TrustArc

SOLUTIONS BRIEF

Guide to HIPAA Compliance

How to Build and Implement a Program to Demonstrate Compliance with HIPAA

This *Guide to HIPAA Compliance introduces* the Health Insurance Portability and Accountability Act (HIPAA) and outlines the requirements to comply. The brief includes examples along with solutions to help build, implement, and demonstrate ongoing HIPAA compliance.

This document is intended as a general overview of the subject and cannot be regarded as legal advice. The information was based on the state of the market on the date the document was published.

What is the Health Insurance Portability and Accountability Act (HIPAA)?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created one of the first federal privacy laws in the U.S., although it was not necessarily intended as such. HIPAA was originally passed to address health insurance and its portability and to ensure that people would not be penalized for pre-existing conditions as they moved from one job to another. However, **HIPAA did include both a Privacy Rule and Security Rule** that have become, over time, the foundational data protection standards in the U.S. for the healthcare industry.

HIPAA was amended in 2009 (final rules issued in 2013) by the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act to promote the adoption and meaningful use of health information technology. The HITECH Act extended HIPAA enforcement to business associates and **added the breach notification rule**. The breach notification rule is a requirement to notify both the authorities and the impacted individuals of a breach of their information.

Companies considering if HIPAA applies to them should note that HIPAA does not apply to all healthcare entities. But HIPAA does apply to both covered entities and business associates as defined by the law:

Covered entities include health plans, health care clearinghouses (such as billing services and community health information systems), and health care providers that engage in certain electronic transactions related to payment for healthcare.[1] This means that providers that do not charge for healthcare or file insurance claims are not likely to fall under HIPAA.

Business associates are vendors to the covered entities with access to protected health information (PHI) / patient data to provide services to covered entities such as law firms, transcriptionists, and hosted software providers. Cloud providers who only transmit PHI without actual access are still considered business associates even if the data is encrypted and the service providers cannot access the data itself.

The Office for Civil Rights (OCR) under the U.S. Department of Health and Human Services (HHS) enforces HIPAA. It provides a wealth of information to assist both covered entities and business associates in their HIPAA compliance efforts. Achieving, maintaining, and demonstrating compliance with HIPAA means companies must implement the HIPAA Security Rule's administrative, physical and technical safeguards; exercise heightened diligence over their vendors with whom they share PHI; and meet the HIPAA breach notification requirements.

1. U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

What's new with HIPAA?

Business Associate Enforcement

Once HIPAA expanded to include business associates in its enforcement action, the impact of HIPAA compliance became much larger. Imagine a doctor whose business associate had a data breach that compromised PHI. Before HIPAA's expansion to include business associates, only the covered entity could be penalized by OCR for the breach. This could put many small providers out of business. However, now the liability and regulatory oversight fall onto the business associate, which is often much larger than the covered entity. For example, now, if there is a data breach by a business associate, like an email provider for a hospital, OCR would be able to hold the email provider liable as opposed to the doctor.

The implications of business associates being subject to HIPAA directly have been quite dramatic. Under the HITECH Act, business associates are now responsible for security safeguards and breach notifications. Due to this change, many covered entities revised their business associate agreements and increased due diligence on vendors.

The responsibility for security may fall to business associates. But, if the covered entities do not perform adequate due diligence, then the covered entities could be liable as well. In addition, OCR extended its audit program to business associates.[2] This all has meant that business associates have had to quickly come up to speed on HIPAA, security, and incident response processes.

Companies may choose to enter the healthcare market deliberately or may fall into it because a healthcare company purchases its products or services. For example, a customer service ticketing vendor might not target healthcare, but healthcare companies may want to purchase the service. This is significant because **many businesses may never intend to enter a market subject to HIPAA**, yet if they do, they become subject to HIPAA requirements. Ride-sharing is another example to consider. While patients using transportation to and from hospitals does not make the ride-sharing company a business associate, if the company decided to commercialize the opportunity, partner with healthcare companies, and potentially bill insurance for non-emergency transportation, this new strategy would likely make them a business associate.

Increased Enforcement Activity

OCR has been engaging in more enforcement actions and entering into resolution agreements - typically settlement agreements with corrective actions and oversight. Some of the resolutions entered into in 2018 date back to infringements that occurred or were reported in 2012. The enforcement process can take several years and involves an incredible amount of resources, time, and effort on multiple sides. Entities subject to investigation often need to bring in third parties to assist with the investigation, post-resolution, and any remediation action. In addition, **the fines for violating HIPAA can be severe**, ranging from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for each violation.

2. U.S. Department of Health & Human Services, Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

Complying with HIPAA

Fitting new Technology into Older Laws

The challenge with our technologically-driven society is that our laws cannot keep up with the pace of technology. HIPAA was adopted in 1996 (over 20 years ago - before there were even smartphones) and faced minimal amendments. This means that companies trying to build technology to older standards often face challenges in identifying how to address PHI and safeguards. For example, a company just entering the market might read HIPAA and be unsure how and when to encrypt PHI (i.e., In transmission? In local storage? In long-term storage? In the backup, etc.).

The HIPAA Security Rule safeguards are either required or addressable - a company must implement the required safeguards. Still, addressable safeguards have some leeway in how the purpose of the control is met (either implemented as provided by HIPAA, met with an alternative control, or not met because it is not applicable). No matter the option, the determination must be documented. For example, encryption is an addressable requirement under HIPAA. For encryption in particular, although it is an addressable safeguard (technically meaning that encryption is not necessarily required), there are heavy consequences associated with unencrypted laptops under state data breach notification laws and HIPAA. This is challenging for covered entities to know how and when to meet the safeguard requirements. Business associates, especially those that did not intend to enter the healthcare arena, may find meeting the requirements even more challenging.

Specific Compliance Element Challenges

Some of the ongoing activities that are the most work-intense in a successful HIPAA program are risk assessments, vendor management, and integration with other privacy laws such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

1

Risk Assessments

For risk assessments, entities must consider both the regular risk assessment required under the administrative safeguards and the risk assessments with new or changing processes/projects. For regular risk assessments, a company-wide risk assessment to review the company's status under HIPAA requirements should be done annually but no less than every two years.

For a risk assessment on new or changed products, privacy impact assessments should be an ongoing activity that is built into several company processes. These include project management, vendor consideration, technology purchases, relocation/opening of facilities, expanding scope, and mitigation following suspicious activity. Any time an element of a product or a project changes, there should be an evaluation of the change's impact on its approved state. If there has never been a connection to PHI and then an element of PHI is added as a scope expansion, the privacy office should review the impact

of the change on that activity.

2

Vendor Oversight

Vendor oversight is an area that many companies struggle with in general, not solely in the context of HIPAA. However, proper vendor management is especially critical under HIPAA. As a covered entity, a company needs to do proper due diligence upfront and repeat that due diligence at timed intervals over the life of the relationship with the vendor. The same is true for business associates that share PHI with subcontractors.

The right agreements must also be in place - business associate agreements or comparable language in contracts - to ensure that critical elements are addressed, such as security obligations, marketing permissions, and breach notifications. At a very basic level, the outsourced vendors may not realize they are now classified as business associates, and they need to be aware that they either need to come into compliance with HIPAA or decline the business opportunity.

3

Integration with Other Laws

Risk assessments, vendor management, breach notifications, and other key provisions under HIPAA are not unique to HIPAA. Many other privacy laws or requirements address one or more of these same provisions. Even just in the U.S., companies have data breach notifications in every state, and there are federal laws such as the Children's Online Privacy Protection Act (COPPA) as well to consider. Examples of state-specific laws include the new consumer privacy laws passed in 2018 in both California (CCPA) and Colorado.

There are also global laws to manage if the company has business activities subject to those laws (for example, EU GDPR and Canada's Personal Information Protection and Electronic Documents Act - PIPEDA). Many other countries also have privacy laws as well. Companies with activities that fall under another jurisdiction need to examine where the laws intersect and where they provide provisions that oppose each other.

The below chart shows how HIPAA requirements may overlap with requirements from other laws.

HIPAA Requirements	California CCPA	EU GDPR	Canada PIPEDA	China Cybersecurity
Notice	✓	✓	✓	✓
Risk Assessment	✓	✓	✓	✓
DPIA/ PIA	✓	✓	✓	
Vendor Management	✓	✓	✓	✓

Individual Rights	✓	✓	✓	✓
Consent Provisions	✓	✓	✓	✓
Security Requirements	✓	✓	✓	✓
Incident Response	✓	✓	✓	✓
Breach Notification	✓	✓	✓	

Companies should review these specific laws for complete information and to determine subjectivity and compliance needs.

Ten Steps to HIPAA Compliance

A sample 10-step guide to HIPAA compliance follows:

Assess
Business Activities

1. Determine if HIPAA applies to any part of the business - as a covered entity or a business associate
2. Conduct a gap analysis, where applicable, against the Administrative requirements, Privacy Rule, Security Rule, and Breach Notification Rule
3. Determine if cross-compliance overlaps with other privacy regimes (i.e., U.S. federal, U.S. state, or other geographies)
4. Map processes to determine the scope and reach of HIPAA to business activities, data, systems/applications, and vendors (including how to manage individual privacy rights)

Implement
HIPAA Compliance

5. Develop or enhance privacy and security policies to comply with HIPAA
6. Build a successful, ongoing vendor management program addressing contracts, due diligence, and ongoing monitoring
7. Implement individual rights mechanisms and coordination with upstream and downstream entities
8. Develop a privacy impact assessment process that integrates into the company culture

Maintain
HIPAA Compliance

9. Perform a thorough annual company risk assessment that is consistent year-over-year and includes assessing technical vulnerabilities
10. Maintain a calendar of compliance activities, including policy reviews and updates, employee training, vendor assessments, and reporting to executives

TrustArc's HIPAA Compliance Solutions

TrustArc offers a broad range of solutions to help companies build and manage a privacy program.

HIPAA Assessment

TrustArc will work with a company to perform a detailed and comprehensive assessment of its current privacy program against the core privacy requirements of HIPAA and its associated regulations.

The assessment project consists of two phases:

PHASE 1

A checklist-based assessment of the company's practices to identify those elements or activities needing development or revision per the HIPAA Privacy and Security Rule requirements.

PHASE 2

Development of a detailed Strategic HIPAA Privacy and Security Priorities Plan based upon the gaps identified during Phase 1.

The result of this approach is to provide the company with a better understanding of its compliance posture and to provide a concrete action plan for closing any gaps or improving the efficiency of risk management activities.

HIPAA Consulting

TrustArc also offers Consulting to help with:

- **Policies to address HIPAA compliance**
- **Incident response and testing**
- **Building a data governance program**
- **Risk analysis**
- **Privacy/Security awareness and training**
- **Framework readiness (i.e., HITRUST, NIST, etc.)**

TrustArc PrivacyCentral

Your command center for data privacy operations. Imagine having an intelligence dashboard that demonstrates your privacy compliance status and identifies gaps for needed actions. PrivacyCentral dynamically monitors where your company stands concerning quickly changing data privacy laws such as GDPR, HIPAA, CPRA, and PIPL. Get real-time, actionable insights to reach compliance.

With simple inputs, you can:

Understand which laws and regulations apply to you and what are the most important steps to mitigate risk.

Develop a privacy strategy that is trackable, measurable, and scalable.

Create an action plan — and accountability mechanisms — against specific laws.

Learn how PrivacyCentral can supercharge your privacy program

Get a tailored consultation with our privacy experts.

Book Now

Why TrustArc?

TrustArc has extensive experience working with companies in the healthcare field, including covered entities and business associates, established businesses and start-ups, technology-focused companies, direct patient-care providers, and clinical research companies. We assist companies throughout the lifecycle of HIPAA compliance, from immediate needs, such as determining subjectivity, initial risk assessments, and employee training, to long-term needs, such as vendor management, data inventory, and PIAs. We can also partner with companies on corrective action plans under regulatory oversight.

Manage HIPAA Compliance with PrivacyCentral

Schedule a Tailored Consultation

About TrustArc

As the leader in data privacy, TrustArc automates and simplifies the creation of end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation, that is essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information, visit www.trustarc.com.