aptible

COMMON HIPAA QUESTIONS

As a DevOps platform, we talk to a lot of software engineering teams. Explosive growth in digital health over the last few years means there are many developers and managers who haven't worked under HIPAA before. This guide is for engineering teams who could use some help with the basics.

This document is lengthy, but if you read it all, by the end you will have a solid understanding of HIPAA and how it will affect your engineering organization.

One caveat: This guide is for informational purposes only. Aptible is not a law firm, and this is not legal advice. You should contact an attorney to obtain advice with respect to any particular issue or problem.

What is HIPAA?

HIPAA is a federal law that protects the privacy and security of health data. It is enforced by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS).

HIPAA was passed in 1996 and updated by a law called HITECH in 2009. In 2013, HHS published a large administrative "Omnibus" rule to implement HITECH. For our purposes, HIPAA, HITECH, and the Omnibus Rule all refer to the same concept: The HIPAA regulations.

The HIPAA regulatory rules are, in practice, the most important aspect of HIPAA because they define the obligations of regulated entities and penalties for non-compliance. When we talk about "HIPAA compliance," we are referring to compliance with the regulatory rules.

The HIPAA regulations apply to organizations, not products or features. A company can say it is "HIPAA-compliant", but it doesn't make sense to refer to a product that way.

If you are regulated, HIPAA requires that you ensure your organization:

1. Control how you use regulated data internally and how you disclose it externally.
2. Manage data security and risk with formal policies and internal controls.
3. Identify and respond to security incidents and potential breaches of regulated data.

That is a drastically simplified summary, of course. In practice, the requirements are more complicated. The pilot audit protocol HHS used for its first round of audits has several hundred "key activities," most of which contain several audit procedures. The most challenging part of a good HIPAA compliance program is being able to prove to an auditor, customer, or OCR that you did everything you were required to, and that you made reasonable decisions along the way.

Who does HIPAA regulate?

HIPAA's formal name is the Health Insurance Portability and Accountability Act of 1996. HIPAA has a special limit: it only regulates entities that handle data that has been (or will be) related to a health insurance transaction.

HIPAA divides regulated entities into two categories:

1. **Covered Entities** - Health insurers, self-insured employers, claims clearinghouses, and health care providers who engage in certain types of electronic insurance transactions. In practice, almost all providers that take insurance are regulated, even if only some of their patients use insurance.

2. **Business Associates** - There are several kinds of business associates. The most common type is an organization that handles PHI on behalf of a covered entity or another business associate. HIPAA requires that business associate relationships be formalized in a contract or agreement, commonly called a "Business Associate Agreement" or BAA.

Business associate relationships can form a chain, usually when multiple sub-vendors are needed to provide a service. This is very common in cloud-based SaaS.

An example may be helpful: Stitch is a team communication platform for healthcare professionals. Doctors and other providers can chat, send private messages, and share pictures, video, and files with each other. Stitch has a freemium model where larger customers pay for advanced features. Stitch runs on Aptible, which in turn runs on AWS.

In this example, Stitch's customers are usually covered entities. Stitch is their business associate, because Stitch handles PHI on their behalf. Stitch in turn has several business associates, including vendors like Aptible. For a typical Aptible customer, AWS is Aptible's business associate. Aptible customers don't need to execute a BAA with AWS unless they want to use a HIPAA-eligible AWS product on their own, such as S3.

To determine whether your specific organization is regulated, you should consult an attorney.

What data does HIPAA regulate?

To be regulated, health data must be individually identifiable - what HIPAA calls “protected health information” (PHI).

PHI is a very, very broad category.

As **HHS says**:

> Protected health information is information, including demographic information, which relates to:
>
> - the individual’s past, present, or future physical or mental health or condition,
> - the provision of health care to the individual, or
> - the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

PHI is broader than just health insurance transaction data. HIPAA is like a springing trap - it hooks you, then expands to cover much more data than the hook.

Two special notes:

1. **De-Identification:** Aggregate or de-identified data is not considered PHI. HIPAA has specific rules for how to de-identify datasets.
2. **Encryption:** Encrypting PHI does not change its status as PHI. You and anyone who handles encrypted PHI for you must still comply with the HIPAA rules, including the requirement to have a BAA in place.

Who will check if we are HIPAA-compliant?

- **The Office for Civil Rights** of the Department of Health and Human Services is conducting its first round of HIPAA business associate audits in 2016. The audits will be a mix of on-site audits and "desk" audits, where entities submit proof of compliance remotely. HHS publishes a sample audit protocol that will likely resemble the procotol used for the upcoming audits.

- **Your Customers & Partners** will want to see evidence of your security and compliance practices before they entrust you with sensitive data. Compared to the likelihood of an HHS audit, customer audits are almost guaranteed. Smaller entities may send you a short checklist or schedule a brief meeting to review your security posture.

Larger, more sophisticated customers and partners will run you through an extensive vendor security review process involving a combination of:

- Security and compliance questionnaires
- Risk assessment reviews of your answers
- Negotiation of remedial controls and timelines for implementing those controls
- Requests for third-party assessments of your risk and security management program (vuln scans, pen tests, HITRUST/SOC/ISO certifications, etc.)
- Requests for direct evidence of your risk and security management program (policies and procedures, audit logs, training records, subvendor contracts, etc.)

- **Third-Party Auditors** you hire to assess your organization. HITRUST is commonly used, although many consulting firms will conduct HIPAA-specific assessments.

Can we be fined for HIPAA violations where there is no breach of PHI?

Yes, HHS can impose fines for violations of any provision of the HIPAA rules, not just ones that result in breaches.

Breaches are the only violations with reporting requirements, but HHS may investigate any complaint that a covered entity or business associate is not complying with the HIPAA regulations. That said, OCR usually reserves fines for cases where a breach occurs. HHS has the discretion to determine the amount of a penalty, up to certain limits, and must consider factors such as the nature and extent of the harm resulting from a violation. Breaches are more likely to cause serious harm, whereas other violations may be less harmful.

How do we become HIPAA-compliant?

The dumb answer is just "follow the HIPAA rules." If you comply with the rules, then you are "HIPAA-compliant." Duh.

There are several problems with the dumb answer:

1. **Complexity** - Again, look at a sample audit protocol. Even if you determine the applicable rules and satisfy them all at a single point in time, maintaining compliance over time is difficult and expensive, especially in terms of your team's time.

2. **Ambiguity** - You are responsible for implementing what HIPAA calls "reasonable and appropriate safeguards" over PHI, but it's not always clear which rules apply to you, and how. For example, encryption in transit is an "addressable" implementation specification under the Security Rule. Is it reasonable and appropriate not to encrypt traffic between an app and a database inside a virtual private cloud? What if the database protocol doesn't support encryption? Should you use a different database? There is little official guidance for engineers and developers today, although HHS has announced plans to publish some in the future.

3. **Uncertainty** - There is no official certification for HIPAA. Ultimately only OCR can decide whether you have been compliant or not, following an investigation or enforcement action. Obviously you would like to avoid those. Hopefully the upcoming HITECH audit program results will clarify how HHS interprets some of its own rules.

A better answer to *"How do we become HIPAA-compliant*?" might be:

1. Decide which HIPAA rules apply to you.
2. Decide how your technology maps to the rules.
3. Decide on a repeatable, scalable strategy for tracking compliance events. The low end might be a spreadsheet, the high end might be a GRC ("governance, risk management, and compliance") system. Examples of things you might want to track include:
    - Checklists for regular organizational and app security reviews
    - Audit logs for app and backend access permission establishment, modification, and termination
    - Audit logs for app and backend access events
    - Product security documentation
    - Internal control documentation (i.e., "policies and procedures")
    - Internal and external security assessment results
    - BAAs and other critical legal contracts
    - Incident response tickets
    - Your own vendor security assessments
4. Decide on a risk management framework (e.g., NIST SP 800-37 Rev 1) and begin with a preliminary risk assessment.
5. Decide on internal administrative controls (aka "policies and procedures").
6. Design, conduct, and audit training for your workforce.
7. Select, implement, and maintain security controls.
8. Conduct operations, including regular security assessments.
9. Respond to potential privacy and security incidents, including HIPAA breaches.
10. Repeat all of the above on a regular basis. "No less than annually and as needed based on operational events" is a good starting point. Again, look at a sample audit protocol. Even if you determine the applicable rules and satisfy them all at a single point in time, maintaining compliance over time is difficult and expensive, especially in terms of your team's time.

You will probably want help with this at some point. You can hire in-house, hire a consultancy, buy a product/service (such as Aptible), or some combination of those.

What are the HIPAA rules?

HIPAA has three main "rules," or sets of regulations, that specify how regulated organizations need to operate and handle PHI. HIPAA actually has more rules, but most of the time when we use the phrase "HIPAA compliance," we are referring to these three.

The Privacy Rule

The Privacy Rule applies to PHI in all forms (oral, written, electronic, etc.), and covers issues such as:

- Making sure your workforce only uses and discloses PHI for certain authorized business purposes. No peeking at celebrity medical records, looking up your friends' data out of curiosity, or selling PHI.
- Using or disclosing just the minimum necessary amount of PHI to accomplish whatever the current task is. Don't transmit an entire medical record if you don't need to.
- Executing BAAs with your customers, vendors, and partners.
- De-identification standards for PHI.
- Patient rights to access, amend, restrict use of, and obtain an accounting of disclosures of their own PHI.
- Requirements specific to covered entities, such as designating a privacy officer, workforce privacy training, safeguards, handling complaints, internal sanctions, publishing and updating a notice of privacy practices, and more.

The Security Rule

The Security Rule applies only to electronic PHI. It contains requirements for administrative, physical, and technical safeguards. It also requires published policies and procedures that document how you select and enforce those safeguards.
You must retain documentation and evidence of your Security Rule compliance for six years.

For many engineering organizations, the Security Rule is the hardest, most burdensome part of HIPAA. It can also be confusing: The rule is divided into "standards," which are required but often vague, and "implementation specifications," which are either required or "addressable" and usually not much more specific than the standards. HHS is working on collecting questions from digital health developers, but firm guidance and best practices are still be hard to come by.

In order to help you understand how the Security Rule may apply to a cloud-based SaaS team, we've included some questions and notes. You can read the text of the regulations to compare.

Administrative Safeguards

Management controls, encoded in policies and procedures, related to how you select and implement a security management program, including risk management.

Specific safeguards include:

Security Management Process:

- **Risk Analysis (required):** How do you compare different types of risks to each other? How do you track risk over time? How do you get information about risks, and decide which ones are relevant?
- **Risk Management (required):** How do you use risk analysis results to decide on and prioritize security controls? What levels of risk are acceptable?
- **Sanction Policy (required):** What happens to employees who violate your policies, including the HIPAA rules? How do you track sanctions?
- **Information System Activity Review (required):** How do you audit app-level and backend activity?

Assigned Security Responsibility (required): Do you have a formal HIPAA Security Officer?

Workforce Security:

- **Authorization and/or Supervision (addressable):** How do you administratively determine whether an employee or contractor should access PHI?
- **Workforce Clearance Procedure (addressable):** How do you administratively clear them for access?
- **Termination Procedures (addressable):** When and how do you administratively terminate access?

Information Access Management:

- **Isolating Healthcare Clearinghouse Function (required):** Only applies if you have a healthcare clearinghouse function. You probably don't. If you're not sure, ask a lawyer.
- **Access Authorization (addressable):** How do you technically and procedurally control access rights to PHI?
- **Access Establishment and Modification (addressable):** Same as above.

Security Awareness and Training:

- **Security Reminders (addressable):** Periodic reminders to fill the gaps between security training sessions.
- **Protection from Malicious Software (addressable):** Can be part of security training. Do you run anti-virus on laptops and workstations? How do you enforce that configuration? Do you have a secure systems development lifecycle policy? Do you use code review, code testing, continuous integration, or continuous delivery?
- **Log-in Monitoring (addressable):** How do you monitor app and backend logins? Do you use an alerting and notification system?
- **Password Management (addressable):** Do you require password managers? Does your security training cover passwords and password management?

Security Incident Procedures (required): How do you respond to and report potential and confirmed security incidents?

Contingency Planning:

- **Data Backup Plan (required):** How is PHI backed up?
- **Disaster Recovery Plan (required):** How does your organization handle availability incidents? Do you have a formal disaster recovery plan? What is your bus factor?
- **Emergency Mode Operation Plan (required):** What happens if an entire AWS region goes down? What happens if your office loses power, or part/all of your workforce is unavailable?
- **Testing and Revision Procedure (addressable):** Do you conduct tabletop and/or technical testing? How often? What are the procedures and evaluation criteria?
- **Applications and Data Criticality Analysis** (addressable): Are some of your apps and database more critical than others?

Evaluation (required): How do you evaluate and track your own Security Rule compliance? How often? Do you have a security assessment strategy? What mix of internal and external products and services do you use? Do you vuln scan and/or pen test? Do you run a vulnerability bounty program?

Business Associate Contracts and Other Arrangement (required): Do your vendor BAAs include appropriate security obligations? How do you ensure that?

Physical Safeguards

Controls to protect the physical facilities, computers, and devices that house PHI, such as data centers, offices, laptops, thumbdrives, workstations, etc. Most cloud-deployed SaaS companies try to limit their physical footprint, in terms of handling PHI. Specific scoping measures might include prohibiting your team from downloading or persisting PHI to laptops, phones, and portable media.

Specific safeguards include:

Facility Access Controls:

- **Contingency Operations (addressable):** Does your workforce need physical access to systems and devices that house PHI in the event of an emergency? Probably not.
- **Facility Security Plan (addressable):** Do you maintain a facility or equipment that houses electronic PHI? Probably not.
- **Access Control and Validation Procedures (addressable):** Same as above.
- **Maintenance Records (addressable):** Same as above.

Workstation Use (required): Most SaaS engineering teams will use laptops and desktops for work. Do you have a laptop security policy? How do you enforce it?

Workstation Security (required): How do you secure work computers, including laptops?

Device And Media Controls: Ideally you leave all PHI in your production cloud environment, and do not permit PHI to be stored on hardware or electronic media that you manage.

Disposal (required): How you destroy devices and media that handle PHI, if any?

Media Re-use (required): How you securely wipe devices and media that handle PHI, if any?

Accountability (addressable): How you track devices and media that handle PHI, if any?

Data Backup and Storage (addressable): How you back up devices and media that handle PHI, if any?

Technical Safeguards

Controls implemented through engineering processes. The technical safeguards contain elements of privacy and security by design, and should be incorporated as early as possible into your technical design process.

Specific safeguards include:

Access Controls:

- **Unique User Identification (required):** How do you ensure each user is uniquely identified? Do you have a method to discourage, prohibit, or obviate shared accounts?
- **Emergency Access Procedure (required):** Are there any types of emergencies or availability events that would require you or your users to have special access to your apps or backend?
- **Automatic Logoff (addressable):** How do you manage app and backend sessions? Are there differences between app, database tunnel, and SSH methods?
- **Encryption and Decryption (addressable):** Do you encrypt PHI at rest? If so, where and how? How do you manage keys?

Audit Controls (required): How do you audit app and backend activity? Where are logs stored? Who can access them? Can they be modified? How are audit logs backed up? How long are they retained?

Integrity Controls:

- **Mechanism to Authenticate Electronic Protected Health Information (addressable):** Do you have app or backend integrity checking for data at rest? You might do this already without realizing it: AWS S3 has built-in integrity checking

Person or Entity Authentication (required): How do your app and backend handle authentication? Do you implement MFA? Do you enforce password entropy or lifecycle requirements?

Transmission Security:

- **Integrity Controls (addressable):** SSL/TLS has built-in integrity checking. Do you use additional network integrity controls?
- **Encryption (addressable):** How do you encrypt data in transit?

  What SSL/TLS ciphers and key lengths do you permit? How do you manage certificates?

The Breach Notification Rule

This rule establishes:

- What constitutes a reportable HIPAA breach
- What you must do in case of a breach
- Who you must notify in the event of a breach. Possible entities include:
  - Your customers
  - Individuals whose identity was breached
  - HHS
  - Law enforcement
  - The media
- How quickly you must notify

In many cases, your BAA with a larger customer will be more stringent than what the Breach Notification Rule requires. For example, you might have to report breaches sooner than 60 days following your discovery of the breach.

The Breach Notification Rule also contains the rules under which unauthorized access to encrypted PHI can be excluded from being a reportable breach.

Next Steps

Now you know just enough about HIPAA to be dangerous. As you plan out your go-to market strategy, you'll be able to identify potential issues before they arise. If you'd like to chat about how to design and scale a HIPAA-compliant engineering organization in the cloud, feel free to contact us.

Learn more about how Aptible simplifies HIPAA at at www.aptible.com