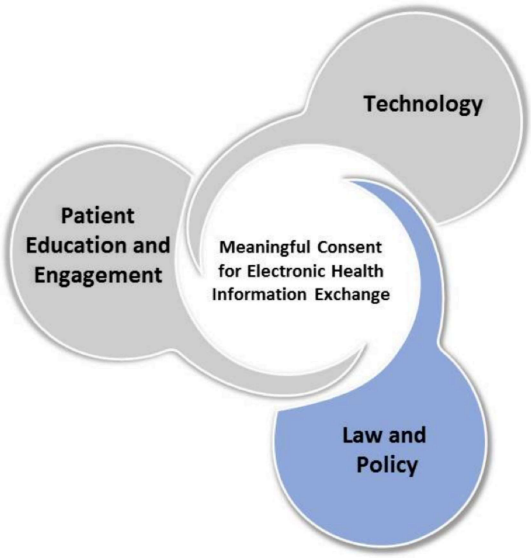
Health Information Privacy Law and Policy

What Type of Patient Choice Exists Under HIPAA?

Most health care providers must follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Privacy Rule), a federal privacy law that sets a baseline of protection for certain individually identifiable health information ("health information").

The Privacy Rule generally permits, but does not require, covered health care providers to give patients the choice as to whether their health information may be disclosed to others for certain key purposes. These key purposes include treatment, payment, and health care operations.



How Can Patient Choice Be Implemented in Electronic Health Information Exchange (eHIE)?

While it is not required, health care providers may decide to offer patients a choice as to whether their health information may be exchanged electronically, either directly or through a Health Information Exchange Organization (HIE). That is, they may offer an "opt-in" or "opt-out" policy [PDF - 713 KB] or a combination.

Are There Specific Legal Requirements for Opt-In or Opt-Out Policies?

The U.S. Department of Health and Human Services (HHS) does not set out specific steps or requirements for obtaining a patient's choice whether to participate in eHIE. However, adequately informing patients of these new models for exchange and giving them the choice whether to participate is one means of ensuring that patients trust these systems. Providers are therefore encouraged to enable patients to make a "meaningful" consent choice rather than an uninformed one.

You can read more about patient choice and eHIE in guidance released by the Office for Civil Rights (OCR): The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment [PDF - 164KB].

Are There Privacy Laws that Require Patient Consent?

Yes. There are some federal and state privacy laws (e.g., 42 CFR Part 2, Title 10) that require health care providers to obtain patients' written consent before they disclose their health information to other people and organizations, even for treatment. Many of these privacy laws protect information that is related to health conditions considered "sensitive" by most people.

How Does HIPAA Affect These Other Privacy Laws?

HIPAA created a baseline of privacy protection. It overrides (or "preempts") other privacy laws that are less protective. But HIPAA leaves in effect other laws that are more privacy-protective. Under this legal framework, health care providers and other implementers must continue to follow other applicable federal and state laws that require obtaining patients' consent before disclosing their health information.

The resources listed below provide links to some federal, state, and organization resources that may be of interest for those setting up eHIE policies in consultation with legal counsel. Implementers may also want to visit their state's law and policy sites for additional information.

Federal, State, and Organization Resources about Consent, Personal Choice, and Confidentiality

We encourage providers, HIEs, and other health IT implementers to seek expert advice when evaluating these resources, as privacy laws and policies continually evolve. The resources are not intended to serve as legal advice or offer recommendations based on an implementer's specific circumstances.

Federal Law, Regulation, Guidance, and Policy

Health Information in General

- **Individual Choice: The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment [PDF - 164 KB]** – guidance regarding the HIPAA Privacy Rule as it relates to the Choice Principle in the Privacy and Security Framework.

Sensitive Health Information (e.g., behavioral health information, HIV/AIDS status)

- **Mental Health and Substance Abuse: Legal Action Center in Conjunction with SAMHSA's Webinar Series on Alcohol and Drug Confidentiality Regulations (42 CFR Part 2)** – slides and videos providing an overview of alcohol and drug confidentiality rules, further explanation of SAMHSA FAQs, and supplemental material.

- **Mental Health and Substance Abuse: SAMHSA – Health Resources and Services Administration (HRSA) Center for Integrated Health Solutions** – resources and examples to help providers understand and address patient confidentiality issues, including those related to pediatrics.
- **Student Health Records: U.S. Department of Health and Human Services and Department of Education Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and HIPAA to Student Health Records [PDF - 259 KB]** – overview of FERPA, HIPAA, and where they may intersect; includes an FAQ section.
- **Family Planning: Title 42 – Public Health – 42 CFR 59.11 – Confidentiality** – federal rules about consent and confidentiality of patient information as it pertains to federally funded family planning clinics.

Policy

- **Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information [PDF - 60KB]** – ONC's privacy and security policy framework for eHIE, meant to help guide the nation's adoption of health IT and help improve the availability of health information and health care quality.
- **Privacy and Security Program Instruction Notice (PIN) for State HIEs [PDF - 258 KB]** – a common set of privacy and security requirements to help State HIE Cooperative Agreement recipients create privacy and security policies and practices for HIE services. The guidance also assists state policy leaders and other stakeholders who are setting up common privacy and security policies and practices for communities, regions, and states. The PIN can serve as a framework and offer specific direction and guidance to these efforts.
- **Governance Framework for Trusted Electronic Health Information Exchange [PDF - 300 KB]** – ONC's guiding principles on eHIE governance. The document provides a common conceptual foundation applicable to all types of governance models and expresses the principles ONC believes are most important for HIE governance. The Governance Framework does not prescribe specific solutions but lays out milestones and outcomes that ONC expects for and from HIE governance entities as they enable eHIE.
- **Principles and Strategy for Accelerating HIE [PDF - 872 KB]** – ONC's general principles and strategy for accelerating health information exchange, including focusing on privacy and security issues and potential solutions.

Federal Advisory Committee (FACA) Recommendations

- **Health IT Policy Committee's Tiger Team's Recommendations on Individual Choice [PDF - 119 KB]** – FACA recommendations to HHS on privacy and security policies and practices that will help build public trust in HIT and eHIE and enable their proper use to improve health care quality and efficiency. These recommendations informed ONC's State HIE PIN as well as the eConsent and Data Segmentation efforts.
- **Health IT Policy Committee's Tiger Team's Recommendations on Exchange of Health Information in Query Response Models and Meaningful Consent [PDF - 280 KB]** – set of recommendations on query model of exchange that include meaningful choice for patients.

State Law

Organizational Policy and Procedures

Was this page helpful?

- ◯ Yes
- ◯ No

Next

Form Approved OMB# 0990-0379 Exp. Date 9/30/2025

Content last reviewed on September 1, 2022

Resources

News

Topics

Archived Content

Links

Privacy Policy

Disclaimers

Viewers & Players

GobiernoUSA.gov

HHS Vulnerability Disclosure Policy

Connect with us: