carahsoft.
TECHNOLOGY BY POLICY

Health Insurance Portability and Accountability Act

Legislation Overview

August 21, 1996

Overview

HIPAA was created in the late 90s with the passage of the Health Insurance Portability and Accountability Act of 1996, which was signed by President Clinton.

The law established the legislative foundation for the protection of sensitive patient health information. The act also aimed to reduce fraud, ensure people could maintain health insurance between jobs, and standardize the exchange of electronic health information.

HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened HIPAA's privacy and security rules by establishing stricter penalties for non-compliance, expanding the scope of "covered entities" to include business associates, and requiring providers to notify HHS and patients when data breaches occur.

HIPAA Privacy Rule

The Standards for Privacy of Individually Identifiable Information (HIPAA's "Privacy Rule") established nationally recognized standards for the disclosure of individually identifiable health information. The Privacy Rule was officially published by HHS on December 28th, 2000.

What is Protected Health Information?

Individually identifiable health information is defined as data that can reasonably be used to identify an individual, including demographic information, relating to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual

Who the Privacy Rule Applies To

HIPAA's Privacy Rule applies to all "Covered Entities", including:

- Health Plans (payers/insurance companies)
- Health Care Providers
- Health Care Clearinghouses (data transformation/exchange organizations)
- Business Associates
    - Person or organization that handles protected health information (PHI) on behalf of a covered entity, such as an Electronic Health Record (EHR) vendor or AI software vendor
    - Must be entered into a formalized business associate contract with the covered entity where they've agreed to protection requirements of PHI

Privacy Rule Disclosure Exceptions

Under The Privacy Rule, covered entities and business associates may not share PHI without the expressed written consent of the patient, unless the use case falls under the following exceptions:

- Information is being disclosed directly with the patient
- Information is being used directly for Treatment, Payment, or Healthcare Operations (TPO)

- Informal permission is granted by the patient when given the opportunity to agree or object
- Public interest and benefit activities
    - Required directly by law
    - Public health activities conducted by government authorities like the FDA or CDC
    - Law enforcement purposes
    - Research activities approved by an accredited privacy board

De-Identification Under the Privacy Rule

If the PHI use case doesn't fall under the listed exceptions, then the only other option to use the data without patient authorization is to de-identify the data. De-identification refers to the process of removing demographic and other identifiable information from the PHI data set.

There are 2 HHS approved methods of de-identifying PHI data sets:

- **Expert Determination Method:** A person with appropriate knowledge of statistics and scientific principles renders the data unidentifiable
- **Safe Harbor Method:** Removing all identifiers including names, geographic information, contact information, SSNs, account numbers, photographs, etc..

Other HIPAA Privacy Rule Compliance Considerations

The Minimum Necessary Standard: Covered entities must not disclose more than necessary for the use case when sharing PHI

"A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being."

Department of Health and Human Services (HHS)

HIPAA Security Rule

In addition to The Privacy Rule, HHS issued The Security Rule to protect individuals' electronic PHI (ePHI). The Security Rule, published February 20th, 2003, established administrative, cyber, and physical security standards for covered entities to adhere to.

According to the rule, covered entities and business associates must follow these general rules:

- Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.
- Protect against reasonably anticipated threats to the security or integrity of the information.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce.

Covered entities and business associates are required to conduct a risk assessment and analysis of their ability to protect ePHI and address any security issues that prevent them from adhering to the above rules.

Administrative Safeguards in the Security Rule

Regulated entities must implement the following administrative safeguards:

- Security Management Process**:** Regularly conduct assessments and address security deficiencies

- Assign Security Responsibilities**:** Designate a security official to develop policies and implement compliance
- Workforce Security**:** Ensure that employees who work with ePHI have authorization and supervision
- Information Access Management**:** Implement policies and procedures for authorizing employee access to information only when access is appropriate for their job role, like the Minimum Necessary Standard of The Privacy Rule
- Security Awareness and Training**:** Train all employees on security policies and establish sanctions against workers who violate those policies
- Security Incident Procedures**:** Have a plan in place to deal with security incidents and mitigate the damage
- Contingency Plan**:** Have a plan to deal with damaged information systems that contain ePHI, including data backups and continuing business practices
- Evaluation**:** Perform periodical assessments of security policies and procedures and document findings
- Business Associate Contracts**:** Before allowing a business associate to handle ePHI, create a contract that holds them accountable to The Security Rule and overall HIPAA compliance

Physical Safeguards in the Security Rule

Regulated entities must implement the following physical safeguards:

- Facility Access Control: Limit physical access to information systems
- Workstation Use and Security: Establish policies and procedures for proper use and who can access
- Device and Media Controls: Govern hardware usage and ensure proper disposal

Technical Safeguards in the Security Rule

Regulated entities must implement the following technical safeguards:

- Access Control: Limit ePHI access only to authorized personnel
- Audit Control: Maintain hardware and software logs and examine activity
- Authentication: Implement procedures to verify that users are who they say they are
- Transmission Security: Implement technical security measures to ensure safety of ePHI during transmission over an electronic network

"A major goal of the Security Rule is to protect the security of individuals' ePHI while allowing regulated entities to adopt new technologies that improve the quality and efficiency of health care."

Department of Health and Human Services (HHS)

HHS's Proposed Rule to Strengthen HIPAA Cybersecurity Protections

On December 27th, 2024, HHS's Office for Civil Rights published a Notice of Proposed Rulemaking (NPRM) to modify HIPAA's Security Rule to strengthen the cybersecurity requirements. This proposed rule is up for comment and HHS will take those public comments into account before publishing the finalized rule amendment.

To summarize, the NPRM aims to add the following major requirements:

- Written documentation of all security policies, procedures, plans, and analyses
- Specific compliance time periods for existing requirements
- Data flow model that illustrates the flow of ePHI through information systems
- More detailed risk analysis, incident response plans and compliance audits
- Notification to regulators within 24 hours of any employee ePHI access changes
- Encryption of ePHI at rest and in transit

- Technical configuration controls like anti-malware protection and disabling network ports
- Multifactor authentication
- Vulnerability scanning and penetration testing
- Network segmentation
- Technical controls for data back up and disaster recovery
- Business associates and subcontractors must notify covered entities about any security incidents
- Health plan sponsors must agree to comply with the Security Rule and notify health plans of any security incidents

Keep an Eye Out: *HHS is expected to publish the final rule after the public comment period ends (3/7/2025).*

Enforcement and Compliance

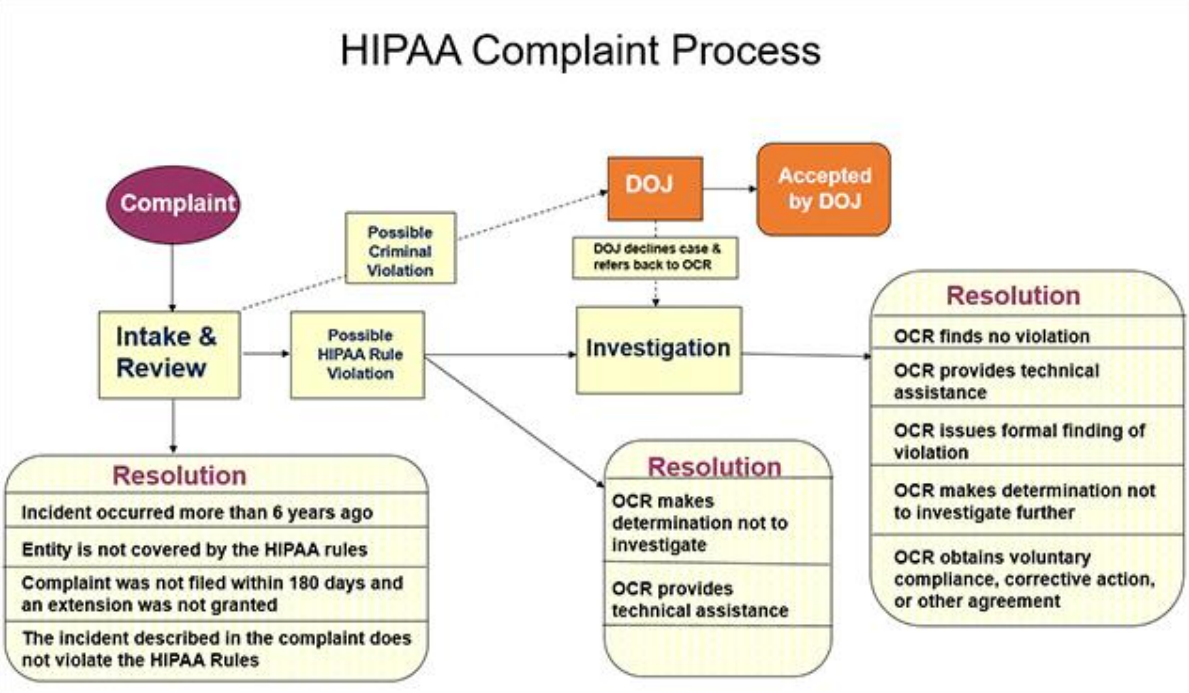
HHS's Office for Civil Rights (OCR) is in charge of enforcing HIPAA's Privacy and Security rules and penalizing covered entities who are noncompliant.

The OCR ensures compliance by investigating complaints submitted directly to them and conducting compliance audits at random.

HHS's HIPAA enforcement webpage can be found here.

OCR's HIPAA Complaint Process

The below graphic illustrates the OCR's workflow process behind investigating a HIPAA complaint:



Complaint Investigation Statistics

The following OCR data sets illustrate the complaint investigation landscape:

Complaints received per year:

Year	Complaints Received
2021	34,077
2020	27,182
2019	28,261
2018	25,912

Outcome of Complaint Investigations:

Year	Resolved After Intake and Review	Technical Assistance	Investigated: No Violation	Post-Investigational Technical Assistance	Investigated: Corrective Action Obtained	Total Resolutions
2018	16989	6912	267	289	632	25089
2019	19584	8770	444	252	803	29853
2020	19826	5091	661	80	872	26530
2021	20661	4139	817	89	714	26420

History of the Audit Program

The HITECH Act mandates that The OCR conducts periodical audits of covered entities and business associates to ensure HIPAA compliance.

In 2011-2012, the OCR conducted a pilot phase of audits where they conducted 115 investigations and took the lessons learned from that pilot to hone their auditing process.

“Phase 2” of the audit program was announced in 2016, where the OCR audited 166 covered entities and 41 business associates were investigated. The full 2016-2017 audit survey details which organization types were audited and what the results were.

After the 2016 round of audits concluded, the OCR began focusing more on complaint investigations and breach reports. In 2020, the OCR relaxed enforcement to facilitate telehealth and allow the industry to focus on fighting the COVID-19 Pandemic. In a 2024 HHS OIG report, the OCR cited lack of funding as a major obstacle in trying to fully and continuously implement the audit program.

The OCR signaled that it has restarted conducting audits in 2024, with 50 covered entities and business associates selected to be audited into 2025.

Audit Requirements

The OCR has published their Audit Protocol, which fully outlines the documentation requirements they expect audited organizations to provide upon request.

The audit criteria are listed out by audit types, which include Privacy, Security, and Breach.

Privacy - The Privacy Rule audit focuses on the organization’s policies and procedures surrounding the usage and disclosure of patient data. This includes aspects like employee training, verification requirements, patient notification, and the minimum necessary standard.

Example: Safeguards: §164.530(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

Security **-** The Security Rule audit tests the strength of the organization's security policies and procedures, both cyber and physical security. This includes regular risks analysis, mitigation plans, recovery plans, physical safeguards, employee training, and technical safeguards like encryption.

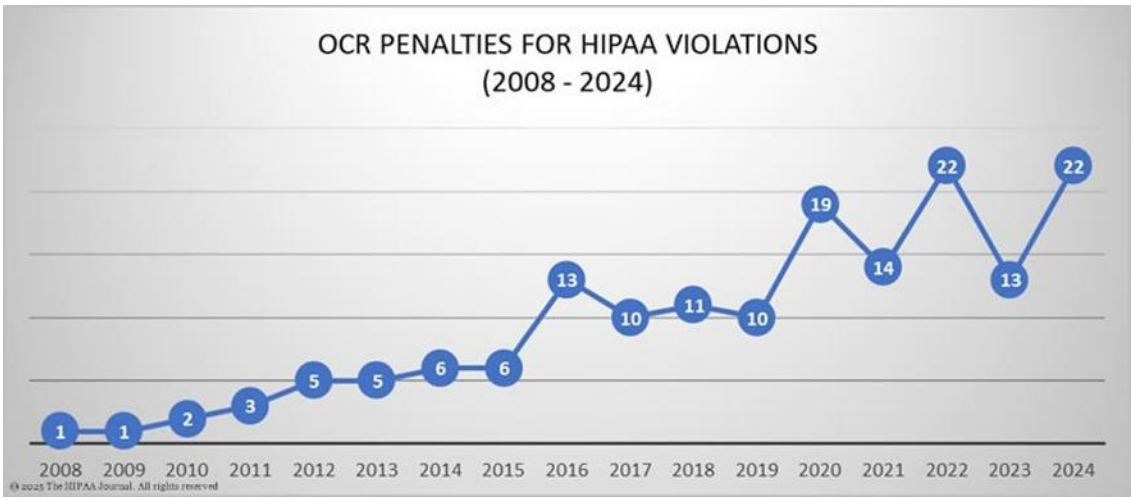
Example: Transmission Security -- Integrity Controls: §164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Breach - The Breach audit criteria tests the organization's ability to report a data breach to the OCR and other stakeholders. This includes when to notify patients, the media, business associates, and the methods of notification.

Example: Timeliness of Notification: A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

Enforcement Trends

The OCR has increased the number of monetary penalties issued over time, according to this graphic from The HIPAA Journal's 2024 Healthcare Data Breach Report.



Available Cybersecurity Frameworks

The OCR's enforcement program doesn't follow a specific security framework, but experts agree that covered entities should center their HIPAA Security Rule compliance efforts around one of their choosing. This will help ensure that all aspects of HIPAA are met and save time and effort around planning/implementation. Recommended frameworks include:

HITRUST

The HITRUST Common Security Framework (CSF) is a framework developed by the non-profit HITRUST Alliance Inc. HITRUST is a very popular framework that was developed specifically for the healthcare industry in 2007, although it is utilized across many industries today.

> *"HITRUST® provides the only assurance mechanism proven to be reliable against threats. 99.4% of HITRUST certified environments reported no breaches over the past two years. It's the only assessment and certification system that can offer validated, quantifiable assurance — proving your organization's commitment to security."*
>
> HITRUST Alliance Inc.

ISO 27001

The ISO/IEC 27001 is a popular standard for information security management systems (ISMS) co-developed by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). Originally published in 2005, the framework has been continuously improved upon, and the most recent version is from 2022.

NIST CSF

The National Institute of Standards and Technology (NIST) also has a cybersecurity framework, called The NIST Cybersecurity Framework (CSF) 2.0. The guide provides a taxonomy of cybersecurity outcomes that can be used by an organization to better understand, assess, prioritize, and communicate its cybersecurity efforts.

NIST also has published SP 800-66 Rev. 2, titled "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide", which provides guidance and resources that are specific to HIPAA compliance.

What Does This Means for the Healthcare Industry?

Build Strong Partnerships with Industry

Hire experts in AI and HIPAA compliance to guide implementation and conduct risk assessments. Bake data privacy and security language into contracts with business associates and hold them accountable. Work with like-minded business associates who value patient privacy and deeply understand/can demonstrate the flow of data in any of their AI products and information systems.

Choose a Cybersecurity Framework

Pick one that best fits your organization's needs and stick to the standards for all risk assessments and documentation practices. This consistency will help organizations be secure and will help auditors like the OCR quickly understand how your organization has addressed the requirements established through HIPAA.

Have a Robust Cybersecurity Posture

Secure data through technical safeguards like encryption and multi-factor authentication. Regularly test defenses and train employees. Establish policies and procedures for dealing with and recovering from a security incident. Stay up to data with any new cybersecurity requirements, like the newly proposed HIPAA amendments from HHS.

Be Audit Ready

Ensure all documentation is readily available in a centralized location and up-to-date. This will help any potential audits go smoothly and will reduce the chances of non-compliance.

Create an AI Strategy that Fosters Data Security and Privacy

Limit access of ePHI, including ePHI data in AI solutions, only to employees who need it for their job roles and enforce authentication of those employees. Place a human in the loop to fact-check and act as a failsafe for AI applications.

Control and Maintain Privacy of PHI

If a covered entity or business associate wants to use ePHI for training or research purposes with an AI solution/model, then they must receive expressed written consent from all the data owners (patients). If a covered entity or business associate wants to use ePHI without getting expressed consent, then they need to de-identify the data set using HHS's approved de-identification methods.

Don't forget to check for any state and local regulations that may apply to data privacy or security in healthcare on top of HIPAA.

What Does This Means for the Contractors?

Contractors who enter into business associate agreements with covered entities should:

- Deeply understand HIPAA's Privacy and Security Rules
- Deeply understand their solutions and how data flows between all their information systems
- Stay up to date on any upcoming modifications to HIPAA, like HHS's proposed security rule modification
- Get ahead of modifications by beginning to implement the security controls mentioned in the NPRM
- Conduct risk assessments and implement technical safeguards to protect against security incidents
- Communicate with partners and covered entities and bake any legal concerns into contractual language
- Know roles and responsibilities and assign ownership to employees
- Establish a data governance strategy that dictates which employees need access to ePHI and control access

Actionable Highlight: *Start looking into creating data flow illustrations and utilizing data encryption techniques in preparation of the HIPAA Security Rule update.*

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.