, abuse of an individual who is physically disabled or incompetent or abuse of an individual with intellectual disability is known or in good faith suspected.

- Sec. 52-146e. Disclosure of communications. (a) All communications and records as defined in section 52-146d shall be confidential and shall be subject to the provisions of sections 52-146d to 52-146j, inclusive. Except as provided in sections 52-146f to 52-146i, inclusive, no person may disclose or transmit any communications and records or the substance or any part or any resume thereof which identify a patient to any person, corporation or governmental agency without the consent of the patient or his authorized representative.

(b) 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.

(c) The patient or his authorized representative may withdraw any consent given under the provisions of this section at any time in a writing addressed to the person or office in which the original consent was filed. Withdrawal of consent shall not affect communications or records disclosed prior to notice of the withdrawal.

Sec. 52-146k. Privileged communications between victim and domestic violence counselor or sexual assault counselor.

Sec. 52-146n. Disclosure of confidential communications between Judicial Department employee and employee assistance program counselor prohibited. Information re participation in employee assistance program.

Sec. 52-146p. Disclosure of privileged communications between marital and family therapist and person consulting such therapist prohibited. Exceptions (includes consent)

Sec. 52-146q. Disclosure of confidential communications between social worker and person consulting such social worker prohibited. Exceptions.

Sec. 52-146r. Disclosure of confidential communications between government attorney and public official or employee of public agency prohibited.

Sec. 52-146s. Disclosure of confidential information between professional counselor and person consulting such professional counselor prohibited. Exceptions.

Sec. 52-146v. Disclosure of confidential communications between peer support team member and first responder prohibited. Exceptions.

Sec. 52-146w. Disclosure of patient communication or information relating to reproductive health care services by covered entity prohibited. Exceptions.

Sec. 52-146x. Disclosure of patient communication or information relating to gender-affirming health care services or reproductive health care services by covered entity prohibited. Exceptions

2. **CT has APCD (All Payor Claims Databases) since 2012. That is now managed under OHS, along with Connie Exchange (CE).**

Federal Agency for Healthcare Research and Quality

https://www.ahrq.gov/data/apcd/index.html

- Under "Overview of All-Payer Claims Databases"

States: All-payer claims databases (APCDs) are large State databases that include medical claims, pharmacy claims, dental claims, and eligibility and provider files collected from private and public payers.

APCD data are reported directly by insurers to States, usually as part of a State mandate. There is national and local momentum to establish and implement APCDs. To date, 18 States have legislation mandating the creation and use of APCDs or are actively establishing APCDs

- Under "All-Payer Claims Databases Measurement of Care: Systematic Review and Environmental Scan of Current Practices and Evidence"

States: Barrier 1: Missing Data Elements

APCDs are currently primarily built on administrative claims data submitted by health plans (preferably with Medicare claims as well). However, several factors affect the completeness of the data that are submitted.

There are also restrictions regarding data from potentially sensitive claims, such as those related to behavioral and mental health, HIV, and worker's compensation.

Furthermore, data are typically limited to claims only. Any other data sources, such as public health data, electronic health record data, and aspects of hospital care that are part of a bundled payment (e.g., medications) that are not captured within submitted claims are not present in the APCD

Finally, States or external organizations could develop public report cards for the completeness of data submission by insurers.

3. **CT APCD**

https://portal.ct.gov/-/media/OHS/Health-IT-Advisory-Council/APCD-Advisory-Group/Charters/APCD-AG_Charter-08112022_final.pdf

- Under "Group Charter" All-Payer Claims Database Advisory Group

August 11, 2022 Article 1: Name

States: Section 1: The name of this this workgroup is the All-Payer Claims Database Advisory Group

(APCD-AG), legislatively established in 2012 as the APCD Advisory Council, and then on October 31, 2017 as a workgroup of the Health Information Technology Advisory Council (HITAC).

- OHS APCD

Article 2: Purpose

Section 1: Connecticut General Statute Section (CGS §) 17b-59f established the HITAC to advise the executive director of the Office of Health Strategy (OHS) and Connecticut's Health Information Technology Officer in developing priorities and policy recommendations to advance CT's health information technology and health information exchange efforts and goals. The APCD-AG, as set forth in this Charter, was established as a working group of the HITAC by subsection (e)(1) of CGS § 17b-59f to "implement a state-wide multipayer data initiative to enhance the state's use of health care data from multiple sources to increase efficiency, enhance outcomes and improve the understanding of health care expenditures in the public and private sectors." CGS § 19a-755a-b enumerates the goals of CT's APCD program:

- To be made available to any state agency, insurer, employer, health care provider, consumer, or researcher to review healthcare services utilization, costs and quality while protecting patient privacy;

4. OHS Data Compendium

https://portal.ct.gov/OHS/Pages/Data-Compendium

Download the excel file to see all the variables that FOI requests can access. All provider, client, employer, diagnosis codes, dates of service and amounts billed and paid.

5. **CT OHS Environmental Scan Report**

https://portal.ct.gov/-/media/OHS/Health-IT-Advisory-Council/Publications/20170517_Environmental-Scan-Report_Summary-of-Comments.pdf

- Under "Environmental Scan Summary of Findings and Priority Recommendations 2017"

States: Summary of Comments

Summary of Council Members Comments

¬Couple of suggestions to an overall excellent document. Court Support Services Division (CSSD) part of the Judicial Branch don't seem represented or mentioned in the list of state agencies. They oversee probation, Behavioral Health (BH) providers submit a fair amount of data to them. They are often overlooked because they are not part of the executive branch but I believe they

should be part of any HIT steering committee.

6. **CT OHS Statewide Health IT Plan**

https://portal.ct.gov/-/media/OHS/Health-IT-Advisory-Council/Publications/Connecticut-Statewide-Health-IT-Plan-amended.pdf

- Under "CT Statewide Health Information Technology Plan"

States: Focus area 4: Support Behavioral Health Providers with Adaption of EHR and HIE Services. 2/2022, page 11.

Some sectors of the healthcare delivery system continue to lag in terms of EHR adoption, including behavioral health providers in Connecticut. Compared to other stakeholder groups, many of them expressed a strong desire to exchange data with fellow behavioral health providers and, to a lesser extent, with other types of medical care providers. During the environmental scan in the first half of 2021, a considerable number of survey respondents – about a quarter – indicated opposition to data sharing, citing patient confidentiality as the reason. Given the diversity of opinion among behavioral health providers and concerns from patients regarding the privacy of their records, more research and outreach will be required to better understand both the opportunities and the challenges related to the use of information technology and electronic information exchange in this specialty area. In recent years, EHR and care coordination platform vendors have made huge strides in product support for behavioral health providers; because this domain was left out of the Medicare and Medicaid EHR Incentive Programs, however, there are a significant number of independent and small practice providers who generally are not documenting care outside of their handwritten visit notes. With the strong push for primary care and behavioral health care integration, in large part due to the common occurrence of comorbidities such as depression and chronic disease, it is valuable for practitioners of this specialty to receive support in the form of education, technical assistance, mentorship, and most of all, financial incentives for adoption and use of certified EHR technology.

- Key Considerations

¬Consider behavioral health provider incentives including leveraging federal funding sources to support providers in implementing adequate privacy and security protocols as they adopt and use new information technology systems.

¬Consider the growth of telehealth in the behavioral health realm and include requirements, as well as funding, for an audit program (inclusive of telehealth providers

and practices) as part of any EHR incentive program or hosted EHR or care coordination offering.

¬It is important to better understand the perspectives and needs of behavioral health providers and patients before implementing new policies, funding, or other incentives.

¬ Providing a hosted EHR and/or a care coordination option for behavioral health practices accepting Medicaid payments would be a significant step toward more holistic, person-centered care; look for consent management services as part of that package.

7. **OHS Health IT Statewide Health IT Plan**

https://portal.ct.gov/-/media/OHS/Health-IT-Advisory-Council/Publications/Connecticut-Statewide-Health-IT-Plan-amended.pdf#:~:text=The%20Council%20in%20its%20advisory%20capacity%20to%20the,health%20IT%20projects%2C%20meeting%20monthly%20since%20its%20inception.

- Under "Focus Area 4: Support Behavioral Health Providers with Adoption of HER and HIE

States: Some sectors of the healthcare delivery system continue to lag in terms of EHR adoption, including behavioral health providers in Connecticut. Compared to other stakeholder groups, many of them expressed a strong desire to exchange data with fellow behavioral health providers and, to a lesser extent, with other types of medical care providers. During the environmental scan in the first half of 2021, a considerable number of survey respondents – about a quarter – indicated opposition to data sharing, citing patient confidentiality as the reason. Given the diversity of opinion among behavioral health providers and concerns from patients regarding the privacy of their records, more research and outreach will be required to better understand both the opportunities and the challenges related to the use of information technology and electronic information exchange in this specialty area. In recent years, EHR and care coordination platform vendors have made huge strides in product support for behavioral health providers; because this domain was left out of the Medicare and Medicaid EHR Incentive Programs, however, there are a significant number of independent and small practice providers who generally are not documenting care outside of their handwritten visit notes. With the strong push for primary care and behavioral health care integration, in large part due to the common occurrence of comorbidities such as depression and chronic disease, it is valuable for practitioners of this specialty to receive support in the form of education, technical assistance, mentorship, and most of all, financial incentives for adoption and use of certified EHR technology.

- Key Considerations

¬Consider behavioral health provider incentives including leveraging federal funding sources to support providers in implementing adequate privacy and security protocols as they adopt and use new information technology systems.

¬Consider the growth of telehealth in the behavioral health realm and include requirements, as well as funding, for an audit program (inclusive of telehealth providers and practices) as part of any EHR incentive program or hosted EHR or care coordination offering.

¬ It is important to better understand the perspectives and needs of behavioral health providers and patients before implementing new policies, funding, or other incentives.

¬ Providing a hosted EHR and/or a care coordination option for behavioral health practices accepting Medicaid payments would be a significant step toward more holistic, person centered care; look for consent management services as part of that package.

- Under Focus area 5:

  States: Protect the Privacy of Individual and Family Health Information Connecticut legislators have a long legacy of taking actions to protect individual privacy and have put special protections in statute for behavioral health information. These regulations would need to be reviewed periodically when technology advancements occur, such as the statewide HIE in Connecticut.

8. Department of Public Health CGS Chapter 368a*

https://www.cga.ct.gov/current/pub/chap_368a.htm#sec_19a-25c

Sec. 19a-25a. Regulations re electronic signatures for medical records. The Commissioner of Public Health shall adopt regulations, in accordance with the provisions of chapter 54, if he deems such regulations are necessary to implement the use of electronic signatures for medical records maintained in hospitals as defined in section 19a-490. Until such regulations are promulgated, hospitals shall submit to the Department of Public Health for review and approval, any current or proposed protocol for the use of electronic signatures for medical records including, but not limited to, protections for patient confidentiality and medical record security.

Sec. 19a-25c. Medical records systems: Electronic and paper formats authorized. A health care institution licensed by the Department of Public Health pursuant to chapter 368v may create, maintain or utilize medical records or a medical records system in electronic format, paper format or both, provided such records or system is designed to store medical records or patient health information in a medium that is reproducible and secure.

- **CT Health Information Network Plan (Eventually became Connie Exchange)**

Under "CGS 19a-25e

States: Sec. 19a-25e. Connecticut Health Information Network plan. (a) The Department of Public Health and The University of Connecticut Health Center may, within available

appropriations, develop a Connecticut Health Information Network plan to securely integrate state health and social services data, consistent with state and federal privacy laws, within and across The University of Connecticut Health Center and the Departments of Public Health, Developmental Services and Children and Families. Data from other state agencies may be integrated into the network as funding permits and as permissible under federal law.

(b) The Department of Public Health and The Center for Public Health and Health Policy at The University of Connecticut Health Center shall collaborate with the Departments of Administrative Services, Developmental Services, and Children and Families to develop the Connecticut Health Information Network plan.

(c) The plan shall: (1) Include research in and describe existing health and human services data; (2) inventory the various health and human services data aggregation initiatives currently underway; (3) include a framework and options for the implementation of a Connecticut Health Information Network, including query functionality to obtain aggregate data on key health indicators within the state; (4) identify and comply with confidentiality, security and privacy standards; and (5) include a detailed cost estimate for implementation and potential sources of funding.

- Under: Sec. 19a-25f. Disclosure of personally identifiable information by state agencies to the Connecticut Health Information Network.
  Notwithstanding any provision of this chapter or chapter 14, 319, 319b, 319o, 319t, 319v or 368z, or any regulation adopted pursuant to said chapters, the state agencies that participate in the Connecticut Health Information Network, subject to federal restrictions on disclosure or redisclosure of information, may disclose personally identifiable information held in agency databases to the administrator of the Connecticut Health Information Network and its subcontractors for the purposes of (1) network development and verification, and (2) data integration and aggregation to enable response to network queries. No state agency that participates in the Connecticut Health Information Network shall disclose personally identifiable information to the Connecticut Health Information Network if such disclosure would constitute a violation of federal law, including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191) (HIPAA), as amended from time to time, and the Family Educational Rights and Privacy Act of 1974, 20 USC 1232g, (FERPA), as amended from time to time, and any regulations promulgated thereunder at 34 CFR Part 99. The administrator of the Connecticut Health Information Network and its subcontractors shall not disclose personally identifiable information.

9. **CT Generl Statutes on Connie Exchange Under Social Services**
   https://www.cga.ct.gov/current/pub/chap_319o.htm#sec_17b-59a

- Sec. 17b-59a. (Formerly Sec. 4-60i). Development of uniform information and technology standards. Health information technology plan. Electronic data standards. State-wide Health Information Exchange. Report
- Sec. 17b-59d. State-wide Health Information Exchange. Established.

- Sec. 17b-59a. (Formerly Sec. 4-60i). Development of uniform information and technology standards. Health information technology plan. Electronic data standards. State-wide Health Information Exchange. Report. (a) As used in this section:

(1) “Electronic health information system” means an information processing system, involving both computer hardware and software that deals with the storage, retrieval, sharing

and use of health care information, data and knowledge for communication and decision making, and includes: (A) An electronic health record that provides access in real time to a patient's complete medical record; (B) a personal health record through which an individual, and anyone authorized by such individual, can maintain and manage such individual's health information; (C) computerized order entry technology that permits a health care provider to order diagnostic and treatment services, including prescription drugs electronically; (D) electronic alerts and reminders to health care providers to improve compliance with best practices, promote regular screenings and other preventive practices, and facilitate diagnoses and treatments; (E) error notification procedures that generate a warning if an order is entered that is likely to lead to a significant adverse outcome for a patient; and (F) tools to allow for the collection, analysis and reporting of data on adverse events, near misses, the quality and efficiency of care, patient satisfaction and other healthcare-related performance measures.

- (b) The Commissioner of Social Services, in consultation with the executive director of the Office of Health Strategy, established under section 19a-754a, shall (1) develop, throughout the Departments of Developmental Services, Public Health, Correction, Children and Families, Veterans Affairs and Mental Health and Addiction Services, uniform management information, uniform statistical information, uniform terminology for similar facilities, and uniform electronic health information technology standards, (2) plan for increased participation of the private sector in the delivery of human services, and (3) provide direction and coordination to federally funded programs in the human services agencies and recommend uniform system improvements and reallocation of physical resources and designation of a single responsibility across human services agencies lines to facilitate shared services and eliminate duplication.

10. Health Information Technology

https://www.cga.ct.gov/current/pub/chap_368dd.htm

- Sec. 19a-754a. Office of Health Strategy established. (a) There is established an Office of Health Strategy, which shall be within the Department of Public Health for administrative purposes only. The department head of said office shall be the executive director of the Office of Health Strategy, who shall be appointed by the Governor in accordance with the provisions of sections 4-5 to 4-8, inclusive, with the powers and duties therein prescribed

11. OHS Health Systems Planning Unit

https://www.cga.ct.gov/current/pub/chap_368z.htm#sec_19a-612

- Sec. 19a-612. Health Systems Planning Unit within Office of Health Strategy. (a) There is established, within the Office of Health Strategy, established under section 19a-754a, a unit to be known as the Health Systems Planning Unit. The unit, under the direction of the executive director of the Office of Health Strategy, shall constitute a successor to the former Office of Health Care Access, in accordance with the provisions of sections 4-38d and 4-39.

(b) Any order, decision, agreed settlement or regulation of the former Office of Health Care Access which is in force on July 1, 2018, shall continue in force and effect as an order or

regulation of the Office of Health Strategy until amended, repealed or superseded pursuant to law.

Sec. 19a-613. Powers and duties. Data collection. (a) The Health Systems Planning Unit may employ the most effective and practical means necessary to fulfill the purposes of this chapter, which may include, but need not be limited to:

(1) Collecting patient-level outpatient data from health care facilities or institutions, as defined in section 19a-630;

(2) Establishing a cooperative data collection effort, across public and private sectors, to assure that adequate health care personnel demographics are readily available; and

(3) Performing the duties and functions as enumerated in subsection (b) of this section.

(b) The unit shall: (1) Authorize and oversee the collection of data required to carry out the provisions of this chapter; (2) oversee and coordinate health system planning for the state; (3) monitor health care costs; and (4) implement and oversee health care reform as enacted by the General Assembly.

12 . DPH Office of Health Care Access

https://portal.ct.gov/DPH/Communications/About-Us/Office-of-Health-Care-Access

The major functions of the Office of Health Care Access (OHCA) include the administration of the certificate of need (CON) program; preparation of the State-wide Health Care Facilities and Services Plan; health care data collection, analysis and reporting; and hospital financial review and reporting.

OHCA has statutory authority to gather and analyze significant amounts of hospital financial, billing and discharge data. Information collected, verified, analyzed and reported on includes hospital expenses and revenues, uncompensated care volumes, and other financial data as well as hospital utilization, demographic, clinical, charge, payer and provider statistics.

13.OHS State Innovation Model

https://portal.ct.gov/-/media/OHS/Healthcare-Cabinet/2016-Meetings/State-Innovation-Model_HCC_Description_6-14-16_Final-(003).pdf

Under: 2020 Goals: State Innovation Model Draft Driver Diagram

~Provide transparency on cost and quality by creating a public common scorecard to report provider performance

~States: All payers in CT use financial incentives to reward improved quality and reduced cost: launch Medicaid Quality Improvement & Shared Savings Program (MQISSP)

~States: Create a statewide multi-payer core quality measure set for use in value-based payment models
Develop and deploy measurement solutions to support the

use by all payers of EHR-based, outcome, health equity and care experience measures in value-based payment scorecards

~Community & Clinical Integration Program (CCIP): Provide technical assistance & awards to MQISSP participating entities to achieve best-practice standards in: comprehensive care management; health equity improvement; & behavioral health integration

14.The State of Connecticut State Innovation Model Final & Annual Report 2019-2020

https://portal.ct.gov/-/media/OHS/SIM/Work-Stream-Updates/Final-AY4-Annual-Report_SIM_Master.pdf

Under "Public Scorecard"
States: How it helps: Health care payers track performance measures to determine whether providers meet quality goals for the purpose of value-based payment arrangements, including PCMH+. The public scorecard will share provider network scores on certain measures, including care experience. This will allow consumers to compare provider quality and make informed healthcare decisions

.

15.CT health insurance exchange, Access Health Ct, failed to report 44 privacy breaches, April, 2022.

https://healthitsecurity.com/news/ct-health-insurance-exchange-failed-to-report-44-breaches-audit-finds

16.US Department of Justice

Justice-Involved Health Information: Policy and Practice Advances in Connecticut, 2014
https://www.ojp.gov/ncjrs/virtual-library/abstracts/justice-involved-health-information-policy-and-practice-advances

- States: This report describes three initiatives in Connecticut that facilitate the sharing of offender health information among corrections and community healthcare providers, so as to ensure the continuity of healthcare after release from confinement.

The third initiative, the Connecticut Health Information Network (CHIN), is a federated network that enables the integration and sharing of diverse data for State-level policy purposes. CHIN provides access to appropriate health, human service, and education information across State agency databases for agency personnel, policymakers, researchers, and government officials.

17.CT Department of Social Services

https://portal.ct.gov/DSS/ITS/DSS-HealthIT/Business-Intelligence-and-DSS-HealthIT/Enterprise-Master-Person-Index

- **Enterprise Master Person Index (EMPI)**

Coordinated, accountable, patient-centered care is reliant on seamlessly orchestrated access to data and a consolidated view of an individual's health history. Driven by its vision of a fully-integrated, person-centered system, facilitating efficient and evidence-based healthcare delivery for all its residents, DSS implemented an Enterprise Master Person Index (EMPI) in January 2016. The EMPI uniquely identifies individuals across a myriad of systems, settings and populations to enable a single, unified health record for statewide outcomes improvement and real-time health information exchange. Essentially, the EMPI serves as an enterprise solution for maintaining consistent, accurate and current demographic data, ensuring that each individual is represented once across all subscribing systems.

The EMPI serves as an authoritative source of information by instituting consistent, accurate and current demographic data on individuals receiving services from the State using an enterprise unique identifier. By encompassing accurate person identification at every point across the network, DSS is able to build a total picture of each individual for coordinated care improvements, population health initiatives, operational efficiency and treatment plan success.

Today, the EMPI is used by the state's eligibility and enrollment system (DSS-ImpaCT), the state's Health Insurance Exchange (HIX) system Access Health Connecticut (AhCT), and The Office of Early Childhood. EMPI is hosted by the State's Bureau of Enterprise Systems and Technology (BEST). The state uses NextGate as its EMPI solution provider.

Currently, Phase II (2019-20) work includes 1) onboarding additional subscribing systems, 2) implementing the Relation Registry, and 3) integration with the Medicaid HIE platform (HealthShare) to support Project Notify and the Personal Health Record. Preliminary discussions have occurred with at least nine sister agencies, with six agencies expressing interest in the use of this technology. Many state agencies operate/purchase/create independent identity management solutions to support direct care delivery functions. A shared technology solution can support interoperability within and across agencies as well as support the exchange of information to coordinate services and support better care for people.

The Department of Social Services (DSS) is responsible for Health Information Technology (Health IT), including Health Information Exchange (HIE) for the State's Medicaid population. The DSS has made steady progress on implementing its roadmap for Health IT and HIE in Connecticut focusing on Medicaid beneficiaries. Our strategic goals are aligned with Health IT vision and goals of the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS). This vision is anchored in providing an integrated person-centered system facilitating, efficient and evidence-based health care delivery for all Connecticut residents.

18.CT DSS Health Information Service Provider for Direct Secure Messaging

https://portal.ct.gov/-/media/Departments-and-Agencies/DSS/DSS-Health-IT/direct_faq.pdf

- In April of 2014, the State of Connecticut Department of Social Services (DSS)

established a Health Information Service Provider (HISP)1 in order to provide Direct Secure Messaging for eligible providers (EPs) participating in the Medicaid Electronic Health Record (EHR) Incentive Program and their referral partners.

19.Legislation proposed to require patients to opt-in with written consent to electronic health exchanges.

https://www.cga.ct.gov/2011/FC/2011SB-01147-R000429-FC.htm

This states it took effect October 1, 2011.

https://www.cga.ct.gov/2011/jfr/s/2011SB-01147-R00HS-JFR.htm

Comments on the proposal of the bill: DSS Commissioner was against requiring written consent because the exchange wouldn't succeed if they required consent.

20.CT Personal Health Information Disclosure

https://www.cga.ct.gov/2016/rpt/2016-R-0050.htm

21.Connecticut Data Privacy Act

https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF

https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act (p 7 exemptions)

On May 10, 2022, Governor Ned Lamont signed Senate Bill 6: An Act Concerning Personal Data Privacy and Online Monitoring.
The CTDPA gives Connecticut residents certain rights over their personal data and establishes responsibilities and privacy protection standards for data controllers that process personal data. It protects a Connecticut resident acting in an individual or household context, such as browsing the Internet or making a purchase at a store. It does not protect an individual acting in an employment context, such as applying for a job.

The CTDPA applies to people who conduct business in Connecticut or who produce products or services targeted to Connecticut residents and that, during the prior calendar year, controlled or processed the personal data of:

- at least 100,000 consumers; or
- 25,000 or more consumers and derived over 25% of gross revenue from the sale of personal data.

It also applies to service providers (called "processors") that maintain or provide services involving personal data on behalf of covered businesses.

The key distinction between a controller and a processor is their decision-making authority over personal data. Under the CTDPA, a processor may only process data at the request and under the direction of a controller. The processor is contractually bound by the controller's instructions as to what the processor must and may do with personal data. If a processor were to begin exercising decision-making authority with respect to the purposes and means of personal data processing, it would become a controller with respect to that processing and subject to the obligations imposed on controllers under the CTDPA.

Sensitive data is a subset of personal data that includes:

- Any data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual activity or orientation, citizenship, or immigration status;
- Genetic or biometric data used to uniquely identify an individual;
- Personal data of a child under the age of 13; and
- Information that identifies an individual's specific location with a defined degree of precision and accuracy (called "precise geolocation data").

Under the CTDPA, a controller needs a consumer's consent to process sensitive data. Universal opt-out mechanisms are designed to afford consumers the ability to communicate a request to opt-out of the processing of their personal data across multiple websites at once, rather than having to make individual opt-out requests through each controller's website. Under the CTDPA, universal opt-out mechanisms must be recognized by controllers as valid consumer requests beginning January 1, 2025.

22.American Health information Management Association Sample "Right to restrict records" form

https://library.ahima.org/doc?oid=300415

23. Insurer's Policies on Connie Exchange

- Anthem sharing data with Connie Exchange

https://www.anthem.com/privacy/

- Anthem on data sharing, CARIN Alliance, Interoperability

https://www.bcbs.com/sites/default/files/file-attachments/page/Final%20final%20Interop_OnePager_g.pdf

- Cigna on CT Privacy Rights

https://www.cigna.com/static/www-cigna-com/docs/cigna-us-state-law-privacy-notice.pdf

- Cigna on privacy, data, CARIN and apps

https://www.cigna.com/legal/privacy/sharing-and-protecting-your-health-care-data

- UCONN Health on Connie Exchange – with various information videos

https://health.uconn.edu/health-interoperability-learning/health-it-for-clinicians/introducing-connie-our-state-recognized-hie/

- Connecticare privacy policy with no mention of HIE or Connie Exchange.

https://www.connecticare.com/content/dam/connecticare/pdfs/legal/privacy_notice.pdf

- Hartford Hospital Privacy Practice and HIE

  https://www.connecticare.com/content/dam/connecticare/pdfs/legal/privacy_notice.pdf

- Yale New Haven Hospital Privacy Policy with no mention of HIE or Connie Exchange
  https://www.ynhh.org/patients-visitors/patient-rights-responsibilities/your-privacy
- ECHN Privacy Practice on Connie Exchange
  https://www.echn.org/about-echn/privacy-protection/
- Middlesex Hospital
  https://middlesexhealth.org/files/dmHTMLFile/cc2229-middlesex-joint-notice-of-privacy-practices-04.01.20.pdf