A Comprehensive Guide to HIPAA-Compliant Cell Phone Safeguards and Policies

Given the Health Insurance Portability and Accountability Act's (HIPAA) extensive protections and restrictions regarding electronic protected health information (ePHI), cell phones present a challenging grey area to navigate. However, implementing a HIPAA-compliant cell phone policy and appropriate security controls will help your healthcare entity properly adhere to regulations.

HIPAA-Compliant Cell Phone Policies and Usage

Achieving and maintaining HIPAA compliance can easily be threatened by healthcare personnel's cell phone usage. At first consideration, cell phones and their various security risks would seem opposed to HIPAA compliance but the right implementations can help any healthcare entity with their efforts.

Ensuring HIPAA-compliant cell phone usage requires:

- Understanding ePHI as it relates to HIPAA compliance and potential breaches
- Knowing what telecommunication methods to monitor
- The beneficial policies and security measures healthcare entities should implement

As a HIPAA compliance and cybersecurity expert, [REDACTED] can advise your compliance program. Further, as a managed security services provider (MSSP), [REDACTED] provides many of the cybersecurity measures and training programs healthcare personnel should implement.

Understanding ePHI and HIPAA Compliance

Implementing HIPAA policies and security measures with respect to cell phones first requires understanding the ePHI that must be safeguarded. The Department of Health and Human Services (HHS) refers to and summarizes the HIPAA Privacy Rule's understanding of ePHI as "individually identifiable health information" covering:

- Physical or mental health or conditions (whether past, present, or future)
- Provisioned healthcare and any payments thereof

- Demographic data (when not individually identifiable)

“De-identified health information” doesn’t count as ePHI. To be considered de-identified, the data must neither identify an individual nor provide a reasonable basis to do so via one of two methods:

- A statistician’s formal determination
- All specified identifiers related to the individual and their relatives, household members, and employers must be removed to the extent that a given healthcare entity “has no actual knowledge that the remaining information could be used to identify the individual.”

HIPAA-Permissabe ePHI Uses and Disclosures

An individual’s ePHI may only be used or disclosed (i.e., made known or accessed by a nonauthorized party) with their written consent or in the following circumstances without it:

- To the individual
- For conducting the individual’s treatment, payment, and healthcare operations
- Following a clear opportunity provided to the individual to agree, acquiesce, or object
- As a result of or incidental to permissible uses and disclosures—so long as reasonable safeguards have been adopted and the shared information was kept as minimal as possible
- For public interest and benefit purposes, although rigid circumstances and procedures must be met to remain compliant
- As part of limited data sets, if it is de-identified information that also meets additional criteria:
    - Used and disclosed for research, healthcare operations, or public health purposes
    - The individual has given consent in a data use agreement
    - Specified safeguards have been implemented to protect the identifiable portions of the information

Understanding HIPAA's Definition of ePHI Breaches

Ensuring HIPAA-compliant cell phone usage also requires understanding what the regulations define as constituting a "breach." Your organization cannot prevent security issues it doesn't understand.

HHS and the Breach Enforcement Rule define a breach as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information." Thus, any ePHI accessed, acquired, or interacted with by nonauthorized personnel, without receiving an individual's written consent, or outside the six circumstances described above constitutes a HIPAA breach.

This definition of breach does allow for specific exceptions:

- If the covered entity or business associate responsible demonstrates that the probability that the ePHI has been compromised is low—based upon conducting a risk assessment that includes the following factors:
    - The nature and extent of the used or disclosed ePHI, notably, the types of identifiers and chance of an individual's identification
    - The unauthorized party that used the ePHI in question or to whom the disclosure occurred
    - If the ePHI was actually used or viewed
    - If the use and disclosure risks have been mitigated appropriately
- If the acquisition, access, or use of ePHI by a covered entity's employee or a business associate acting under their authority was unintentional, made in good faith, and within their authoritative scope
- If an authorized person made the disclosure to another person that is generally authorized to access individuals' ePHI within the scope of their responsibilities due to:
    - Being employed by the same healthcare entity
    - Being employed by the healthcare entity's business associate
    - Operating as part of an organized healthcare arrangement in which the healthcare entity participates
- If the party to whom ePHI is disclosed is unable to retain the information in any capacity

Are Cell Phones HIPAA-Compliant?

Generally, HIPAA regulations specify:

- The security standards that must be upheld to safeguard ePHI
- Entities' responsibility to regularly conduct risk analysis for determining the necessarily implemented administrative, technical, and physical measures

While unprotected cell phone access to or transmission of ePHI would significantly risk a HIPAA breach, the regulations do not explicitly prohibit cell phone or other specific technology usages outright. However, inadvertent use or disclosure and data or device theft that do constitute HIPAA breaches exponentially increase if ePHI is accessed on a cell phone or discussed over unsecure lines of communication.

So long as the appropriate security controls and processes are in place, cell phone use does not constitute a HIPAA breach.

Are Cell Phone's Conversations HIPAA-Compliant?

Both phone call conversations and faxed documents do not factor as ePHI, per the HIPAA Privacy Rules' definitions under 45 CFR § 160.103. However, a phone conversation may constitute the disclosure of PHI if any discussion of identifiable health information falls outside of the HIPAA permissible circumstances listed above.

With the use of a second cell phone line app, HIPAA-compliant telecommunications may be more easily achieved. These services provide a secondary line for phone calls, texting, and voicemail personnel to interact with inside a segmented window on an existing device.

As an organizational policy, your entity's representative on a phone or web-conferencing call should always identify themselves and confirm the other person's identity. This practice helps ensure that the entity's representative confirms their authorization to discuss PHI and that they are speaking to the individual whose information is being discussed (or someone acting in an official and recognized capacity as the individual's representative).

Security Controls and Policies for HIPAA-Compliant Cell Phone Usage

HIPAA requires healthcare entities and their business associates to implement and maintain technical, administrative, and physical safeguards. The first two categories directly apply to cell phone usage. While there are ultimately no realistic physical safeguards that may be adopted for cell phones, certain technical measures (e.g., passcodes and authentication, encryption) will virtually eliminate physical security and compliance risks.

Healthcare entities should consider technical safeguards ranging from activating (or deactivating) native device capabilities to implementing additional security measures. In addition, some technical safeguards may also be provided as native to cell phone applications and services.

Administrative safeguards consist of the mobile device policies that healthcare entities should enact and enforce. These policies should establish behavior expectations that oversee personnels' cell phones usage.

Device-Native Technical Safeguards for HIPAA-Compliant Cell Phone Usage

Many cell phones come equipped with native capabilities that healthcare professionals and business associates should activate or deactivate as part of organization-wide HIPAA compliance.

Native security capabilities to enable include:

- Passcodes – All cell phones and other portable devices that may be locked with pass- or pin codes should have the security feature enabled. Locking devices will certainly not deter all potential attempted and unauthorized access instances but provides an immediate barrier to protecting any stored ePHI.
- Device Encryption – Android and iOS cell phones natively provide device encryption capabilities. Device-level encryption methods render firmware, software, and stored data unreadable without the associated cryptographic key. Device-level encryption is critical for HIPAA-compliant cell phone use, as it provides entities with a security measure that enforces two of the specified exceptions to incidents that constitute data breaches:
    - The ability to demonstrate that the probability ePHI was compromised is low.
    - The party to whom ePHI was disclosed (accidental or otherwise) will not be able to retain the data in any capacity (e.g., reading it on the screen, transferring it to another device) without the cryptographic key.

Deactivation as a Technical Safeguard

While most technical safeguards and security measures native to devices—or to the IT resources and storage they access—will need to be enabled, automatic backup and file sharing capabilities should be deactivated.

These capabilities do provide benefits in personal device usage. However, this functionality constitutes a HIPAA violation if ePHI is automatically backed up to any personal and unsecure storage locations (e.g., Google Drive, a cell phone carrier's cloud storage) or shared.

As with many HIPAA violations, automatic backups would most likely lead to inadvertent noncompliance. Unfortunately, HIPAA penalty enforcement does not consider whether an incident that qualifies as a violation was intentionally or inadvertently committed.

Multifactor Authentication (MFA) and Stored Login Credentials

Multifactor authentication (MFA) requires users accessing a given IT resource (e.g., system, application, cloud service) to provide at least one additional method of identity verification as part of the login process. Generally, personnel provide a standard username and password combination before receiving a prompt for additional verification. This capability should be activated for any IT resource capable of interacting with or storing ePHI that provides MFA.

MFA methods for IT resources accessed via mobile device include:

- **One-time passwords (OTPS)** – OTPS may enforce MFA via various methods, including:
    - "Authenticator" applications – These applications display a randomly generated pin code that remains a valid credential for identity verification for a set duration (e.g., 30 seconds). After the duration concludes, a new random pin code is displayed.
    - SMS or Email – This MFA method will send the user the OTP via SMS or email for manual input.
- **Biometric identification** – These methods include:
    - Fingerprint scanning
    - Facial recognition

In addition to enforcing MFA, any cell phone that stores or interacts with ePHI should not also store login credentials for any IT resource. If a hacker obtains access to the cell phone, stored credentials allow them to immediately access apps, services, cloud storage, and more without enforcing any additional security measures.

Implemented Technical Safeguards for HIPAA-Compliant Cell Phone Usage

Some technical safeguards that healthcare entities should implement will not be native to cellphones. The safeguards include:

- **Virtual private networks (VPNs) or virtual private clouds (VPCs)** – VPNs and VPCs provide secure network and cloud connections to protect any ePHI data transmitted to or from a cell phone.
- **Remote wiping or disabling** – Should a cell phone be lost or stolen, these capabilities allow an entity's security team to delete ePHI (and other data) or prevent any access to it.

- **Firewalls and antivirus** – Mobile device-specific implementations of standard security measures should be enforced on cell phones to prevent viruses, malware, phishing, and other common intrusion methods.

Administrative Safeguards for HIPAA-Compliant Cell Phone Usage

As important as technical safeguards are for protecting ePHI that cell phones interact with or store, your organization must also construct, promulgate, and enforce official policies to help ensure HIPAA compliance. A HIPAA cell phone policy should include specifications for:

- **Secure network and internet connections** – Healthcare personnel's cell phones should never connect to any entity IT environments or interact with ePHI over public or unsecure networks.
- **Email restrictions** – ePHI should never be transmitted via email.
- **Cell phone cameras** – While cell phone cameras provide an efficient and easy means for uploading images or providing a reference to colleagues, personnel should never take photos of anything that constitutes PHI.
- **Contacts** – Storing patient contact information on a phone constitutes a HIPAA compliance violation waiting to happen. Similarly, any patient that stores healthcare provider contact information on their cell phone may cause a HIPAA violation. Since entities cannot control their patients' cell phone contacts, they should consider adding a disclaimer (to be verified as binding by appropriate legal counsel) amongst signed forms.
- **Updates and Other Configurations** – Cell phones should be configured to automatically install all available updates upon their release (e.g., operating systems, applications, threat signatures). Further, policies should prohibit any changes to HIPAA-specific and general cybersecurity configurations that the entity deems necessary.
- **Security awareness training** – Healthcare entities should regularly provide their personnel with regular training to educate them on security practices and IT-related HIPAA compliance efforts. Advanced security awareness training may include elements such as phishing simulations to help personnel better recognize indicators of malicious activity.

Ensure HIPAA-Compliant Cell Phone Usage

As with other HIPAA compliance efforts, ensuring that healthcare personnel's cell phone usage adheres to regulations requires extensive technical and administrative safeguards to protect

ePHI. While cell phones are not inherently HIPAA-compliant or noncompliant, interacting with or storing ePHI on mobile devices presents a far greater likelihood for violations to occur.

Without conscientious effort, healthcare personnel may inadvertently violate HIPAA-compliant cell phone practices.

To establish, assess, or remediate your organization's cell phone policies and security implementations for HIPAA compliance, contact [REDACTED] today. As a HIPAA (and HITRUST) compliance and cybersecurity expert, we can help your organization maintain regulatory adherence.