Ostendio

MyVCM™ Trust Network

Healthcare and HIPAA Compliance Frequently Asked Questions

Note: This FAQ document is intended to provide an initial overview to the HIPAA and HITECH regulations. It is not intended to take the place of legal guidance for specific regulatory questions you may have.

What's HIPAA?

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA does the following:

- Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
- Reduces health care fraud and abuse;
- Mandates industry-wide standards for health care information on electronic billing and other processes; and
- Requires the protection and confidential handling of protected health information

What's the HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

What's the HIPAA Security Rule?

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

What is the HITECH Act?

The Health Information Technology for Economic and Clinical Health Act (HITECH) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act also widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for non-compliance; and it provides for more enforcement.

What is PII?

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

What is PHI?

According to the US Department of Health and Human Services, protected health information (PHI) is individually identifiable information (see below for definition) that is:

- except as provided in item 2 of this definition,
- transmitted by electronic media;
- maintained in electronic media; or
- transmitted or maintained in any other form or medium (includes paper and oral communication).

Protected health information excludes individually identifiable health information:

- in education records covered by the Family Educational Rights and Privacy Act;
- in employment records held by a covered entity in its role as employer; and
- regarding a person who has been deceased for more than 50 years.

What is individually identifiable health information?

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and is created, or received by a health care provider, health plan, or health care clearing house; and relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual, and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Individually identifiable health information (i.e., PHI) is subject to state and federal privacy and security rules including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA).

Who has to worry about PII and PHI?

Any health plan, health care clearing-house, or health care provider who transmits any health information in electronic form in connection with a qualified transaction and their business associates.

What is considered individually identifiable data?

Data is classed as "individually identifiable" if it includes any of the 18 types of identifiers for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual. These identifiers are:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
- All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- FAX number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers or serial numbers
- Web URLs
- IP address
- Biometric identifiers, including finger or voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

All protected health information is subject to federal Health Insurance Portability and Accountability Act (HIPAA) regulation.

What is electronic protected health information?

Electronic protected health information (ePHI) is any protected health information (PHI) that is created, stored, transmitted, or received electronically.

Electronic protected health information includes any medium used to store, transmit, or receive PHI electronically. For instance, the HIPAA Security Rule covers:

- Media containing data at rest (storage)
    - Personal computers with internal hard drives used at work, home, or traveling
    - External portable hard drives, including iPods and similar devices
    - Magnetic tape
    - Removable storage devices, such as USB memory sticks, CDs, DVDs, and floppy disks
    - PDAs, tablets, and smartphones
- Data in transit, via wireless, Ethernet, modem, DSL, or cable network connections
    - Email, Instant Messaging
    - File transfer

So how does this impact my business?

If you are covered entity, you are responsible for your and to some extent, your business associates' compliance efforts.

If you are a business associate, you will be required to show the covered entities and government agencies that you work with that you are compliant with the privacy requirements.

Bottom line, if you handle any of these data records, you are responsible under the HIPAA HITECH rules.

Are there penalties for noncompliance?

Yes there are; anywhere from a minimum of $100 per incidence of a violation to a maximum that will ultimately be at the discretion of HHS and is dependent on how many different kinds of violations are found. For instance,

- NY Presbyterian / Columbia University- was fined $4.8M for a breach of 6,800 people's records.[1]
- Concentra / Humana - was fined $1.7M for a breach of 148 people's records.[2]

The numbers of records disclosed were not the determining factors in the computation of the fines, it was related to the kinds of violations and subsequent remediation efforts.

Do I have to report a breach?

Yes. Any breach of 500 records or more must be reported within 60 days of discovery. Any breach of less than 500 records must be reported annually.

What's a covered entity?

Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Generally, these transactions concern billing and payment for services or insurance coverage. For example, hospitals, academic medical centers, physicians, and other health care providers who electronically transmit claims transaction information directly or through an intermediary to a health plan are covered entities. Covered entities can be institutions, organizations, or persons.

Researchers are covered entities if they are also health care providers who electronically transmit health information in connection with any transaction

[1] US Dept. of Health and Human Services
[2] Modern Healthcare

for which HHS has adopted a standard. For example, physicians who conduct clinical studies or administer experimental therapeutics to participants during the course of a study must comply with the Privacy Rule if they meet the HIPAA definition of a covered entity.

If any of the following definitions apply to you, your organization is most likely a Covered Entity.

Health Plan – With certain exceptions, an individual or group plan that provides or pays the cost of medical care. The law specifically includes many types of organizations and government programs as health plans.

Health Care Clearinghouse – A public or private entity, including a billing service, re-pricing company, community health management information system or community health information system, and “value-added” networks and switches that either process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or receive a standard transaction from another entity and process or facilitate the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

Health Care Provider – A provider of medical or health care services (see the definition in the next paragraph), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Care – Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

What's a business associate?

Business Associate – A person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

What's the relationship between the covered entity and the business associate?

The Covered entity is ultimately responsible for HIPAA and HITECH compliance. They are required to ensure through contracting practices that any business associates comply with the privacy requirements.

With implementation of the omnibus rules in 2013, Covered Entities are required to obtain "satisfactory assurances" (i.e. that their Protected Health Information will be protected as required by the rules) from their Business Associates, and Business Associates are required to get the same from their sub-contractors (now Business Associates). This "chain of assurances" (and liability) follows the Protected Health Information wherever it leads and has widespread ramifications including those related to breach notification.

With this ruling, Business Associates are also responsible for HIPAA and HITECH compliance, not only for themselves as entities, but also must get assurances on compliance from any sub-contractors that handle PHI.

Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records are all included as part of the privacy and security sections of the law.

Is compliance a one-time effort?

No compliance is an ongoing effort. According to HHS, risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

What's a compliance program?

An effective compliance program should encompass all areas of regulation that are applicable to your business. Many businesses address billing and reimbursement and HIPAA compliance, but compliance programs also should cover employment, Occupational Safety and Health Administration (OSHA) requirements, Clinical Laboratory Improvement Amendments of 1998 (CLIA) regulations, the Employee Retirement Income Security Act requirements, and other healthcare regulatory areas, including self-referral/stark law and anti-kickback regulations.

What's a compliance manager?

A compliance manager is a professional that keeps the legal and ethical integrity of a company intact through policy enforcement and program planning. They make sure all departments of a business are complying with the rules and regulations the company upholds. Compliance managers are responsible for keeping up to date with changing laws that affect the

corporate world and are responsible for preparing reports to present to their upper management detailing these laws and how the employees of the company are following them.

What is the salary of a full-time Compliance Manager?

The median pay for Compliance Managers comes out to approximately $94K per year in the United States, but employers in San Francisco offer the most; the average salary in that city is around $115K[3].

What does a Compliance Manager do?

Compliance Managers work to identify where issues with legality and ethics within a company are taking place and then fix these problems quickly and effectively. Depending on where these problems occur, serious compliance problems may result in legal consequences or firing of the individual breaching compliance within the company. Compliance Managers work with upper levels of management to ensure strategies are in place to deal with compliance problems when they occur before the reputation and integrity of the company and its staff is jeopardized.

Since the majority of this information and data normally comes through human resources and/or senior management, what is the employer's responsibility to ensure that training has taken place so that the employee does not get caught up in a violation?

The HIPAA Regulations require the employer to implement a security awareness and training program for all members of its workforce (including management). Therefore, the employer must ensure that all employees and contractors are aware of their obligations to maintain the privacy and security of protected health information (PHI) and comply with the employer's policies

[3] Salary.com

and procedures. If an employee receives the training and fails to comply — resulting in a breach, the employer organization may have a defense to a claim. The government agencies may then pursue the individual employee for the fine or penalty.

If PHI is sent to the intended recipient in an unsecured (non-encrypted) email, does that, in itself, constitute an actual breach? And must it be reported to the regulators?

Provided the individual is someone who is authorized to receive PHI, then it is not considered a breach and does not have to be reported to the regulators. Delivery of unencrypted PHI to an unauthorized individual through email may constitute a security breach incident that must be reported.

However, since email is not a secure method of transmission, the message should be encrypted to ensure it is only viewable by the intended recipient.

If my organization is a business associate, and we use remote data storage services from another vendor, are they required to sign a Business Associate agreement with us?

Yes, the vendor that is receiving PHI on behalf of your organization and ultimately the Covered Entity would be required to sign a Business Associate agreement. The rules issued in 2013, added a definition for subcontractor and have concluded that "subcontractors of a covered entity—i.e., those persons that perform functions for or provide services to a business associate, other than in the capacity as a member of the business associate's workforce, are also business associates to the extent that they require access to protected health information."

Is there a data retention requirement in HIPAA/HITECH?

HIPAA Security specifies that any documentation that is required by HIPAA (i.e., policies, procedures, actions, activities, etc.) must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

Is payroll/HRIS information (i.e., enrollment data) considered PHI?

The information is not considered PHI if it is held in an employment record held by a Covered Entity only in its role as an employer. However, if the employer is a self-insured health plan, then the health plan function would cause the entity to be considered a health plan. Consequently, information held by the self-insured health plan is considered PHI.

What are the compliance issues and scope for paper-based systems? Are all of the safeguards required for electronic PHI required of paper-based systems?

All safeguards apply to paper PHI, except for the technical safeguards, which are typically aimed at computer systems.

Policies and procedures outlining the controls in place must be developed for the protection of paper records.

What is the definition of "data at rest" as mentioned in the encryption policy and procedures?

Data at rest – defined by the National Institute of Standards and Technology (NIST) as "data in storage" (i.e., data located in databases, file systems, and email servers) includes all data in computer storage but is not limited to archived data or data that is not accessed or changed frequently.

Typically data at rest can be found in files stored on hard drives, USB thumb drives, backup tape and disks, storage area networks (SAN) or network

attached storage (NAS) and may include representations of the document in the computer's display buffers.

Who typically performs the risk assessment?

The designated HIPAA security official should perform the risk assessment. However, we recommend involving IT, compliance and internal audit so that the assessment process includes persons knowledgeable about the IT environment, organizational risks and controls, compliance issues and involves persons with skills in performing risk assessments.

Can internal audit or compliance provide HIPAA compliance assertion or does it have to be provided by a third party?

Internal audit cannot provide a third-party attestation report as this is required to be performed by a public accounting firm and performed under AICPA attestation standards. However, internal audit can be an integral component of a company's HIPAA compliance efforts by helping management gain comfort around its assertions around HIPAA compliance.

When my firm is finished implementing our compliance program, can we market the fact that we're HIPAA compliant?

There is actually no certification authority that determines HIPAA compliance. The reality is the best that organizations can do is to operate in a manner that is consistent with the regulatory framework. As a practical example OCR, the Government's Office for Civil Rights, reserves the right to make a judgment after the fact. They are looking to ensure organizations are doing what is reasonable under the guidelines.

Is the HIPAA compliance examination mandatory?

HIPAA requires that an organization perform periodic evaluations to ensure the organization's policies and procedures meet the HIPAA standards.

What are the challenges for Business Associates, including Health Information Organizations?

Compliance is a challenge because business associates constantly answer the same questions over and over again, though often phrased differently or in different formats (word docs vs spreadsheets). They often must provide different forms of evidence for each of these reviews. Not having evidence, or not having validated (externally audited) evidence, can slow the process and extend sales and implementation cycles.

What are the Challenges for Covered Entities?

Compliance is problematic for covered entities because they need to collect and review different forms of evidence and responses to questions from business associates. This takes time, does not typically leave security and compliance groups with lots of confidence since the evidence is so scattered and largely self-attested. Angst is often created between business buyers and compliance groups.

What does a third-party HIPAA audit typically cost?

According to Catalyze, a healthcare cloud provider, the estimates for the different types of audits are:

HIPAA Gap Assessment. The best starting point. It is meant to identify gaps and remediation plans for those gaps. It's the cheapest option and least time consuming. It often does not require an onsite visit from an auditor. A gap assessment leads to a full HIPAA audit; after the gap assessment, organizations spend time addressing the gaps before beginning a full HIPAA audit. Costs in the range of $17,800-$22,800.

Full HIPAA Audit. A full HIPAA audit, when applied to technology vendors, assesses an organization against all the requirements in HIPAA Security Rule. It's a long list. It includes both technical settings and configurations as well as administrative requirements like training and business associate agreements. It will involve an auditor visit and will require documentation to support claims about security and compliance; this can include showing specific technology settings like password rules and guest access. Costs in the range of $27,000-$32,000[4].

Validated HITRUST Assessment. HITRUST is a more complete, certifiable version of HIPAA. It was created by large healthcare enterprises to mirror PCI compliance. It is similar to a full HIPAA audit but goes into much more granular detail about the maturity of controls and compliance programs. There's now a standard web app that you use to enter information. Those entries are then validated by HITRUST approved assessor. Then HITRUST, the organization, reviews all the entries, typically asks for more evidence, and you hopefully get HITRUST certified at the end. Costs in the range of $44,000-$59,000.

Are there software solutions for HIPAA Compliance?

There are a number of different solutions to manage HIPAA compliance. Cloud or SaaS based software solutions tend to provide an affordable approach to managing your overall compliance program, especially for organizations that do not have a large Compliance or Privacy department. When evaluating SaaS solutions we recommend you look for solutions that address both the initial set up and also the ongoing management of your compliance program. We also recommend you look for solutions to cover compliance across a number of standards and regulations, not just HIPAA.

[4] "What is the cost of a HIPAA Audit?" Catalyze 2015

If you have any additional questions or need help developing or improving your compliance program, please contact us at info@ostendio.com.