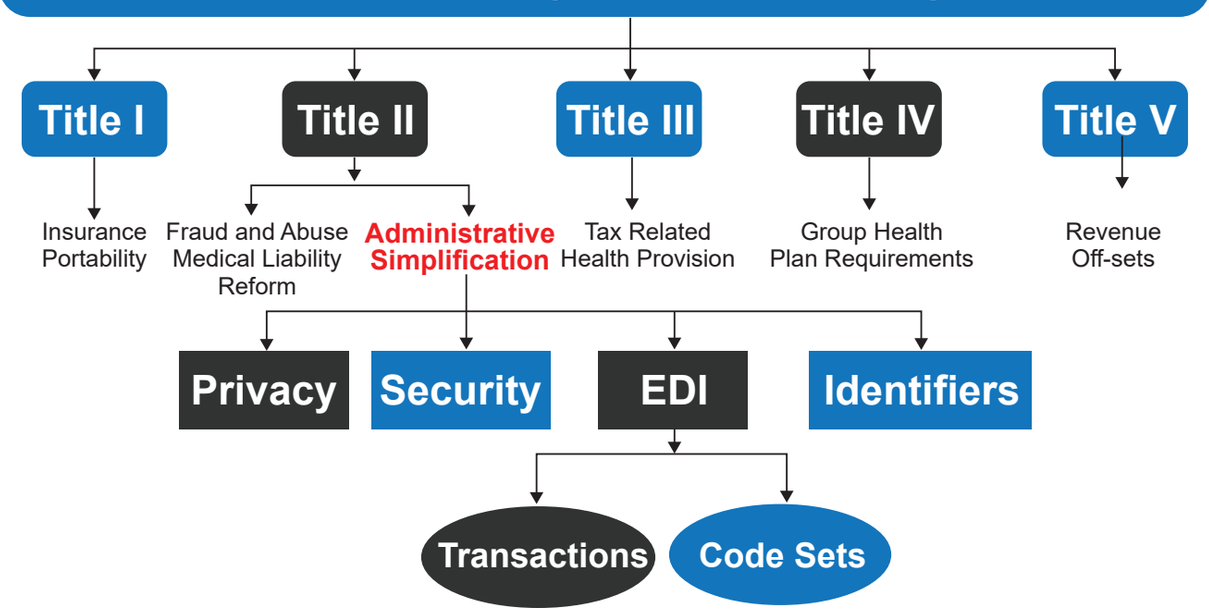
Credible & Evidence-based HIPAA Compliance Program

HIPAA Fundamentals

An Infographic

HIPAA Mandate

HIPAA
Health Insurance Portability and Accountability Act of 1996



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

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.

ecfirst | HIPAA™ Academy

Re⍟magining Cyber Defense

Global Cybersecurity & Compliance Expert

Credible & Evidence-based HIPAA Compliance Program

HIPAA Fundamentals

An Infographic

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?
  - Attorney
  - Accountant
  - Consultant
  - Cleaning Service
  - Data Aggregator
  - Vendor
  - Cloud Services

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

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

Whom Does HIPAA Impact?

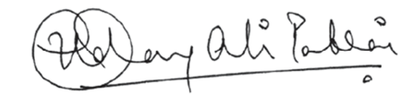
- Payers
- Providers
- Clearinghouses
- Business Associates and their Subcontractors (Final Rule update)

Office for Civil Rights (OCR)

- Administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules.
- Conducts HIPAA complaint investigations, compliance reviews, and audits.

ecfirst | HIPAA™ Academy

Re(i)magining Cyber Defense



Global Cybersecurity & Compliance Expert

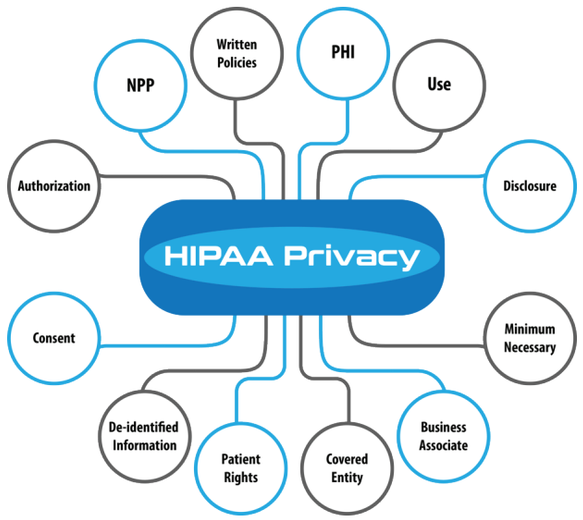
Credible & Evidence-based HIPAA Compliance Program

HIPAA Privacy Rule

An Infographic

Privacy Rule

- 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.



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.
- Final Rule: Requires that when Business Associates use, disclose, or request PHI from another Covered Entity, they limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

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.

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	

TPO

PHI can be used for a Covered Entities' own Treatment (T), Payment (P), and Healthcare Operations (O) (the day to day actions important to the organization's functioning). Examples of healthcare operations which might need PHI are for training medical and administrative staff, quality control, preparing accreditation applications, or even limited marketing.

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.

Credible & Evidence-based HIPAA Compliance Program

HIPAA Privacy Rule

An Infographic

Uses and disclosures of Protected Health Information: General rules §164.502

- **Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes STD** §164.502(a)(5)(i)
- **Deceased individuals STD** §164.502(f)
- **Personal representatives STD** §164.502(g)
- **Confidential communications STD** §164.502(h)
- **Uses and disclosures consistent with notice STD** §164.502(i)
- **Disclosures by whistleblowers STD** §164.502(j)(1)
- **Disclosures by workforce members who are victims of a crime STD** §164.502(j)(2)

Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object §164.510

- **Use and Disclosure for Facility Directories; Opportunity to Object STD** §164.510(a)(1) and §164.510(a)(2)
- **Uses and Disclosures for Facility Directories in Emergency Circumstances STD** §164.510(a)(3)
- **Permitted uses and disclosures STD** §164.510(b)(1)
- **Uses and disclosures with the individual present STD** §164.510(b)(2)
- **Limited uses and disclosures when the individual is not present STD** §164.510(b)(3)
- **Uses and disclosures for disaster relief purposes STD** §164.510(b)(4)
- **Uses and disclosures when the individual is deceased STD** §164.510(b)(5)

Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required §164.512

- **Uses and disclosures required by law STD** §164.512(a)
- **Uses and disclosures for public health activities STD** §164.512(b)
- **Uses and disclosures for health oversight activities STD** §164.512(d)
- **Disclosures for judicial and administrative proceedings STD** §164.512(e)
- **Disclosures for law enforcement purposes STD** §164.512(f)(1)
- **Disclosures for law enforcement purposes - for identification and location STD** §164.512(f)(2)
- **Disclosures for law enforcement purposes-- PHI of a possible victim of a crime STD** §164.512(f)(3)
- **Disclosures for law enforcement purposes-- an individual who has died as a result of suspected criminal conduct STD** §164.512(f)(4)
- **Disclosures for law enforcement purposes: crime on premises STD** §164.512(f)(5)
- **Disclosures for law enforcement purposes STD** §164.512(f)(6)
- **Uses and disclosures about decedents STD** §164.512(g)
- **Uses and disclosures for cadaveric organ, eye or tissue donation STD** §164.512(h)
- **Uses and disclosures for research purposes -- Permitted Uses and Disclosures STD** §164.512(i)(1)
- **Uses and disclosures for research purposes -- Documentation of Waiver Approval STD** §164.512(i)(2)
- **Uses and disclosures for specialized government functions -- Military STD** §164.512(k)(1)
- **Uses and disclosures for specialized government functions -- National Security and intelligence activities STD** §164.512(k)(2)
- **Uses and disclosures for specialized government functions -- Medical Suitability Determinations STD** §164.512(k)(4)
- **Uses and disclosures for specialized government functions – Correctional institutions STD** §164.512(k)(5)
- **Uses and disclosures for specialized government functions – Providing public benefits STD** §164.512(k)(6)
- **Disclosures for workers' compensation STD** §164.512(l)

Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations §164.506

- **Permitted uses and disclosures** §164.506(a) STD
- **Consent for uses and disclosures** §164.506(b); (b)(1) and (b)(2) STD

Uses and disclosures: Organizational Requirements §164.504

- **Business associate contracts STD** §164.504(e)
- **Requirements for group health plans STD** §164.504(f)
- **Requirements for a covered entity with multiple covered functions STD** §164.504(g)

Other Requirements Relating to Uses and Disclosures of Protected Health Information §164.514

- **Minimum Necessary STD** §164.514(d)(1)
- **Limited Data Sets STD** §164.514(e)
- **Uses and Disclosures for Fundraising STD** §164.514(f)
- **Uses and Disclosures for Underwriting and Related Purposes STD** §164.514(g)
- **Verification Requirements STD** §164.514(h)

Notice of Privacy Practices for Protected Health Information §164.520

- **Notice of Privacy Practices Content requirements STD** §164.520(a)(1)
- **Right of an Individual to Request Restriction of Uses and Disclosures STD** §164.522(a)(1)
- **Confidential Communications Requirements STD** §164.522 (b)(1)

Access of Individual to Protected Health Information §164.524

- **Right to access STD** §164.524(a)(1)
- **Unreviewable grounds for denial STD** §164.524(a)(2)
- **Reviewable grounds for denial STD** §164.524(a)(3)
- **Review of denial of access STD** §164.524(a)(4)

Uses and Disclosures for which an Authorization is Required §164.508

- **Authorizations for uses and disclosures is required STD** §164.508(a)(1-**3)**

Amendment of Protected Health Information §164.526

- **Right to amend STD** §164.526(a)(1)
- **Denying the Amendment STD** §164.526(a)(2)

Accounting of Disclosures of Protected Health Information §164.528

- **Right to an Accounting of Disclosures of PHI STD** §164.528(a)

Administrative Requirements §164.530

- **Personnel designations STD** §164.530(a)
- **Training STD** §164.530(b)
- **Safeguards STD** §164.530(c)
- **Complaints to the Covered Entity STD** §164.530(d)(1)
- **Sanctions STD** §164.530(e)(1)
- **Mitigation STD** §164.530(f)
- **Refraining from Intimidating or Retaliatory Acts STD** §164.530(g)
- **Waiver of rights STD** §164.530(h)
- **Policies and Procedures STD** §164.530(i)
- **Documentation STD** §164.530(j)

ecfirst | HIPAA™ Academy

Re(imagining Cyber Defense

Global Cybersecurity & Compliance Expert

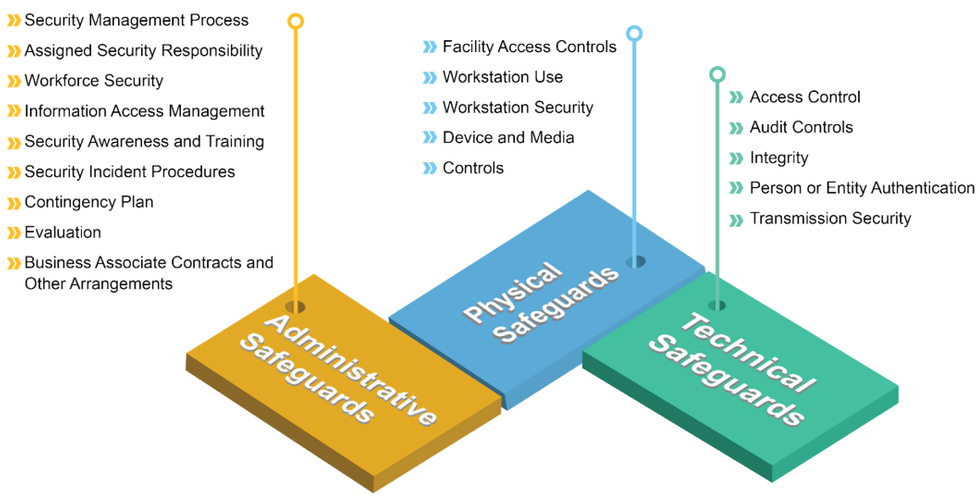
Credible & Evidence-based HIPAA Compliance Program

HIPAA Security Rule

An Infographic

The HIPAA Security Rule

- Establishes a national set of minimum security standards for protecting all ePHI that a CE and BA create, receive, maintain, or transmit. The Security Rule contains the administrative, physical, technical safeguards, organizational standards, and policies and procedures that CEs and BAs must put in place to secure ePHI.
- The Security Rule specifies a series of Implementation Specifications, i.e., detailed instructions for supporting a particular Standard.
- Implementation Specifications
  - Required: A Covered Entity or Business Associate must comply with a required Implementation Specification.
  - Addressable: For addressable Implementation Specifications, Covered Entities must perform an assessment to determine whether the specification is a reasonable and appropriate safeguard in their environment.



Confidentiality, Integrity, and Availability (CIA)

Confidentiality

- ePHI data should not be made available or disclosed to unauthorized persons.
- Allow disclosure privileges only to users who have training and authority to make decisions.
- Install reliable authentication methods to identify system users and access control mechanisms to automatically control each employee's use of medical data.

Integrity

- Integrity refers to the trustworthiness of information resources.
- Data or information has not been altered or destroyed in an unauthorized act.
- Security backups allow reconstruction of data after a security threat or natural disaster.
- Data Integrity – Data has not been changed inappropriately, whether by accident or deliberate, malicious intent.
- Source integrity – Did the data come from the person or business you think it did, or did it come from an imposter?

Availability

- Make PHI accessible to an authorized person when wanted and needed.
- Adding policies and procedures that allow proper personnel to see and use PHI.
- Guard against threats to the systems.
- Have appropriate backups and business continuity plans for operation in the event of an emergency.

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.

ecfirst | HIPAA™ Academy

Re⊙magining Cyber Defense

Global Cybersecurity & Compliance Expert

Credible & Evidence-based HIPAA Compliance Program

HIPAA Security Rule

An Infographic

Administrative Safeguards

Security Management Process STD
§164.308(a)(1)(i)

- *Risk Analysis (R) SPEC §164.308(a)(1)(ii)(A)*
- *Risk Management (R) SPEC §164.308(a)(1)(ii)(B)*
- *Sanction Policy (R) SPEC §164.308(a)(1)(ii)(C*
- *Information System Activity Review (R) SPEC §164.308(a)(1)(ii)(D)*

Assigned Security Responsibility STD
§164.308(a)(2)

Workforce Security STD
§164.308(a)(3)(i)

- *Authorization and/or Supervision (A) SPEC §164.308(a)(3)(ii)(A)*
- *Workforce Clearance Procedure (A) SPEC §164.308(a)(3)(ii)(B)*
- *Termination Procedures (A) SPEC §164.308(a)(3)(ii)(C)*

Information Access Management STD
§164.308(a)(4)(i)

- *Isolating Health Care Clearinghouse Function (R) SPEC §164.308(a)(4)(ii)(A)*
- *Access Authorization (A) SPEC §164.308(a)(4)(ii)(B)*
- *Access Establishment and Modification (A) SPEC §164.308(a)(4)(ii)(C)*

Security Awareness and Training STD
§164.308(a)(5)(i)

- *Security Reminders (A) SPEC §164.308(a)(5)(ii)(A)*
- *Protection from Malicious Software (A) SPEC §164.308(a)(5)(ii)(B)*
- *Log-in Monitoring (A) SPEC §164.308(a)(5)(ii)(C)*
- *Password Management (A) SPEC §164.308(a)(5)(ii)(D)*

Security Incident Procedures STD
§164.308(a)(6)(i)

- *Response and Reporting (R) SPEC §164.308(a)(6)(ii)*

Contingency Plan STD
§164.308(a)(7)(i)

- *Data Backup Plan (R) SPEC §164.308(a)(7)(ii)(A)*
- *Disaster Recovery Plan (R) SPEC §164.308(a)(7)(ii)(B)*
- *Emergency Mode Operation Plan (R) SPEC §164.308(a)(7)(ii)(C)*
- *Testing and Revision Procedure (A) SPEC §164.308(a)(7)(ii)(D)*
- *Applications and Data Criticality Analysis (A) SPEC §164.308(a)(7)(ii)(E)*

Evaluation STD
§164.308(a)(8)

Business Associate Contracts and Other Arrangements STD
§164.308(b)(1)

- *Written Contract or Other Arrangement (R) §164.308(b)(3) SPEC*

Physical Safeguards

Facility Access Controls STD
§164.310(a)(1)

- *Contingency Operations (A) SPEC §164.310(a)(2)(i)*
- *Facility Security Plan (A) SPEC §164.310(a)(2)(ii)*
- *Access Control and Validation Procedures (A) SPEC §164.310(a)(2)(iii)*
- *Maintenance Records (A) SPEC §164.310(a)(2)(iv)*

Workstation Use STD
§164.310(b)

Workstation Security STD
§164.310(c)

Device and Media Controls STD
§164.310(d)(1)

- *Disposal (R) SPEC §164.310(d)(2)(i)*
- *Media Reuse (R) SPEC §164.310(d)(2)(ii)*
- *Accountability (A) SPEC §164.310(d)(2)(iii)*
- *Data Backup and Storage (A) SPEC §164.310(d)(2)(iv)*

Technical Safeguards

Access Control STD
§164.312(a)(1)

- *Unique User Identification (R) SPEC §164.312(a)(2)(i)*
- *Emergency Access Procedure (R) SPEC §164.312(a)(2)(ii)*
- *Automatic Logoff (A) SPEC §164.312(a)(2)(iii)*
- *Encryption and Decryption (A) SPEC §164.312(a)(2)(iv)*

Audit Controls STD
§164.312(b)

Integrity STD
§164.312(c)(1)

- *Mechanism to Authenticate ePHI (A) SPEC §164.312(c)(2)*

Person or Entity Authentication STD
§164.312(d)

Transmission Security STD
§164.312(e)(1)

- *Integrity Controls (A) SPEC §164.312(e)(2)(i)*
- *Encryption (A) SPEC §164.312(e)(2)(ii)*

Organizational Requirements

Business Associate Contracts or Other Arrangements STD
§164.314(a)(1)

- *Business Associate Contracts or Other Arrangements (R) SPEC §164.314(a)(2)(i)(A)*
- *Business Associate Contracts or Other Arrangements (R) SPEC §164.314(a)(2)(i)(B)*
- *Business Associate Contracts or Other Arrangements (R) SPEC §164.314(a)(2)(i)(C)*
- *Other Arrangements (R) SPEC §164.314(a)(2)(ii)*
- *Business Associate Contracts with Subcontractors (R) SPEC §164.314(a)(2)(iii*

Requirements for Group Health Plans STD
§164.314(b)(1)

Implement Safeguards (R) STD
§164.314(b)(2)(i)

- *Ensure Adequate Separation (R) SPEC §164.314(b)(2)(ii)*
- *Ensure Agents Safeguard (R) SPEC §164.314(b)(2)(iii)*
- *Report Security Incidents (R) SPEC §164.314(b)(2)(iv)*

Policies and Procedures and Documentation Requirements

Policies and Procedures STD
§164.316 (a)

Documentation STD
§164.316 (b)(1)

- *Time Limit (R) SPEC §164.316 (b)(2)(i)*
- *Availability (R) SPEC §164.316 (b)(2)(ii)*
- *Updates (R) SPEC §164.316 (b)(2)(iii)*

ecfirst | HIPAA™ Academy

Re imagining Cyber Defense

Global Cybersecurity & Compliance Expert

Credible & Evidence-based HIPAA Compliance Program

HITECH Breach Notification

An Infographic

Secured and Unsecured PHI

Secured PHI

An unauthorized person cannot use, read, or decipher any PHI that he/she obtains because your practice:

- Encrypts the information.
- Clears, purges, or destroys media (e.g., data storagedevices, film, laptops) that stored or recorded PHI.
- Shreds or otherwise destroys paper PHI.

(These operations must meet applicable federal standards.)

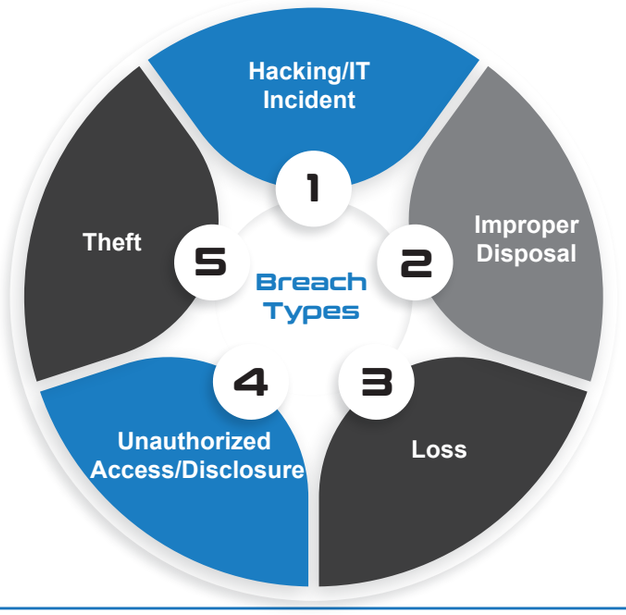
Unsecured PHI

An unauthorized person may use, read, and decipher PHI that he/she obtains because your practice:

- Does not encrypt or destroy the PHI; or
- Encrypts PHI, but the decryption key has also been breached.

Breaches

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.



The Breach Notification Rule

- 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 Notification Rule

Administrative Requirements STD §164.414(a)
Training STD §164.530(b)
Complaints STD §164.530(d)
Sanctions STD §164.539(e)
Refraining from Retaliatory Acts STD §164.530(g)
Waiver of Rights STD §164.530(h)
Policies and Procedures STD §164.530(i)
Documentation STD §164.530(j)
Definitions: Breach - Risk Assessment STD §164.402
Definitions: Breach Exceptions - Unsecured PHI STD §164.402
Notification to Individuals STD §164.404(a)
Timeliness of Notification SPEC §164.404(B)
Content of Notification SPEC §164.404(C)
Methods of Individual Notification SPEC §164.404(D)

Notification to the Media STD *§164.406(a)*
Timeliness of Notification SPEC §164.406(B)
Content of Notification SPEC §164.406(C)
Notification to the Secretary STD §164.408(a)
Breaches Involving 500 or more Individuals SPEC §164.408(B)
Breaches Involving less than 500 Individuals SPEC §164.408(C)
Notification by a Business Associate §164.410(a)
Timeliness of Notification by a Business Associate SPEC §164.410(B)
Content of Notification by a Business Associate SPEC §164.410(C)
Law Enforcement Delay STD §164.412
Administrative Requirements & Burden of Proof STD §164.414

ecfirst | HIPAA™ Academy

Re(i)magining Cyber Defense

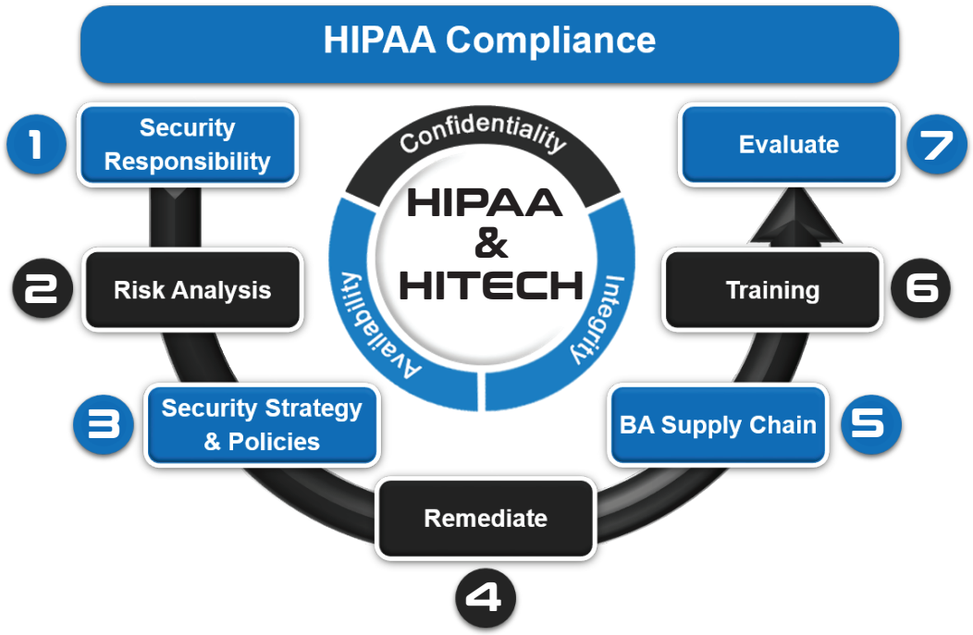
Global Cybersecurity & Compliance Expert

Credible & Evidence-based HIPAA Compliance Program

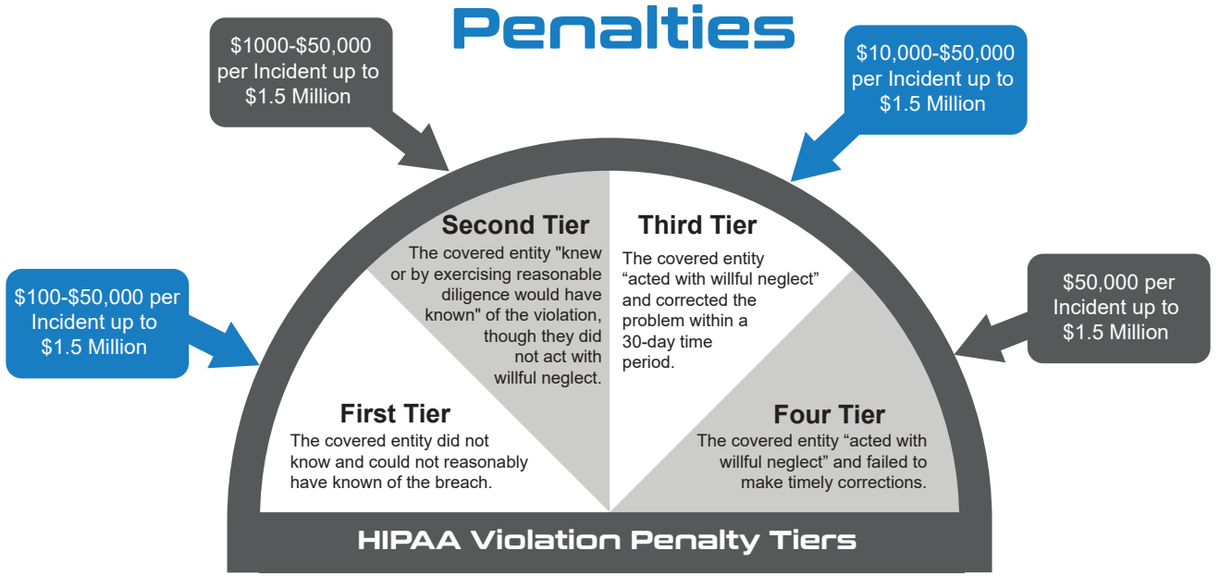
HIPAA Enforcement & Penalty

An Infographic

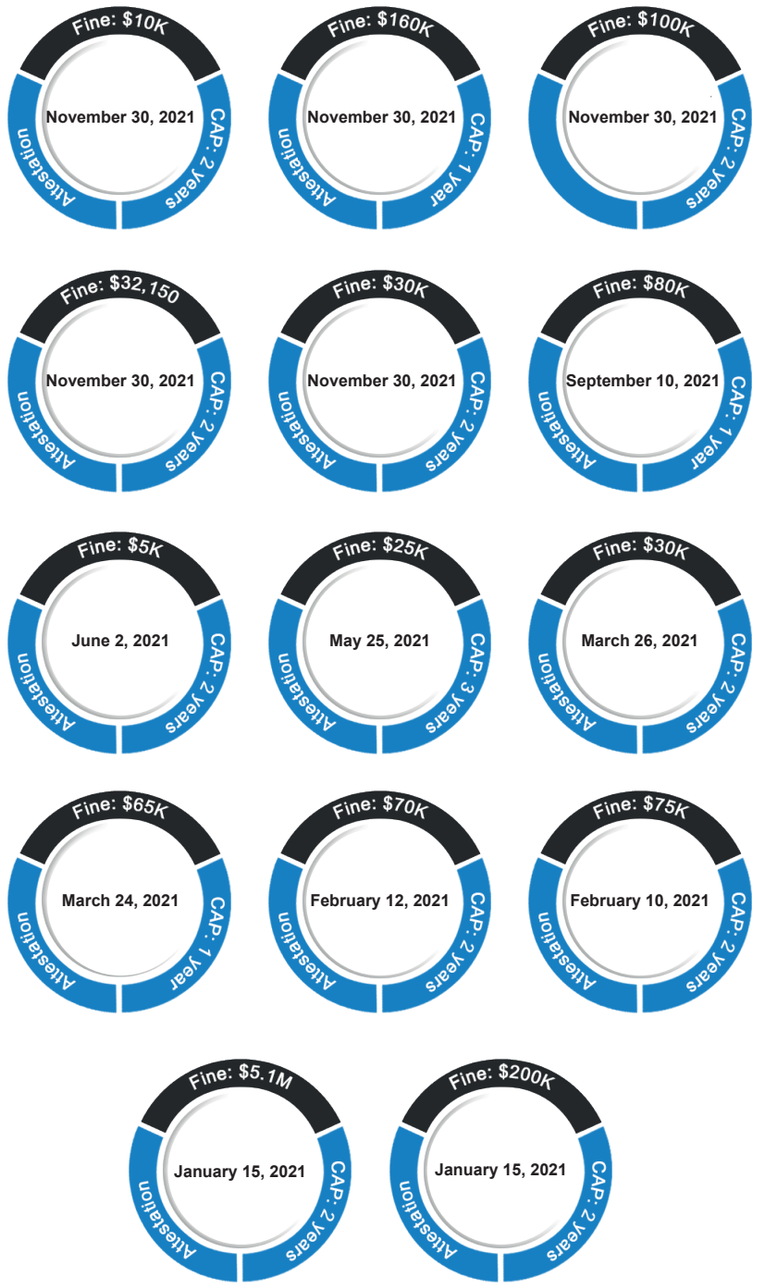
HIPAA Methodology



Penalty Tiers



2021 Compliance Enforcement



ecfirst | HIPAA™ Academy

Re⚲magining Cyber Defense

Global Cybersecurity & Compliance Expert