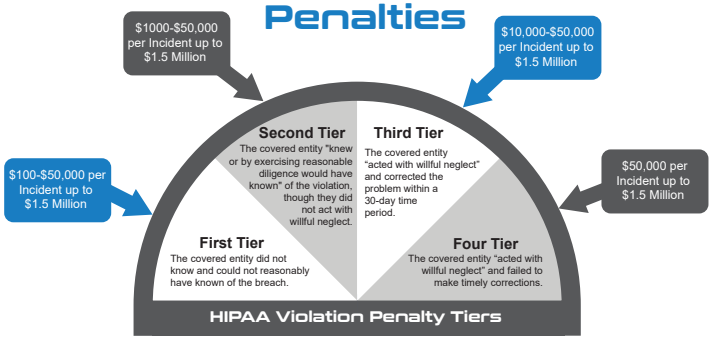
An Infographic

State of HIPAA Compliance

Penalty Tiers



HIPAA Mandate

HIPAA
Health Insurance Portability and Accountability Act of 1996

- Title I — Insurance Portability
- Title II — Fraud and Abuse Medical Liability Reform; **Administrative Simplification**
  - Privacy
  - Security
  - EDI
    - Transactions
    - Code Sets
  - Identifiers
- Title III — Tax Related Health Provision
- Title IV — Group Health Plan Requirements
- Title V — Revenue Off-sets

Signature Methodology

ecfirst Delivers Everything HIPAA

OCR Guidance

Between the **rising pace of breaches** of unsecured PHI and **continued cyber security threats** impacting the health care industry, it is critical that organizations take their HIPAA compliance responsibilities seriously. OCR will pursue civil money penalties for violations that are not addressed.

OCR Director **Lisa J. Pino**

HIPAA Enforcement

The ecfirst HITRUST Ecosystem

Achieve HITRUST Certification

The ecfirst HIPAA Ecosystem

HIPAA Academy · CHP Certified HIPAA Professional, HIPAA Academy · CSCS Certified Security Compliance Specialist · CCSA Certified Cyber Security Architect

Global Cyber Defense Thought Leader

An Infographic

State of HIPAA Compliance

Patient Rights

- The right to ask, see, and copy his/her own medical record.
- A right to amend their records.
- Gets a notice of privacy practices.
- Controls how their PHI is used for certain purposes.
- Receives their information in a confidential manner.
- May file a complaint if they feel their rights have been violated.
- May opt-out of fundraising activities.

Protected Health Information (PHI)

- PHI, which consists of items within a medical record which could be used to link it to an individual patient.
- PHI is protected from being revealed in all forms in which it may occur: paper, electronic, or oral; and whether it is "at rest" or "in transit".

PHI Identifiers

#	Identifiers	#	Identifiers
1	Name	10	Account number
2	Address	11	Certificate/license number
3	Dates related to an individual	12	Any vehicle or other device serial
4	Telephone numbers	13	Device identifiers or serial numbers
5	Fax number	14	Web URL
6	Email address	15	Internet Protocol (IP) address
7	Social Security number	16	Finger or voice prints
8	Medical record number	17	Photographic images
9	Health plan beneficiary number	18	Any other characteristic that would uniquely identify the individual

OCR Audit Protocol

- The OCR HIPAA Audit program analyzes processes, controls, and policies of selected Covered Entities pursuant to the HITECH Act audit mandate.
- Established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits.
- OCR Audit Protocol covers Privacy Rule requirements for the following:
  - Notice of Privacy Practices for PHI
  - Rights to request privacy protection for PHI
  - Access of individuals to PHI
  - Administrative requirements
  - Uses and disclosures of PHI
  - Amendment of PHI
  - Accounting of Disclosures

OCR Guidance

HIPAA impacted organizations are vulnerable to cyber attacks if they fail to understand where ePHI is stored in their information systems.

OCR Director **Lisa J. Pino**

Covered Entity

- Health plans, healthcare clearinghouses, and healthcare providers who must comply with HIPAA regulations and standards because they transmit health information in electronic form in connection with HIPAA covered transactions.
- The law specifies which persons or organizations have a statutory obligation to abide by the law, and labels them as "Covered Entities".
  - Health Plan: Provides or pays the cost of medical care
  - Healthcare Clearinghouse: Processes healthcare transactions for providers and insurers
  - Healthcare Provider: Person or entity who is trained and licensed to give, bill, and be paid for healthcare services.via electronic transmission

Business Associates

- A person or organization that performs a function or activity on behalf of a Covered Entity, but is not part of the Covered Entity's workforce. This individual or company needs to have access to PHI in order to perform a function for the Covered Entity.
- Who Might Be a Business Associate?

The ecfirst HITRUST Ecosystem

e1 ESSENTIALS 1-YEAR HITRUST CERTIFIED
i1 IMPLEMENTED 1-YEAR HITRUST CERTIFIED
HITRUST Authorized External Assessor
r2 RISK-BASED 2-YEAR HITRUST CERTIFIED

Achieve HITRUST Certification

The ecfirst HIPAA Ecosystem

HIPAA Academy
CHP Certified HIPAA Professional HIPAA Academy
CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST
CCSA Certified Cyber Security Architect

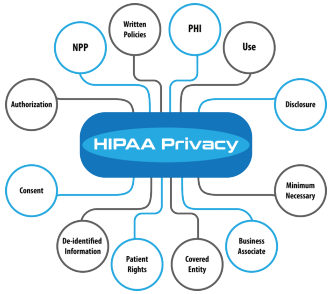
Global Cyber Defense Thought Leader

An Infographic

State of HIPAA Compliance

HIPAA Privacy

- The Privacy Rule protects most Individually Identifiable Health Information (IIHI) held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information PHI.
- The Privacy Rule establishes national standards for the protection of certain health information.
- The Privacy Rule standards address the use and disclosure of PHI as well as standards for individuals' privacy rights.



Using and Disclosing PHI

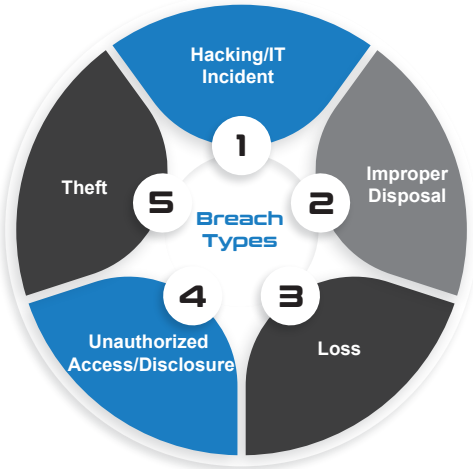
Use	Disclosure
Sharing	Release
Employing	Transfer
Applying	Provision of access to
Utilizing	Divulging in any manner
Examining	Information disclosed when transmitted outside organizations
Analyzing	
Information used when moved inside organization	

HITECH Breach Notification

- The Breach Notification Rule requires HIPAA CEs to notify individuals and the Secretary of HHS of the loss, theft, or certain other impermissible uses or disclosures of unsecured PHI.
- If a breach affects fewer than 500 individuals, the CE must notify the Secretary and affected individuals. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

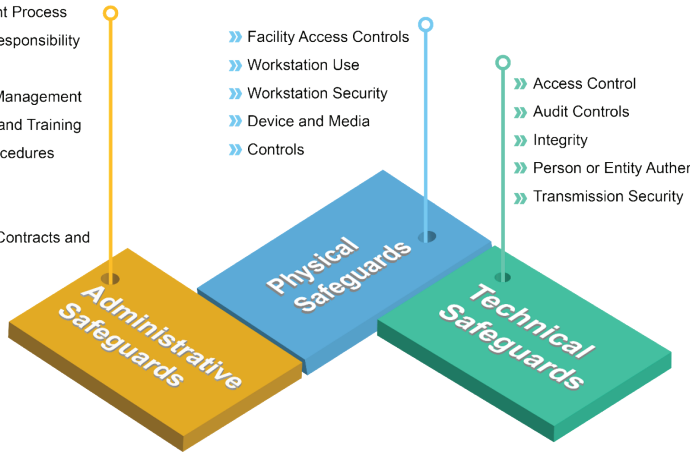
Breach Analysis

The acquisition, access, use, or disclosure of PHI in a manner not permitted by the privacy rule which compromises the security or privacy of the PHI.



HIPAA Security

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements



Notice of Privacy Practices (NPP)

- The Notice of Privacy Practices and individual authorizations are the documents that a healthcare provider maintains to describe its uses and disclosures of PHI, and list the patient rights.
- A form to be given to patients or customers by a Covered Entity which clearly states how the organization addresses HIPAA regulations.

HIPAA Final Rule

Makes Business Associates and their subcontractors of Covered Entities directly liable for compliance with certain requirements of the HIPAA Privacy and Security Rules.

Minimum Necessary

- The Minimum Necessary Standard inherently encourages the use of electronic medical records technologies. If you use enterprise-wide technology to collect data, the resulting information can be quantified and mathematically scrutinized to get an unbiased report of your use of PHI.

Risk Analysis

- Risk Analysis is required by HIPAA
  - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity.

The ecfirst HITRUST Ecosystem

e1 ESSENTIALS 1-YEAR HITRUST CERTIFIED | i1 IMPLEMENTED 1-YEAR HITRUST CERTIFIED | HITRUST® Authorized External Assessor | r2 RISK-BASED 2-YEAR HITRUST CERTIFIED

Achieve HITRUST Certification

The ecfirst HIPAA Ecosystem

HIPAA Academy | CHP Certified HIPAA Professional HIPAA Academy | CSCS CERTIFIED SECURITY COMPLIANCE SPECIALIST | CCSA Certified Cyber Security Architect

Global Cyber Defense Thought Leader