virtru

HIPAA Guide for Email and File Protection:

Ensure Compliance and Maintain Patient Privacy

In this Guide

HIPAA Overview

Safeguards for Email and Files

Core HIPAA Compliance Challenges

Maintaining Patient Confidentiality and Trust

Data-Centric Security as a Best Practice for Compliance and Privacy

Our personal health and medical information contains some of our most sensitive personal data. Advances in modern medical technology and information systems have revolutionized patient care and made our personal health data increasingly valuable, in part due to the digital transformation spurred by meaningful-use requirements for healthcare IT.

As modern medicine evolves to value-based, accountable care models that focus on quality of outcomes rather than quantity of services, the introduction of new digital healthcare delivery models, cloud-based applications, and connected health devices has presented unique challenges and opportunities. Most critically, healthcare providers need to quickly and securely access patients' health information.

Digital health workflows allow distributed healthcare provider teams to more easily coordinate care and interact with their patients, leading to better outcomes. But these trends also bring significant risks to patient confidentiality. Multi-cloud environments that support digital care delivery leave protected health information (PHI) at risk of exposure, raising concerns regarding patient confidentiality and compliance with the Health Insurance Portability and Accountability Act (HIPAA).

While Electronic Medical Record (EMR) systems have made the storage and transmission of PHI more efficient and secure, they cannot support all sharing scenarios. PHI sharing workflows still rely on email and file systems, making email and file protection central to an effective HIPAA compliance and patient confidentiality program.

HIPAA Overview

HIPAA was created by the U.S. Congress in 1996 to modernize healthcare information systems and prevent fraud and theft of PHI.

HIPAA defines PHI to include any data associated with a patient's physical or mental health status, along with any related treatments or payments. In practice, PHI includes personally identifiable information (PII) such as names, social security numbers, and addresses, plus healthcare-centric information such as medical record numbers, insurance plan member IDs, medical device identifiers and serial numbers, and International Statistical Classification of Diseases and Related Health Problems (ICD-10) codes.

A key provision in the regulation is the HIPAA Privacy Rule, which gives patients more control over how PHI is protected when transmitted electronically by "covered entities," or organizations that deal with health-related data, such as healthcare provider organizations, health plans, and even state governments and educational institutions. When covered entities engage third parties, or "Business Associates" in HIPAA parlance, to store, process, and interact with PHI, a Business Associate Agreement (BAA) must be in place to impose safeguards on how the Business Associate uses and discloses PHI. Examples of Business Associates include data protection software vendors, cloud infrastructure providers, and cloud-based file collaboration platform vendors.

HIPAA Privacy Rule vs. Security Rule for Covered Entities

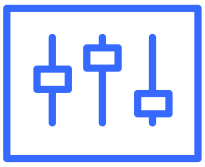
Although the Privacy Rule and Security Rule work together, they are distinct in that they each have a unique purpose.

Privacy Rule: Focuses on the rights of the patient and their ability to control their PHI by setting the standard for, among other things, who may have access to PHI. The Privacy Rule covers the physical security and confidentiality of PHI in all formats including electronic, paper, and oral.

Security Rule: Only deals with the protection of electronic PHI (ePHI) that is created, received, maintained or transmitted. Covered entities are required to implement adequate physical, technical and administrative safeguards to protect patient ePHI, for example when sharing via email or storing on the cloud.

HIPAA Safeguards for Email and Files

Rapid access to PHI is crucial to fulfilling the mission of healthcare provider organizations, and sharing medical records via email and files is often the path of least resistance, especially in emergency scenarios. That means IT teams need to be aware of how the HIPAA Security Rule pertains to email and file systems. The rule outlines several technical safeguards, three of which apply most directly to email and files:

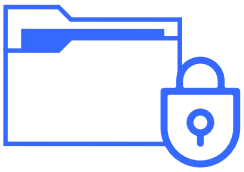


Access Controls

Access controls encompass privileges for employees of covered entities to access PHI to perform their job functions using information systems, applications, programs, or files.

Audit Controls

Audit controls include technology and processes that support the analysis of activity in information systems that contain or use ePHI. These controls are especially relevant for determining whether data has been breached and assessing the impact.



Transmission Security

Transmission security refers to technical measures to protect against unauthorized access to PHI transmitted electronically, including Integrity Controls that prevent improper modification of PHI and encryption that protects PHI from access by unauthorized third parties.

The language in HIPAA encourages covered entities to evaluate their unique risks, and discuss reasonable and appropriate security measures for these technical safeguards. However, HIPAA offers some prescriptive recommendations that are especially relevant in today's world of undefined perimeters, porous cloud environments, and PHI sharing workflows powered by email and files:

"As business practices and technology change, situations may arise where ePHI being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. Where risk analysis shows such risk to be significant, a covered entity must encrypt those transmissions."

HIPAA Considerations in the Cloud

A fundamental example of the "business practice and technology change" referred to in the HIPAA text above is the migration of health IT infrastructure from legacy on-premise Microsoft Exchange environments to cloud platforms that support email and files. The two most relevant platforms are Google G Suite and Microsoft Office 365. Since healthcare organizations are becoming increasingly reliant on these platforms to store and share PHI, both Microsoft and Google have implemented standard BAAs for HIPAA-regulated customers.

But, unfortunately, *signed BAAs do not automatically make G Suite and Office 365 HIPAA compliant*. While G Suite and Office 365 offer native protections like network-level encryption and audit reporting, they lack the persistent, data-centric security measures that ensure HIPAA compliance wherever PHI is shared throughout the course of care.

Further, HIPAA compliance depends on how the security controls in these cloud platforms are used, and that is the responsibility of the covered entity's IT team. Organizations cannot outsource data protection and compliance to their cloud providers. **While most cloud providers deliver security, ultimate responsibility lies with the organization itself.** Most of the industry follows a model called "shared responsibility," which breaks down data security and compliance responsibilities as follows:

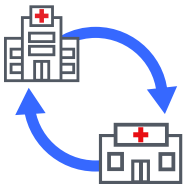
- **Cloud service providers are responsible for the security and compliance of their cloud-based infrastructures, including computing, storage, databases, and networking.**
- **Organizations are responsible for the security and compliance of their own data, networks, applications, and operating systems that live in the cloud.**

Core HIPAA Compliance Challenges for Email and File Protection

Over 60% of reported data breaches in the first half of 2019 alone were due to human error, and healthcare was affected more than any other sector. This figure reveals the constant challenges healthcare information security teams face in enabling PHI access for end users while, at the same time, mitigating HIPAA compliance risks. The following scenarios illustrate these pain points in sharper detail.

Secure PHI Sharing

Sharing PHI with appropriate parties in a timely, secure fashion while preventing unauthorized access and misuse is a core HIPAA compliance challenge. Complexities arise when healthcare providers must exchange PHI with other healthcare providers, payer organizations, new contractors, and employees.



Provider-to-Provider PHI Sharing

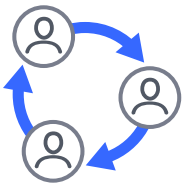
In order to coordinate care and optimize treatment outcomes, healthcare providers need to exchange a wide range of PHI, including patient medical histories, X-rays, MRI scans, blood test results, and treatment plans, across disparate systems.

While EMR and EHR systems may enable secure access to PHI in some scenarios, often they don't support the interoperability needed to give caregivers immediate access to patient records. Provisioning and managing new accounts for out-of-network physicians overburdens the organization's limited IT resources. And if a patient has an unexpected, life-threatening condition and an out-of-network surgeon needs access to medical charts before an emergency operation, the surgeon can't afford to wait for EMR account provisioning. They'll simply get the PHI over email and file systems they already use.

Provider-to-Payer PHI Sharing

Providers also need to exchange medical billing claims that contain PHI with payer organizations, whether they are private insurance companies like Aetna or state-funded healthcare payers like Medicaid and Medicare.

Enabling efficient, secure billing workflows runs into cross-platform provisioning and interoperability issues that resemble those outlined in the provider-to-provider scenario above. EMR and medical billing systems are not always tightly integrated, and provisioning new accounts for external users across siloed IT systems can be a drain on IT resources. Exchanging claims records that contain PHI via email and file systems becomes the de facto sharing mechanism.



Human Resources PHI Sharing

HR and other general and administrative personnel within healthcare organizations also deal with PHI frequently. Through the course of hiring and onboarding new nurses, physicians, specialists, and lab technicians, PHI must be shared for health benefits enrollment and other administrative support. While these PHI exchanges are not directly linked to treatment, supporting new doctors and provider personnel with health benefits is just as critical to care delivery.

These workflows are also subject to the same regulatory scrutiny as patient data exchanges. But because they happen before the employee is formally onboarded and set up with accounts in the organization's IT systems, HR teams often rely on email and file systems to share this data.

In these cases, the most seamless, secure PHI sharing method is often encrypted email or file systems backed with data-centric security. These provide the persistent protection and control wherever PHI is shared, ensuring healthcare providers can adhere to HIPAA's access control, audit control, and transmission safeguards.

Maintaining Patient Confidentiality and Trust

HIPAA is inextricably linked to patient confidentiality, but building a trusted long-term patient relationship goes beyond HIPAA compliance and requires a deeper commitment to keeping patient PHI safe and private.

Risks to Patient Confidentiality and Care

- In a survey of over 200 IT security leaders, when asked: "What concerns you most about data privacy failures?," **damage to patient trust outranked regulatory fines as the top concern** among healthcare industry respondents.
- Breach damages are more than financial. A study found that **in the three years following a data breach, care delivery lagged, and patients had increased mortality rates**.

The challenge of maintaining patient confidentiality and trust goes beyond HIPAA liability. When a primary provider shares patient PHI with another provider, and that secondary provider later fails to adequately protect PHI, HIPAA liability technically falls on the secondary provider. But that doesn't change the fact that it was the primary provider's patient whose privacy was violated. Even though the primary provider isn't likely to face HIPAA noncompliance fines, the circumstances can irreparably damage the delicate relationship between the patient and the primary caregiver. And in cases where the breached PHI includes socially taboo information like mental health records, a breach can lead to acute stress and suffering that poses an immediate health threat.

This reinforces the notion that healthcare organizations need to treat patient confidentiality as a corporate social responsibility. In other words, they need to go above and beyond the bare minimum HIPAA safeguards.

Data-Centric Security as a Best Practice for HIPAA Compliance and Privacy

To preserve HIPAA compliance and patient privacy, health IT security best practices have evolved beyond traditional perimeter-based, network-level protections to embrace data-centric security approaches. Data-centric security encompasses *data control*, or the ability to apply persistent security policies, regardless of location, device type, or hosting model, and *intelligence*, which refers to the real-time visibility of contextual information that enables threat monitoring and incident response workflows.

Data-centric security closely aligns with the HIPAA Security Rule's technical safeguards for email and files mentioned above. Data control assures that access controls and transmission security safeguards via encryption and security policies accompany PHI wherever it's shared. Intelligence covers audit controls via persistent visibility over who has accessed data, when, where, and how.

But the power of data-centric security exceeds these minimum HIPAA compliance safeguards. Security that protects PHI shared via email and files across disparate healthcare environments ensures patient privacy, which helps cultivate relationships that lead to better care outcomes.

Virtru for HIPAA Compliance and Patient Confidentiality

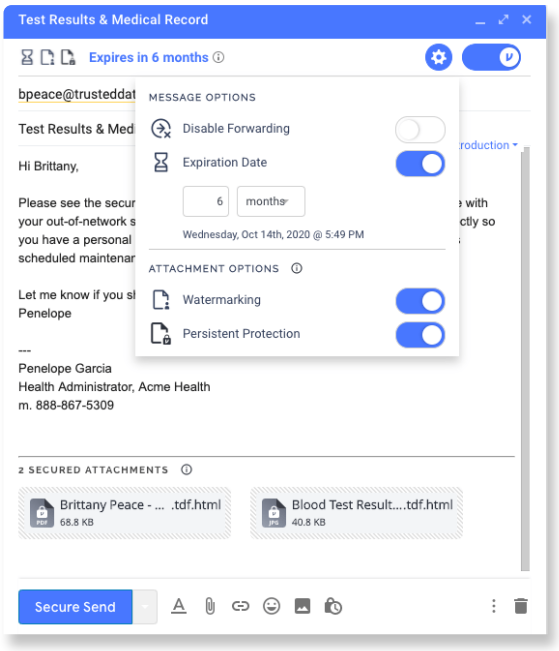
Virtru's data-centric security platform has helped thousands of healthcare organizations with HIPAA compliance and patient confidentiality. Organizations that leverage Virtru to protect email and files avoid HIPAA noncompliance fines by keeping their PHI secure, wherever it's shared. Virtru provides end-to-end encryption, granular access controls, and visibility to enable secure PHI sharing. With Virtru:

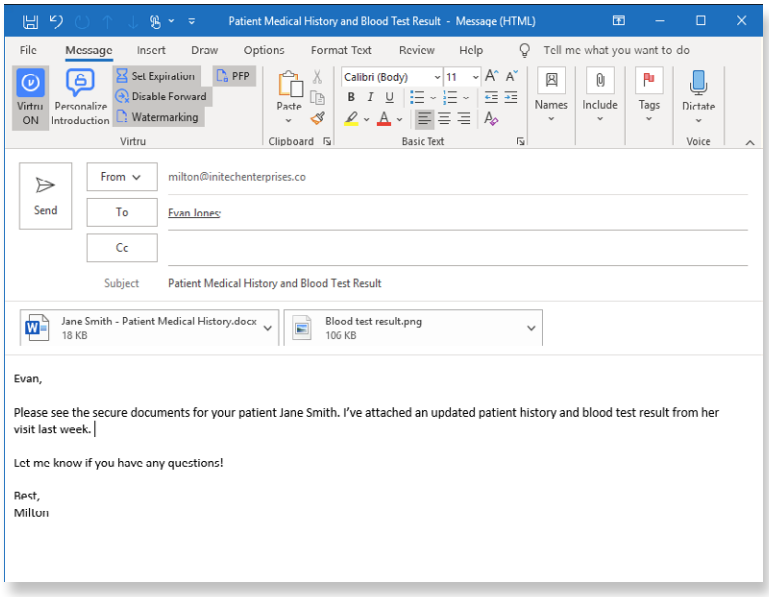
- **Out-of-network providers gain seamless and secure access to patient reports, test results, and treatment plans beyond the EMR to improve care coordination.**
- **Payer organizations securely access billing claims to support faster provider reimbursement cycles.**
- **HR teams easily exchange PHI via email with new doctors, nurses, technicians, and other employees and contractors. while maintaining HIPAA compliance.**
- **Healthcare IT and security teams can easily prove HIPAA compliance with intelligence on who has accessed PHI, when, where, and for how long.**

ComForCare HOME CARE

"Virtru offered us a way to transport our data in a way that was 100% HIPAA compliant. Their protection for email and files and persistent access controls gave us the assurances we needed."

- Nathan West, Director of Technology, ComforCare





Virtru lets you easily protect and control messages and attachments in Gmail (left) and Microsoft Outlook (right)

Meanwhile, ease of use reduces support costs for overburdened IT teams. Virtru security is embedded into the email and file applications already used across healthcare organizations, such as Microsoft Outlook, Gmail, and Google Drive. That means IT teams aren't forced to create new accounts for EMR or billing systems to support one-off PHI sharing scenarios with out-of-network specialists or payers. Also, external recipients don't need to create new portal accounts and manage another password to access PHI protected by Virtru.

Virtu's data-centric approach to security gives healthcare organizations the highest assurances that their patients' privacy will be preserved during the PHI lifecycle and throughout the entire course of care.

Virtru makes it easy to maintain patient confidentiality and compliance. Contact us to learn more: virtru.com/contact-us

virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection.

Visit virtru.com or follow us on Twitter at @virtruprivacy.