HIPAA

QUICK REFERENCE CARD

www.ecfirst.com

HIPAA

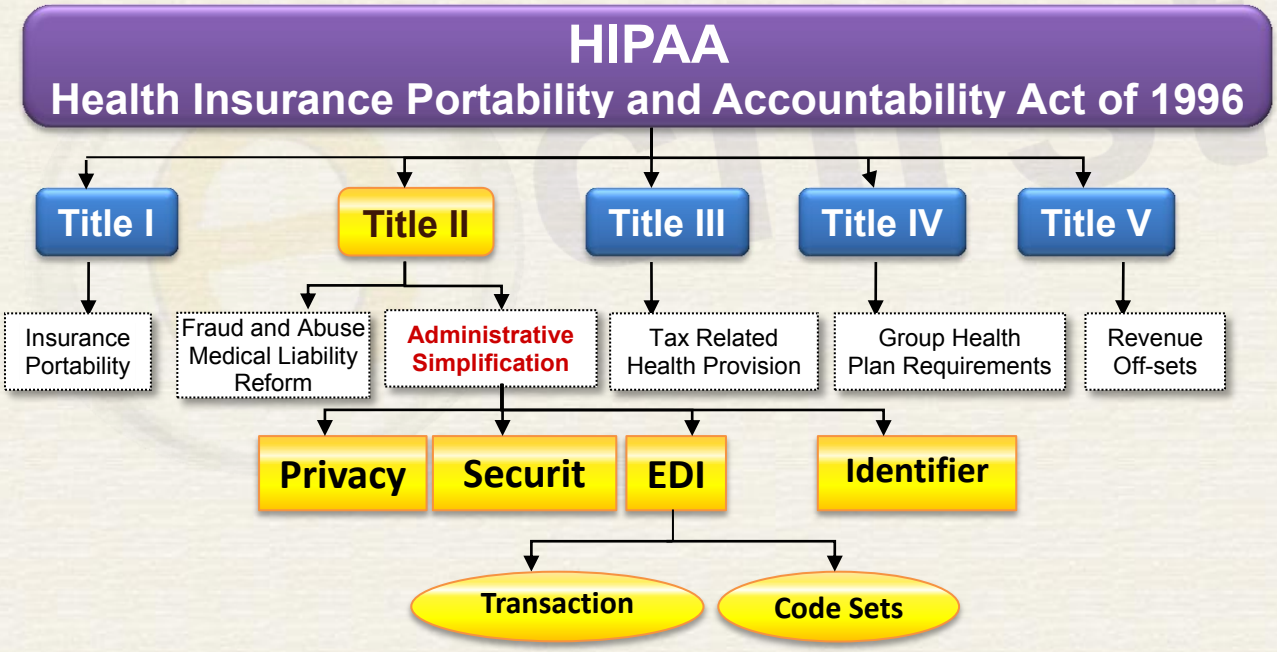
Health Insurance Portability & Accountability Act

Quick Reference Card from ecfirst

INTRODUCTION

HIPAA is an acronym used as a "short title" for the bill, Public Law 104 -191. The full version is Health Insurance Portability and Accountability Act of 1996. You may also hear it referred to as the Kennedy-Kassebaum bill. The purpose of HIPAA includes:

1. To improve portability and continuity of health insurance coverage in the group and individual markets,
2. To combat waste, fraud, and abuse in health insurance and healthcare delivery,
3. To promote the use of medical savings accounts,
4. To improve access to long-term care services and coverage,
5. To simplify the administration of health insurance.



HIPAA includes five Titles. These are:

- Title I- Healthcare access, portability, and renew ability
- Title II - Preventing healthcare fraud and abuse, ADMINISTRATIVE SIMPLIFICATION, Medical liability reform
- Title III - Tax-Related Health Provisions
- Title IV - Application and Enforcement of Group Health Plan Requirements
- Title V - Revenue Offsets

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 has Increases fines, Includes Business Associates for fines and penalties and requires Breach Notification to patients and HHS.

	Date Law/Rule Passed	Compliance Date	Impact
HIPAA	August 21, 1996		
Privacy Rule	April 14, 2001	April 14, 2003	Covered Entities
Revised Privacy Rule	Revised August 14, 2002	April 14, 2003	Covered Entities
		April 14, 2004	Small Health Plans
Business Contracts		April 14, 2004	Covered Entities AND Small Health Plans
Security Rule	February 20, 2003	April 20, 2005	Covered Entities
		April 20, 2006	Small Health Plans
IDENTIFIER			
National Employer ID - Employer Identification Number (EIN)		July 30, 2004	All Employers providing Employee Coverage
National Provider ID	May 23, 2005	May 23, 2007	All Healthcare Providers
		May 23, 2007	Small Health Plans
National Health Plan Identifier	Payer November 5, 2014; Small Health Plans November 5, 2015; Covered Entities November 7, 2016.		All Health Plans, other payers and Covered Entities
National Health Identifier for Individuals	Suspended as of this publication		
HITECH Act	February 17, 2009	February 23, 2010	All Covered Entities and Business Associates
Final Rule	January 17, 2013	Date March 26, 2013	effective date 180 days 9/23/13

HIPAA Terminology

Code Sets
Standardized numeric or alphanumeric descriptions of things like provider location, diagnosis, procedure, medical concepts or terms, or types of transactions being sent between healthcare entities electronically HIPAA codes must be utilized by covered entities.

Data Element
Each detail of a visit to a provider such as patient name, address, date of service, location, and other information captured for record keeping and future evaluation, treatment, billing, and reporting purposes.

Dental Codes (CDT)
Standards set by the American Dental Association to identify procedures done by dentists in their offices published as the Code on Dental Procedures and Nomenclature.

Diagnostic and Procedure Codes (ICD-9-CM) - this code is going to ICD-10; delayed to October 2015.
A code group which can be assigned to diagnosis and procedures. The list is called the International Classification of Diseases, Ninth Revision, Clinical Modification, and is created and maintained by National Center for Health Statistics (NCHS) and the Centers for Medicare and Medicaid Services (CMS).

National Employer Identifier (EIN)
An employer identification number originally created by the IRS for tax purposes and subsequently adopted as the national standard to designate companies providing employee healthcare coverage for HIPAA purposes.

Electronic Data Interchange (EDI)
The generic standards for exchanging business data electronically on which the rules and guidelines for HIPAA Transactions are based. EDI is more universal in scope that just providing guidance for the healthcare industry.

Healthcare Financing Administration Procedure Coding System (HCPCS)
The Healthcare Financing Administration has undergone a name change and is now known as the Centers for Medicare & Medicaid Services (CMS). CMS and HHS update and distribute this code set to be used for things not identified in other approved lists.

National Drug Code (NDC)
These codes are created and maintained by the Food and Drug Administration (FDA) and allow standardized identification of drugs.

National Health Identifier for Individuals (NHI)
Still has not been implemented due to privacy concerns.

National Health Plan Identifier (HPID)
A proposed unique identifier for health plans and other payers of healthcare claims not formally proposed or defined at this time.

National Council for Prescription Drug Programs (NCPDP)
Used for retail pharmacy transactions. Retail pharmacies are the only healthcare entities which use a different set of transmission standards (not codes). The two NCPDP formats which health plans must accept, are Telecommunications Standard Format Version 5.1 and Batch Standard Version 1.0.

National Plan and Provider Enumeration System (NPPES)
A plan within the HIPAA legislation to allow a third party contractor or contractors to create, verify, and assign NPI numbers, and to maintain the National Provider System and the National Provider File database.

National Provider Identifier (NPI)
The unique identifier for healthcare providers used for HIPAA compliance.

Patient Event
A patient visit; the collective service or services included in this particular, unique interaction between this patient and this provider.

Place of Service Code (POS)
A code, maintained by the Centers for Medicare & Medicaid Services (CMS) which shows the payer the location type in which the patient service was rendered. A two digit series of numbers represents the place category.

Physician's Office Codes (CPT)
Services performed in physician's offices are coded from a list called Current Procedural Terminology created by the American Medical Association.

Segment
The renaming of the collective codes and data elements (data content) when repackaged within a transaction bundle or envelope.

Transactions
These are the actual exchanges of electronic data between two healthcare parties.

Transactions and Code Sets
Also called the Standard for Electronic Transactions. These are the rules and guidelines which show the healthcare industry how to exchange electronic data. Compliance is mandatory for all health plans, health clearinghouses, and health providers who receive or submit any health information electronically.

Who Is Impacted by HIPAA?

Health Plans
Individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare + Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans.

Healthcare Providers
Every healthcare provider, regardless of size, who electronically transmits health information in connection with certain transactions.

Healthcare providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for healthcare.

Healthcare Clearinghouses

Healthcare clearinghouses are entities that process non-standard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.

Business Associates & their Subcontractors

Business Associate Defined

In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. The final rule specifically includes the subcontractors of business associates must also comply including having Business Associate Contracts in place.

Business associate services to a covered entity included but are not limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

The final rule also includes Health Information Organization (HIO), Patient Safety Organizations (PSOs) e Prescription Gateways and other persons that provide data transmission services with respect to PHI as a business associate.

BAC is also referred to as a Business Associate Agreement BAA and government uses the term Memorandum of Understanding MOU they are all the same.

HITECH ACT - Top Issues

Business Associate Contract

When a covered entity uses a contractor or other non-workforce member to perform "business associate" services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections). In the business associate contract, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associate. This changed with HITECH.

- Breach Notification
- Increased Penalties
- Business Associates same as CEs

HIPAA Transactions

The HIPAA Administrative Simplification Standard for Electronic Transactions, also referred to as the Transaction and Code Sets, facilitates standardized information exchange between providers and payers. The Transactions Rule applies to all administrative and financial transactions covered by HIPAA.

As required by HIPAA, the Secretary of HHS has adopted standards for the following administrative and financial healthcare transactions:

270. Eligibility, Coverage, or Benefit Inquiry
271. Eligibility, Coverage, or Benefit Information
276. Healthcare Claim Status Request
277. Healthcare Claim Status Notification

278. Healthcare Services Review Request for Review
278. Healthcare Services Review Response to Request for Review
820. Payment Order/Remittance Advice
834. Benefit Enrollment and Maintenance
835. Healthcare Claim Payment/Advice
837. Healthcare Claim Professional
837. Healthcare Claim Dental
837. Healthcare Claim Institutional

National Healthcare Identifier

There are different types of national healthcare identifiers. The National Healthcare Identifiers include:

- National Provider Identifier (NPI)
- National Health Plan Identifier (HPID)
- National Employer Identifier for Healthcare (NEI)
- National Health Identifier for Individuals (NHI)

National Provider Identifier

NPI is a special number 10 digit non disclosing number that all providers (physicians, nurses, hospitals, pharmacies etc.) can use nationwide to identify themselves. The adopted format will allow for over 200 million unique NPIs.

They will be recognized and accepted by all the companies and government organizations with which the providers do business. In addition to physicians; medical groups, hospitals, labs, and nursing - will need the new number in order to send transactions to health plans, Medicare, Medicaid, TRICARE, and electronic claims clearing houses.

Mandatory comply date May 23, 2008. Healthcare Providers.

- NPI = National Provider Identifier (Individual or Organizational) for Healthcare Providers.
- EIN = National Employer Identifier for Healthcare for Companies providing Employee Coverage.
- HPID = National Health Plan Identifier for Health Plans.
- NHI = National Health Identifier for Individuals.
- Numbers are assigned and maintained in NPS

Code Sets

Transactions contain both code sets and identifiers. Code sets are mandated by HIPAA to be standardized and certain fields in transactions must be completed only with values from code sets. Just as individuals within the United States have been assigned a unique Social Security Number, similarly every healthcare provider is assigned a unique national healthcare number, called an identifier, under HIPAA.

A code set is any set of codes used for encoding data elements. A number of different code sets have been adopted under HIPAA. The primary purpose of the code sets is to standardize the identification of those things for which healthcare providers submit claims for reimbursement and send the “minimum necessary” amount of information. This includes:

- Medical diagnosis codes
- Medical procedure codes
- Medical concepts
- Medical supplies

Code sets make it possible for people and organizations located throughout the world to identify or describe things in a standardized way. Their purpose is to eliminate subjectivity and ensure uniformity.

The code sets that have been adopted under HIPAA are:

- International Classification of Diseases, Clinical Modification (ICD-9-CM) Volumes 1 and 2
- Current Procedural Terminology (CPT)
- CD-9-CM, Volume 3, soon to be ICD-10
- Code on Dental Procedures and Nomenclature (CDT)
- National Drug Code (NDC)
- Healthcare Common Procedure Coding System (HCPCS)

Description	Code	Type of Transaction	Sent From	To
Provider uses the 270 to check a patient's insurance eligibility, coverage, and benefits.	270	Eligibility Request	Provider	Health Plan
The Health Plan sends back a 271 to provide the response information	271	Eligibility, Coverage, or Benefit Information	Health Plan	Provider
Provider needs to send a claim number with a 276 to find out about a claim.	276	Healthcare Claim Status Request	Provider	Payer (Health Plan)
Payer sends a 277 telling how the claim is progressing; includes a trace number.	277	Healthcare Claim Status Response	Payer (Health Plan)	Provider
Provider sending a 278 wants an authorization that pre-certifies guaranteed payment for the service, or a request authorizing a referral.	278	Request for Review	Provider	Payer (Health Plan)

Description	Code	Type of Transaction	Sent From	To
A response to the 278 request is also a 278.	278	Healthcare Services Review	Payer (Health Plan)	Provider
To pay insurance premiums, forward remittance advice, or both, use the 820.	820	Payment Order/Remittance Advice	Employer/Plan Sponsor	Payer (Health Plan)
Enroll, up-date data, or un-enroll participants.	834	Benefit Enrollment and Maintenance	Employer/Plan Sponsor	Payer (Health Plan)
Has to be preceded by an 837 from the Provider.	835	Healthcare Claim Payment/Advice	Payer (Health Plan)	Provider
To bill for a service performed, 837 Pro.	837	Professional (Physicians Office)	Provider	Payer (Health Plan)
Hospital charges or Long Term Care, 837 Hospital.	837	Institutional (Hospital)	Provider	Payer (Health Plan)
Dental Care, 837 Dental	837	Dental (Dental Office)	Provider	Payer (Health Plan)

Non Business Associates

Exemptions
Conduits and Financial Institutions, Postal services, Internet Providers are exempted for the definition of a business associate.

Protected Health Information

Any individually identifiable information created or received by a covered entity is PHI, regardless of the media form in which it is (or was) stored. PHI is protected under HIPAA, and the data may be stored, at rest or in transit. At rest can mean data that is:

- Accessed
- Stored
- Processed
- Maintained

In transit can mean data that is transmitted in any form. The Final rule eliminates any HIPAA protection for PHI 50 years after a patient's death.

De-identified Information

De-identified Information is simply Individually Identifiable Health Information (IIHI) with all identifying information removed.

HIPAA specifies two alternative tests for concluding the information is de-identified:

1. A person with appropriate knowledge and experience determines that the information cannot be used to identify the person described by the information
2. Certain specified identifying data elements have been removed and the covered entity has no actual knowledge that the information could be used to identify a person described by the information. This is the called the safe harbor method

Safe Harbor method

The safe harbor method includes a list of data elements that must be removed in order for information to be considered de-identified and allows for a re-identification code.

Limited Data Set

A limited data set may have fields that could possibly identify a person. Thus its use is limited to activities such as research, and the recipient must agree not to try to identify the person.

Use and Disclosure

Use and disclosure are two fundamental concepts in the HIPAA Privacy Rule. Information is used when it moves within an organization. Use refers to doing any of the following to IIHI by employees or other members of an organization's workforce sharing, employing, applying, utilizing, examining, analyzing.

Information is disclosed when it is transmitted between or among organizations. Disclosure is defined as doing any of the following to individually identifiable health information outside of the entity holding the information release, transfer, provision of access to, divulging in any manner.

Permitted Use and Disclosures

Routine disclosure

Covered entities may use and disclose PHI without authorization for their own Treatment, Payment and Health care operations (TPO). HIPAA does not require the review and approval of every routine disclosure of PHI. TPO would be considered Routine disclosures. Exceptions are allowed for a covered entity to disclose PHI to:

- Any other provider (even a non-covered entity) to facilitate that provider's treatment activities
- Another covered entity or any provider (even a non-covered entity) to facilitate that party's payment activities
- Another covered entity to facilitate that some of that entity's health care operations
- Any other covered entity within the same Organized Health Care Arrangement (OCHCA) for any health care operations arrangement

Non Routine disclosure

Covered entities may also use and disclose PHI without individual authorization for certain public interest-related activities. Non-routine requests for disclosures of PHI must be reviewed individually. Research, Subpoenas', State Licensing Boards and releasing information for Public Health among others would be considered non-routine.

All non-routine release of information needs to be listed on the Accounting of disclosures. These also include:

- Oversight of the health care system, including licensing and regulation
- Public health, and in emergencies affecting life or safety
- Research
- Judicial and administrative proceedings
- Law enforcement
- To provide information to next-of-kin
- For identification of the body of a deceased person, or the cause of death
- For facilities' (hospitals, etc.) directories
- Workman's Compensation
- Medical Examiner
- In other situations where the use of disclosure is mandated by other laws

Psychotherapy notes may be disclosed to another covered entity for TPO.

Notice of Privacy Practices

The Notice of Privacy Practices (NPP) describes how a covered entity uses and discloses health information. It must be written in plain, simple language, and it must specify an effective date. It must be given to patients upon first treatment, prominently posted, and made available to anyone who asks for it.

The Final Rule require the NPP to include a list of situations requiring authorization, the NPP must contain a statement indicating that the following uses and disclosures will be made only with authorization from the individual:

- Most uses and disclosures of psychotherapy notes (if recorded by a covered entity)
- Uses and disclosures of PHI for marketing purposes, including subsidized treatment communications
- Disclosures that constitute a sale of PHI

The Final Rule adopts, as proposed, the requirement that if a covered entity intends to send fundraising communications to an individual, the NPP must also inform the individual of this intent and that the individual has the right to opt out of such fundraising communications with each solicitation.6 Finally, the Final Rule requires that the NPP contain a statement indicating that the covered entity is required to notify the patient of any breach of his or her unsecured PHI.

Additionally, consistent with GINA, health plans are required to include a statement in their NPPs that they are prohibited from using or disclosing genetic information of an individual for underwriting purposes. The Final Rule included a limited exception to this requirement for certain issuers of long-term care policies.

Authorization

An authorization allows use and disclosure of PHI for purposes other than TPO and the public-interest disclosures permitted by HIPAA. It must be written in specific terms and signed by the individual or his or her personal representative. It may allow use and disclosure of PHI by the covered entity seeking the authorization or by a third party.

The Final Rule allows a covered entity to combine conditioned and unconditioned authorizations for research, provided the authorization clearly differentiates between the conditioned an unconditioned research components and clearly allows the individual to opt-in to the unconditioned research activities.

Minimum Necessary

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the Minimum Necessary to accomplish the intended purpose.

Under HIPAA, Minimum Necessary means

- Whatever it takes, but just enough to get the job done
- Can be the entire medical record no justification is needed and it is the requestor that will determine what the Minimum Necessary is for a specific situation

Exceptions to Minimum Necessary

The Minimum Necessary provisions do not apply to the following uses or disclosures:

- Requests by a health care provider for treatment purposes
- To the individual who is the subject of the information
- Disclosures that are authorized by the individual
- Required for compliance with the standardized HIPAA transactions
- To the HHS when disclosure of information is required under the

Privacy Rule for enforcement purposes

- That are required by other law

Under Final Rule business associates must comply with the "Minimum Necessary" principle.

Patient Rights

- Patients have a right to see and get a copy of your health records
- Patients have a right to amend your health information
- Patients have a right to ask to get an Accounting of Disclosures of when and why your health information was shared for certain purposes
- Patients may decide if you want to give your Authorization before your health information may be used or shared for certain purposes, such as for Marketing
- Patients have the right to receive your information in a confidential manner
- Patients have a right to restrict who receives your information
- If patients believe that their rights are being denied or their health information isn't being protected, they can:
  - File a complaint with the provider or health insurer
  - File a complaint with the U.S. Government
- Patients are entitled to receive a NPP that tells you how your health information may be used and shared

The Final Rule expands the requirements to include provisions designed to afford individuals with a better understanding of the following in NPP:

- Patient's right to restrict disclosures
- The types of uses and disclosures that require individual authorization
- Patient's right to opt out of certain disclosures
- Rights to notice in the event of a breach
- Rights with respect to the use of their genetic information for health plan underwriting purposes

Definition of Breach

A breach is, generally, an impermissible use or disclosure of PHI and is presumed to be a breach, unless the covered entity or business associate, as applicable, can demonstrate that there is a low probability that the PHI has been compromised.

Breach Notification

Breach of unsecured PHI covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Individual Notice
Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside.

If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.

Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their PHI was involved in the breach.

Media Notice
Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary
Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. 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.

Notification by a Business Associate
If a breach of unsecured PHI occurs at or by a business associate, the business

associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach.

To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

State Law

In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply.

"Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA.

The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws:

- Relate to the privacy of IIHI and provide greater privacy protections or privacy rights with respect to such information
- Provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention
- Require certain health plan reporting, such as for management or financial audits

HIPAA Final Rule Summary

The HIPAA Final Rule's brought sweeping changes to the HIPAA Privacy Rule. These modifications contain both substantive and technical (i.e. conforming/cleanup) changes which include, the following:

General
As per HITECH Act, a business associate is directly liable under the HIPAA Privacy Rule for uses and disclosures of PHI that are not in accord with its BAA or the HIPAA Privacy Rule itself.

As was the case under the HIPAA Privacy Rule before HITECH, business associates remain contractually liable for all other HIPAA Privacy Rule obligations that are included in BAC or other arrangements.

Patient Safety Organizations ("PSOs") are to be treated as business associates of covered entity health care providers; and patient safety activity is deemed to be "health care operations" of covered entity healthcare providers.

Marketing
The Final Rule significantly modifies the proposed rule's approach to marketing by requiring authorization for all treatment and HCOs communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed.

Sale of PHI
The Final Rule clarity that the prohibition on the sale of PHI in the absence of the patient's written authorization extends to licenses or lease agreements, and to the receipt of financial or in-kind benefits. It also includes disclosures in conjunction with research if the remuneration received includes any profit margin. On the other hand, the prohibition on PHI sales does not extend to permitted disclosure for payment or treatment nor to permitted disclosures to patients or their designees in exchange for a reasonable cost-based fee.

Business Associates
Business associates are now directly liable under the HIPAA rules:

- For impermissible uses and disclosures
- For failure to provide breach notification to the covered entity
- For failure to provide access of Electronic Protected Health Information (EPHI) either to the individual or the covered entity
- For failure to disclose PHI to the Secretary
- For failure to provide an accounting of disclosures
- For failure to comply with the requirements of the HIPAA Security Rule

Business associates must comply with the "Minimum Necessary" principle. Business associates are required to have BAA with their sub-contractors that use PHI on their behalf. Business associates must monitor their BAA with their sub-contractors.

Requirements in BAA "cascade down" to sub-contractors and sub-contractors of sub-contractors (i.e. to ALL downstream sub-contractors).

HIPAA Final Rule Summary

Authorizations
The Final Rule allows a covered entity to combine conditioned and unconditioned authorizations for research, provided the authorization clearly differentiates between the conditioned an unconditioned research components and clearly allows the individual to opt-in to the unconditioned research activities.

Decedents
The Final Rule requires a covered entity to comply with the requirements of the HIPAA Privacy Rule with regard to PHI of a deceased individual for a period of 50 years following the date of death.

The Final Rule amends the definition of PHI in 160.103 to make clear that the IIHI of a person who has been deceased for more than 50 years is not PHI under the HIPAA Privacy Rule.

Student Disclosures
The Final Rule permits a covered entity to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student. Written authorization is no longer required to permit this disclosure.

Covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or other person in loco parentis for the individual, or from the individual himself or herself if the individual is an adult or an emancipated minor. Covered entities must document the agreement obtained. The agreement obtained is effective until revoked.

Fundraising
The Final Rule permits a covered entity to use, or disclose to a business associate or to an institutionally related foundation, certain PHI for the purpose of fundraising, without individual authorization if certain conditions are met. Specifically, with each fundraising communication made to an individual, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications (i.e., an opt-out).

Furthermore, the method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. The Final Rule allows for the use or disclosure of demographic information (defined as name, address, other contact information, age, gender, and date of birth), dates of service to an individual, department of service information, treating physician information, outcome information, and health insurance status.

The Final Rule prohibits the conditioning of treatment or payment on the individual's fundraising communication choice, and requires the covered entity's NPP to state that the entity may contact the individual to raise funds and that the individual has a right to opt out of receiving such communications.

Breach Notification
Under the new provisions, an impermissible use or disclosure of PHI is presumed to be a reportable breach unless the covered entity or business associate, as applicable, demonstrates through a documented risk assessment that there is a low probability that PHI has been compromised.

There are exceptions to the definition of "breach." The first exception applies to

HIPAA Final Rule Summary

the unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.

In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The Final Rule exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information. The Final Rule articulates four factors that a risk assessment must consider:

1. The nature and extent of the PHI (e.g., sensitivity of data, likelihood of re-identification)
2. The unauthorized person by whom/to whom the PHI was used/disclosed
3. Whether the PHI was actually acquired or viewed
4. Mitigation efforts

Notice of Privacy Practices

The Final Rule requires certain statements in the NPP regarding uses and disclosures that require authorization. At the same time it is not necessary to list all possible instances wherein an authorization is required. The NPP must contain a statement indicating that an authorization is required for:

- Most uses and disclosures of psychotherapy notes (where appropriate)
- Uses and disclosures of PHI for marketing purposes
- Disclosures that constitute a sale of PHI

As well as a statement that other uses and disclosures not described in the NPP will be made only with authorization from the individual. If a covered entity does not record or maintain psychotherapy notes, it need not include the requisite statement in its NPP.

The Final Rule requires a statement in the NPP that an individual has a right to opt out of fundraising communications (i.e. if the covered entity intends to contact the individual regarding fundraising).

It also requires a statement in the NPP indicating the individual's new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the healthcare item or service.

Only healthcare providers are required to include such a statement in the NPP; other covered entities may retain the existing language indicating that a covered entity is not required to agree to a requested restriction.

The Final Rule also requires that covered entities include in their NPP a statement of the right of an affected individual to be notified following a breach of unsecured PHI.

HIPAA Final Rule Summary

Right to Request a Restriction

The Final Rule indicates that individuals have a new right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the healthcare item or service. The individual, and not the covered entity, is required to notify a downstream Health Information Exchange(s) of the restriction. A family member could make the payment on behalf of an individual and the restriction would still be triggered. The restriction does not apply for the purpose of the covered entity collecting payment and no authorization is required. This restriction only applies to covered entities that are healthcare providers.

Access of Individuals to PHI

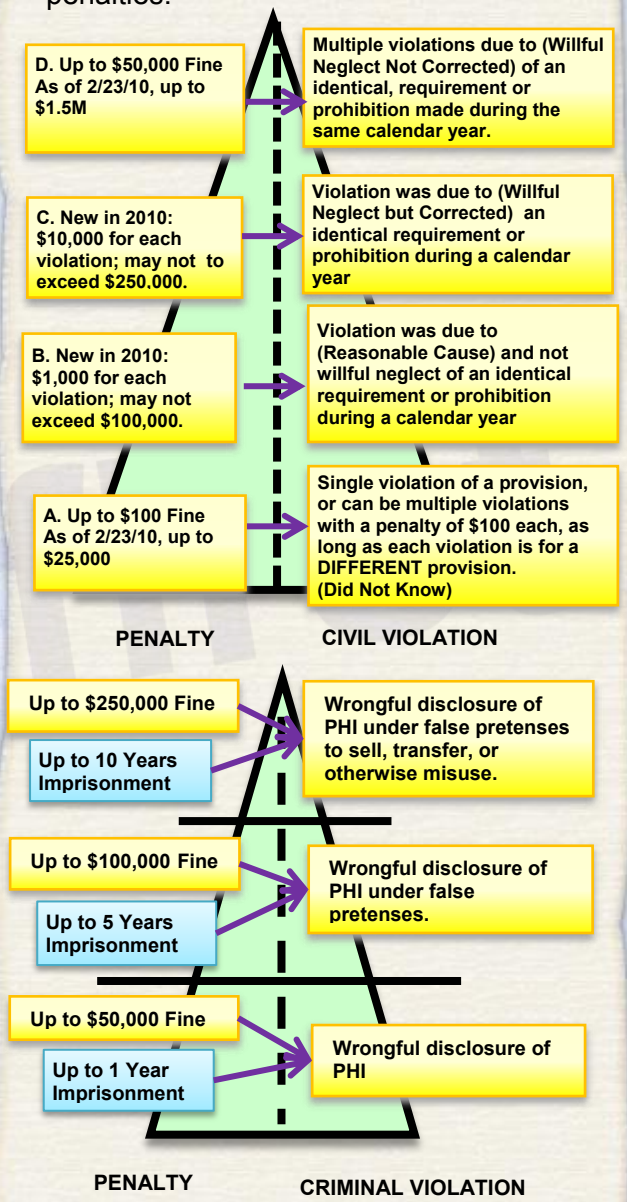
The Final Rule modifies the requirements for right to access and to obtain a copy of PHI. The provision that permits 60 days for timely action when PHI is not maintained or accessible to the covered entity on site is removed. The 30 day provision is maintained. The time period for the request is triggered at the time that the request is made.

GINA

The Final Rule implements provisions of the Genetic Information Non-discrimination Act of 2008 ("GINA"), which prohibit health plans and employers from discriminating on the basis of genetic information. The Final Rule revises the Privacy Rule to expressly include "genetic information" within its definition of "health information" and prohibits health plans from "using or disclosing genetic information for underwriting purposes."

HIPAA Penalties for Non compliance

HIPAA provides both civil and criminal penalties.



HIPAA Identifiers

The Privacy Rule protects all IIHI held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "PHI."

IIHI is information, including demographic data, that relates to:

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

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. IIHI includes many common identifiers (e.g., name, address, birth date, Social Security Number).

List of 18 PHI Identifiers:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
   - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
   - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

Acronyms

Terminology	Description
ADA	American Dental Association
AMA	American Medical Association
ANSI	American National Standards Institute
ARRA	American Recovery and Reinvestment Act
ASC	Accredited Standards Committees
BAA	Business Associate Agreement
BAC	Business Associate Contract
CDT	Current Dental Terminology
DHHS	Department of Health and Human Services
DSMO	Designated Standard Maintenance Organization
EDI	Electronic Data Interchange
EFT	Electronic Funds Transfer
EIN	Employer Identification Number
EPHI	Electronic Protected Health Information
HCFA	Health Care Financing Administration
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IRB	Institutional Review Board
NCPDP	National Council for Prescription Drug Program
NDC	National Drug Codes
NMEH	National Medicaid EDI HIPAA
NPI	National Provider Identifier
NUBC	National Uniform Billing Committee
NUCC	National Uniform Claim Committee
OCHCA	Organized Health Care Arrangement
OCR	Office for Civil Rights
PHI	Protected Health Information
PII	Protected Health Information
PSO	Patient's Safety Organization
TPO	Treatment, Payment or Healthcare Operations
URL	Universal Resource Locator

Glossary

Terms	Definition
Anonymous	Data that were collected without identifiers and that were never linked to an individual. Coded data are not anonymous.
Authorization	Document designating permission.
Compliance Date	Covered entities must comply with the HIPAA Privacy Rule by April 14, 2003.
Confidentiality	The protection of individually identifiable information as required by state and federal legal requirements and Partners policies.
Data Aggregation	Combining of sets of protected health information by a business associate to permit data analyses.
Decedents	Deceased individuals.
Electronic Medical Record	A computer-based record containing health care information.
Electronic Protected Health Information	All individually identifiable health information that is created, maintained or transmitted electronically.
Genetics	The study of how particular traits are passed from parents to children. Identifiable genetic information receives the same level of protection as other health care information under the HIPAA Privacy Rule.
Health Care	Care, services, and supplies related to the health of an individual. Health care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, among other services.
Healthcare Clearinghouse	An organization that standardizes health information.
Health Care Operations	Institutional activities that are necessary to maintain and monitor the operations of the institution.
Health Care Provider	Providers of medical or health care. Researchers who provide health care are health care providers.
Health Information	Patient information collected by a health plan, health care provider, public health authority, employer, healthcare clearinghouse or other organization that falls under covered entity.

Terms	Definition
Health Oversight Agency	A person or entity at any level of the federal, state, local or tribal government that oversees the health care system or requires health information to determine eligibility or compliance or to enforce civil rights laws.
Healthcare Insurance Portability and Accountability Act	Developed in 1996, the acronym HIPAA stands for Healthcare Insurance Portability and Accountability Act. Initially created to help the public with insurance portability, they eventually built administrative simplifications that involved electronic, medical record technology and other components.
HIPAA Violations	If a company fails to comply with HIPAA rules, they are subject to both civil and criminal penalties.
Individually Identifiable Health Information	A subset of health information, this includes demographic information about an individual's health that identifies or can be used to identify the individual.
Privacy Notice	Institution-wide notice describing the practices of the covered entity regarding protected health information.
Privacy Rule	The part of the HIPAA rule that addresses the saving, accessing and sharing of medical and personal information of an individual, including a patient's own right to access.
Protected Health Information	This includes any individually identifiable health information collected from an individual by a healthcare provider, employer or plan that includes name, social security number, phone number, medical history, current medical condition, test results and more.
Psychotherapy Notes	These include notes recorded by the health care provider who is a mental health professional during a counseling session, either in a private session or in a group. These notes are separate from documentation placed in the medical chart and do not include prescriptions. Specific patient authorization is required for use and disclosure of psychotherapy notes.
Public Health Authority	A federal, state, local or tribal person or organization that is required to conduct public health activities.
Research	A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.
Transaction	The exchange of information for administrative or financial purposes such as health insurance claims or payment.

Terms	Definition
Treatment	The provision of health care by one or more health care providers. Treatment includes any consultation, referral or other exchanges of information to manage a patient's care.
Waiver of Authorization	Under limited circumstances, a waiver of the requirement for authorization for use or disclosure of private health information may be obtained from the IRB by the researcher. A waiver of authorization can be approved only if specific criteria have been met.

Reference

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

http://en.wikipedia.org/wiki/The_Final_Rule

http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary
http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf

About Us

Devoted to our Clients. Delivering with Passion.

ecfirst with rich hands-on experience delivers world-class services in the areas of:

- Security regulatory compliance solutions (HIPAA, HITECH Act, PCI DSS, NIST and ISO 27000, State Regulations)
  - ► Risk analysis, technical vulnerability assessment
  - ► Business Impact Analysis & Development of Disaster Recovery Plans
- Security, compliance training and certification
- On-Demand or Managed Compliance
  - ► HITECH data breach and incident response management
  - ► Deployment and implementation of security technologies (including remediation)
  - ► Policy development (privacy and security)
  - ► Encryption implementation (policy, product selection, implementation)
- E-Discovery services
- Software license assessment
- Professional staffing, including project management, security officer, HL7, HIPAA, ICD 9/10 and more

Regulatory Compliance Practice

The ecfirst Regulatory Compliance Practice delivers deep expertise with its full suite of services that include; ISO 27000 readiness and training, HIPAA Privacy Gap Analysis, Meaningful Use Risk Analysis, HITECH Data Breach, Technical Vulnerability Assessment, Policy and Procedure Development, Disaster Recovery Planning, On Demand Consulting, as well as our Managed Compliance Services Program (MCSP).

Compliance and Training Certification

ecfirst, home of the HIPAA Academy, offers the gold standard in compliance training and certification. The HIPAA CHA™, CHP and CSCS™ certifications are the only certifications recognized in the Industry. The ecfirst Certified Security Compliance Specialist™ (CSCS™) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

ecfirst delivers world-class information security and regulatory compliance solutions. With over 2,000 + clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes Microsoft, Symantec, HP, McKesson, EMC, IBM, Kaiser, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.

ecfirst Differentiators

ecfirst combines state of the art tools, the highest credentialed staff, and reporting that maximizes value, efficiency, and information for our clients to deliver the industry's best technical vulnerability assessments. Critical ecfirst differentiators include:

- ISO 27000 suite of consulting and training services easily tailored to your requirements
- Home of The HIPAA Academy – First in the healthcare and information technology industry with the CHP and CSCS™ programs
- Highly credentialed professional consulting team with expertise in information security, HL7, ICD-9/10, HIPAA, HITECH, Meaningful Use
- E-Discovery Services
- Breach notification and incident response services
- Security technology deployment and implementation On Demand or Managed Compliance services
- On Demand Encryption Services to enable implementation of encryption capabilities in your environment (product selection, deployment on all portables/media, policy & more)
- Deep experience in the healthcare and information technology industries
- Compliance based technical vulnerability assessments (external, internal, wireless, firewall systems/DMZ)
- Executive dashboards that may be tailored for senior management to highlight critical findings

Contact ecfirst

Talk to ecfirst and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients.

We deliver value with intensity and are paranoid about our performance for your organization.
For more information, please call **+1.515.987.4044 x17** or visit www.ecfirst.com