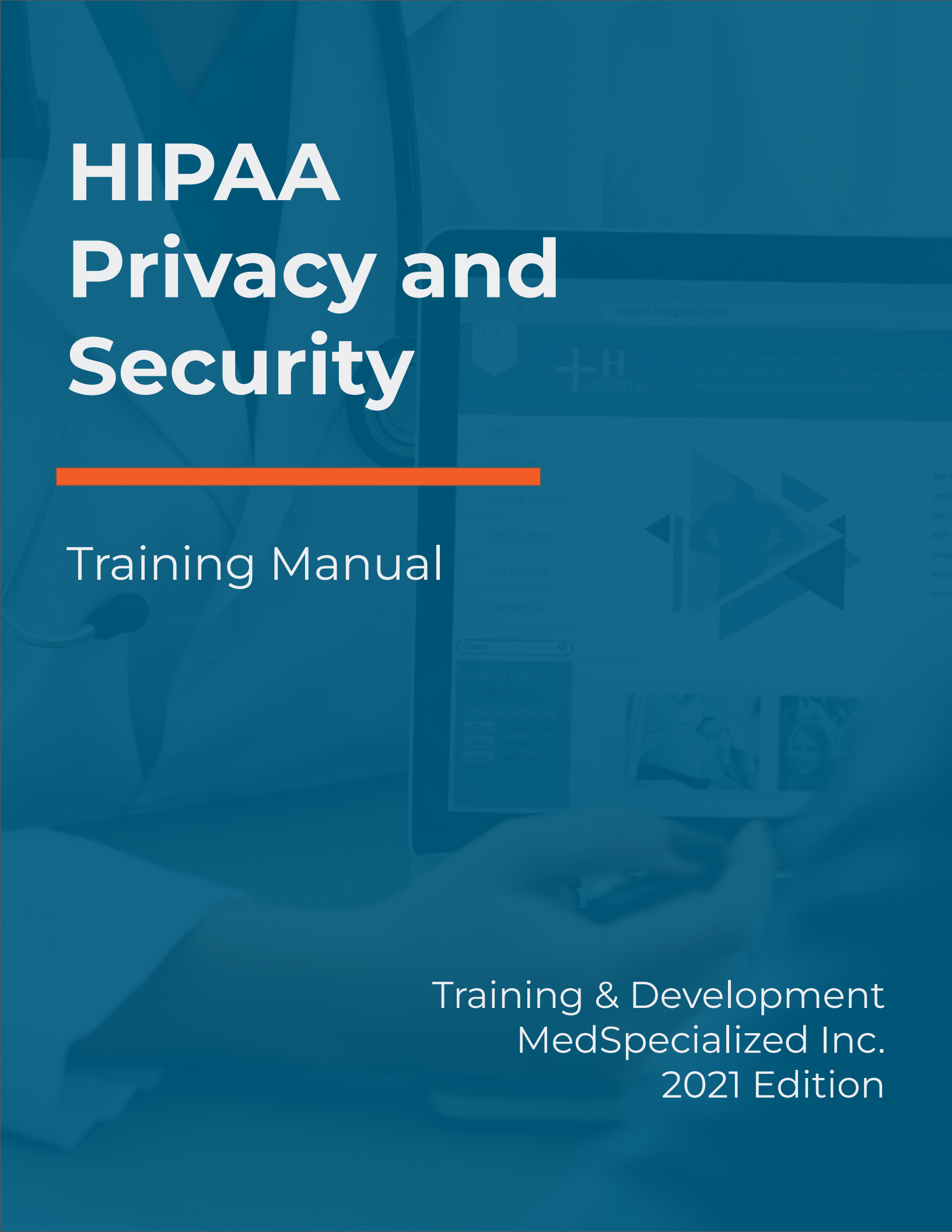
HIPAA Privacy and Security

Training Manual



Training & Development
MedSpecialized Inc.
2021 Edition

HIPAA

Health Insurance Portability and Accountability Act

HIPAA is the federal **Health Insurance Portability and Accountability Act** of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information, and help the healthcare industry control administrative costs.

1996. Enacted by the United States Congress and signed by President Bill Clinton.

2009. Expanded and strengthened by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

2013. The Department of Health and Human Services (HHS) issued the “Final Rule” that implements HITECH’s statutory amendments to HIPAA in January of 2013.

Training

HIPAA: Title I

Health Care Access, Portability, and Renewability

HIPAA Title I is designed to protect the health insurance coverage for workers and their families when they change or lose their jobs.

This provision also prohibits group health plans from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability.

Aside from that, it also forbids individual health plans from denying coverage or imposing pre-existing condition exclusions on individuals who have at least 18 months of creditable coverage without significant breaks.

HIPAA: Title II

Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

HIPAA Title II is requires the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

It also addresses the security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

Five (5) Rules:

- The Privacy Rule
- The Transactions & Code Sets Rules
- The Security Rule
- The Unique Identifiers Rule
- The Enforcement Rule

Training

HIPAA: Title II

The Privacy Rule

The **HIPAA Privacy Rule**, along with the HIPAA Security Rule, form the foundation of the HIPAA regulations. The Privacy Rule explains how and when healthcare professionals, lawyers, or anyone who accesses your PHI can or cannot use that data.

For example: if I want to allow my PHI to be available to someone else, the law requires a signed HIPAA PHI Release form in order for the Doctor's office to share my information with them. Those are the kinds of scenarios covered in the Privacy Rule.

PHI: Protected Health Information

Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present or future physical or mental health or condition, including the health care services provided and payment for those services.

Trainiay

HIPAA: Title II

The Privacy Rule

Examples of PHIs:

- Name
- Postal Address
- All elements of dates (except year)
- Contact information (e.g. email address, phone number, fax number)
- URL & IP addresses
- Social Security Number
- Account numbers
- License numbers
- Medical record number
- Health plan beneficiary number
- Device and vehicle identifiers and serial numbers
- Biometric identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying numbers, codes, or characteristics

HIPAA: Title II

The Privacy Rule

Covered Entity

Any individual, organization or corporation that directly handles Protected Health Information (PHI) or Personal Health Records (PHR) and transmits health information in electronic form.

Examples are hospitals, doctor's offices, health insurance providers, health care clearinghouses, among others.

Business Associate

A person who performs a function or activity on behalf of, or provides services to a covered entity that involves PHI. This may include medical software companies, health IT companies, medical billing companies and medical transcription companies.

Business Associate Contract

An agreement between a covered entity and a business associate. The Privacy Rule requires that the covered entity include certain protections for the health information that their business associates will use or disclose.

Training

HIPAA: Title II

The Privacy Rule

General Principle for Use and Disclosure

A. **Required**. A covered entity must disclose PHI if:

- the individual or their personal representative specifically requests access to these information or when asks for an accounting of disclosures of PHI
- HHS is undertaking compliance investigation or review or enforcement action

B. **Permitted**. A covered entity is permitted, but not required to use and disclose PHI without authorization only on the following purposes or situations:

- To the Individual
- Treatment, Payment, Health Care Operations (e.g. by one or more provider, billing related transaction, referrals, performance evaluations, audits)
- With opportunity to Agree or Object (informal permission by asking the patient outright, if incapacitated or in an emergency situation)

Training

HIPAA: Title II

The Privacy Rule

- Incidental use and disclosure (as long as PHI was limited to the "minimum necessary")
- Public Interest and Benefit Activities (required by law [child abuse, domestic violence], public health activities, victims of abuse/neglect/domestic violence, health oversight activities, judicial and administrative proceedings, law enforcement purposes, decedents, cadaveric organ/eye/tissue donation, research, serious threat to health or safety, essential government functions, worker's compensation)
- Limited Data Set for the purposes of research, public health or health care operations

C. **Authorized**. PHI may be used or disclosed only if:
- the Privacy Rule permits or requires
- the patient or personal representative of the patient authorizes in writing
- PHI of a deceased individual is protected for a period of 50 years following the death of that individual.

HIPAA: Title II

The Privacy Rule

An authorization must:

- be in plain language
- be written in specific terms
- contain specific information regarding the information to be disclosed or used, the persons involved, expiration, right to revoke in writing, and other data

Minimum Necessary Rule

A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

Access to and use of protected health information within a covered entity must be restricted according to the specific roles of the members of the workforce. Therefore, they must develop and implement policies, procedures, and technical safeguards to prevent unauthorized use and disclosure.

HIPAA: Title II

The Security Rule

The **HIPAA Security Rule** applies to all covered entities and business associates who transfer PHI in electronic form. Its major goal is to protect the privacy of the individual's health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

The rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI, specifically:

A. **Ensure confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit**

- **Confidentiality**. Data or information is not made available or disclosed to unauthorized persons or processes.
- **Integrity**. Data or information has not been altered or destroyed in an unauthorized manner.
- **Availability**. Data or information is accessible and usable upon demand only by an authorized person.

Training

HIPAA: Title II

The Security Rule

B. **Identify and protect against reasonably anticipated threats to the security or integrity of the information**

Risk Analysis and Management: an ongoing process; covered entity regularly reviews its records to track access to PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI

C. **Protect against reasonably anticipated, impermissible uses or disclosures**

- **Administrative Safeguards**
  - **Security Management Process/Security Personnel**. Covered entities must establish policies and procedures to prevent, detect, contain, and correct security violations. Part of this process is to follow the procedures in the Risk Management Framework to assess overall risk in your current processes or when you implement new policies.

Training

HIPAA: Title II

The Security Rule

- **Assigned Security Responsibility**. One designated security official must be responsible for the development and implementation of the HIPAA Security Rule.
- **Information Access Management**. Restrict access to ePHI via permissions after you have identified the who should have access in the step above.
- **Workforce Training and Management**. In order to enforce these rules and security policies, organizations need to train their users on what the rules are and how to abide by them.
- **Evaluation**. Establish a process to review and maintain the policies and procedures to stay up to date and current with the HIPAA Security Rule.

Training

HIPAA: Title II

The Security Rule

- **Physical Safeguards**
  - ❖ **Facility Access and Control**. Must limit physical access to its facilities while ensuring that authorized access is allowed.
  - ❖ **Workstation and Device Security**. Implement policies and procedures to specify proper use of and access to workstations and electronic media.
- **Technical Safeguards**
  - ❖ **Access Control**. Authenticate users as necessary to access ePHI, establish and maintain a least privilege model, and have appropriate procedures in place to audit access control lists (ACL) on a regular schedule.
  - ❖ **Audit Control**. Implement hardware, software, and/or procedural mechanisms to record and examine access and other activities related to PHI.

Training

HIPAA: Title II

The Security Rule

- **Integrity Control**. Covered entities need to be able to prove that the ePHI they manage is protected from threats both inside and out, intentional or not.
- **Transmission Security**. When sending data to other business partners, you need to be able to prove that only authorized individuals accessed the ePHI.

B. **Ensure compliance by the workforce**

- **Covered Entity Responsibilities**. Must take reasonable steps to cure the breach or end the violation

HIPAA and the Use of Encryption

Encryption is the process of turning readable text to an unreadable encrypted text that can only be converted back to the original message if a decryption key (from the sender) is obtained. Refer to the diagram below:

HIPAA: Title II

The Security Rule

According to HIPAA's Security Rule, encryption is NOT required, but only addressable. This means that the entity is responsible for doing the necessary analysis to determine if encryption is really needed or not.

- **Data at Rest**. Information is NOT crossing over to the internet. Encryption is ADDRESSABLE.
- **Data in Transit**. Information is crossing over to the internet. Encryption is REQUIRED when sensitive information such as PHI is involved.

When encryption is not necessary according to the analysis done, the presence of alternate protection such as two-factor authentication and malware programs are enough.

HIPAA views email communication as inherently not secure because data crosses over the internet, which makes PHI vulnerable to cyber criminals. However, HIPAA allows PHI to be sent via email provided that it is adequately protected.

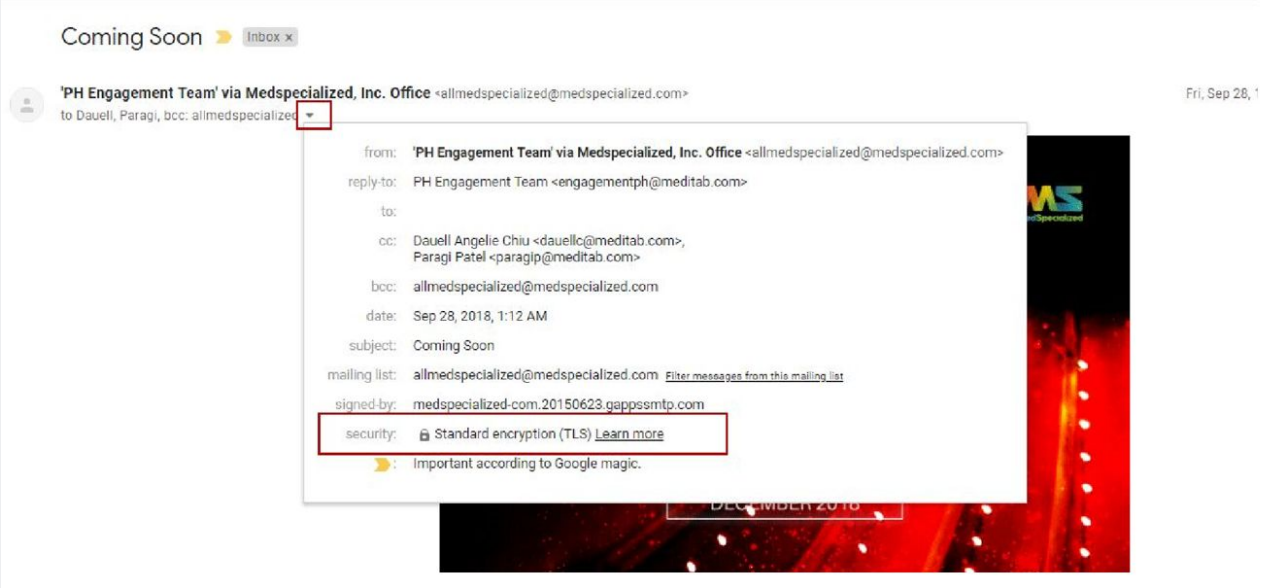
Training

HIPAA: Title II

The Security Rule

The company addresses by implementing these safeguards:

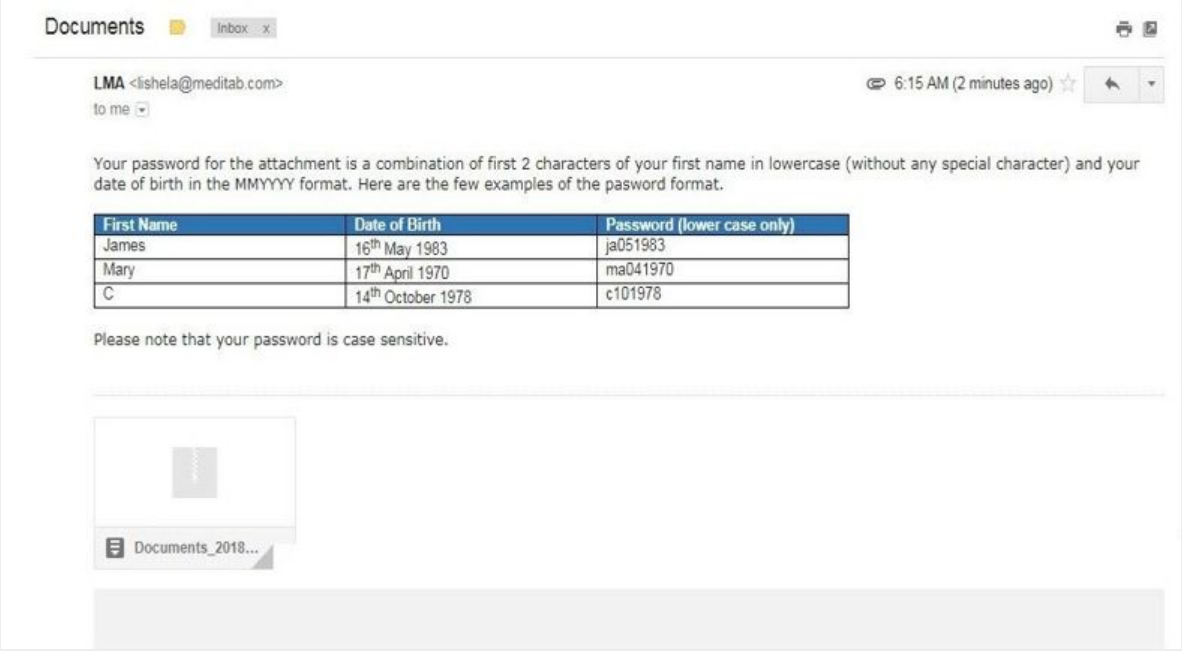
- **Standard encryption (TLS) done by Google**. The company signed a contract with Google wherein Google encrypts all emails sent using our corporate Gmail accounts when it is in transit only. The emails are then automatically decrypted once they have arrived at the recipient's inbox.



HIPAA: Title II

The Security Rule

- **End-to-end encryption**. If Google only encrypts the emails while in transit only, end-to-end encryption means that the file is encrypted when it is in transit and would still be encrypted after it has arrived in the inbox of the recipient. This means that the decryption process is no longer automatic and that the recipient would need a decryption key from the sender to decrypt the file.

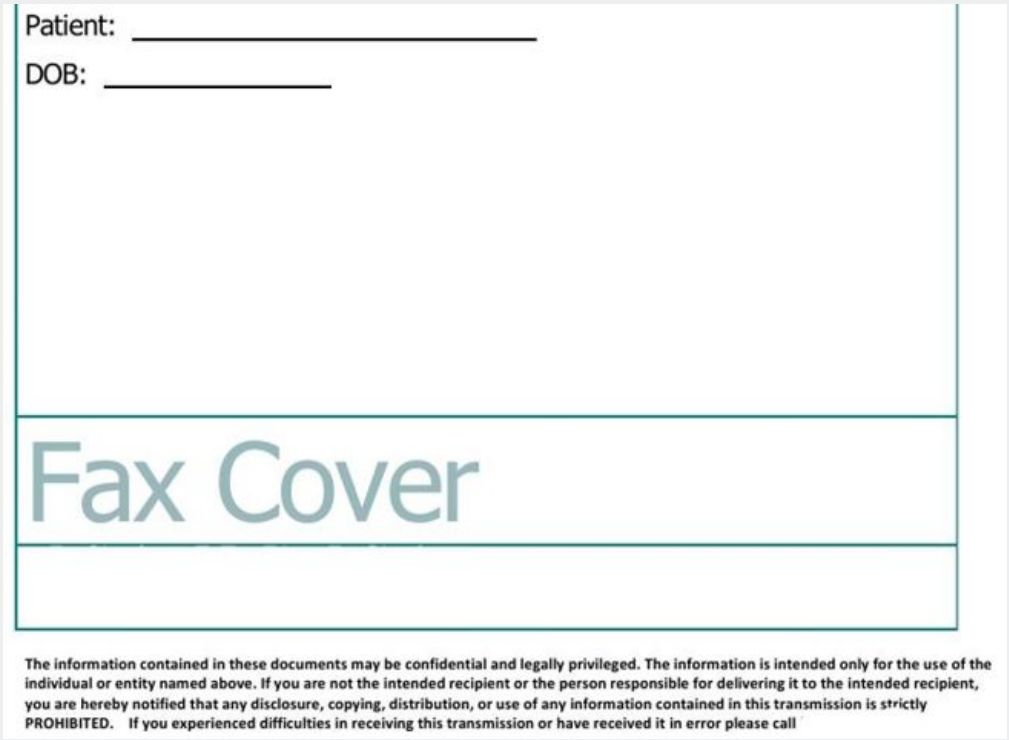


Training

HIPAA: Title II

The Security Rule

- **HIPAA and Faxes Sent to Wrong Numbers**. According to HIPAA, in order to address situations wherein faxes with PHI are sent to the wrong number, a fax cover sheet that highlights the confidentiality of the incoming file should be attached at the beginning of the fax. The fax cover sheet must state that the file contains confidential information and should only be viewed by the intended recipient only.


Patient: _____

DOB: _____

Fax Cover

The information contained in these documents may be confidential and legally privileged. The information is intended only for the use of the individual or entity named above. If you are not the intended recipient or the person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of any information contained in this transmission is strictly PROHIBITED. If you experienced difficulties in receiving this transmission or have received it in error please call

HIPAA

Breach

Breach is the loss of control, compromise, unauthorized disclosure, acquisition, access or any situations where people other than the authorized users have access or potential access to personally identifiable information, whether physical or electronic.

How to Report Breaches

Part of your responsibility as a Medspecialized employee is to report privacy and security breaches involving PHI to the Human Resource Department (relationshr@meditab.com).

Penalties

A. **Civil Penalties**

- **Unknowing**
  Penalty range: $100 - $50,000 per violation, with an annual maximum of $25,000 for repeat violations
- **Reasonable Cause**
  Penalty range: $1,000 - $50,000 per violation, with an annual maximum of $100,000 for repeat violations

Training

HIPAA

Breach

- **Willful neglect but violation is corrected within the required time period**
  Penalty range: $10,000 - $50,000 per violation, with an annual maximum of $250,000 for repeat violations
- **Willful neglect and is not corrected within required time period**
  Penalty range: $50,000 per violation, with an annual maximum of $1.5 million

B. **Criminal Penalties**

- **$50,000 and up to one-year imprisonment**. Knowingly obtains or discloses PHI.
- **$100,000 and up to five years imprisonment**. Involves false pretenses.
- **$250,000 and up to ten years imprisonment**. Involves intent to sell, transfer, or use PHI to commercial advantage, personal gain or malicious harm.

HIPAA

MedSpecialized Corrective and Disciplinary Actions

- **Loss of privileges and/or termination of employment**. Management's decision will depend on the degree of violation. This may range from issuance of warning, suspension, and may even result to termination.
- Medspecialized may also resort to **legal actions** against the employee for damage to company under the Philippine law.

Training

HIPAA

Compliance & Data Protection with Google Apps

Google rolled out a guide that helps Google Apps users comply with HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health).

The guide is intended for the following:

- Security officers
- Compliance officers
- IT administrators
- And other employees in organizations who are responsible for HIPAA implementation and compliance with Google Apps

Under HIPAA, certain information about a person's health or health care services is classified as Protected Health Information (PHI). It is therefore important to organize data on Google services when handling PHI to comply with HIPAA.

Training

HIPAA

Compliance & Data Protection with Google Apps

Google Apps Customers who are subject to HIPAA and wish to use Google Apps with PHI must sign a Business Associate Agreement (BAA) with Google. Under this agreement, PHI is allowed only in a subset of Google Services called “included functionality”.

These services must be configured by IT and is categorized into three:

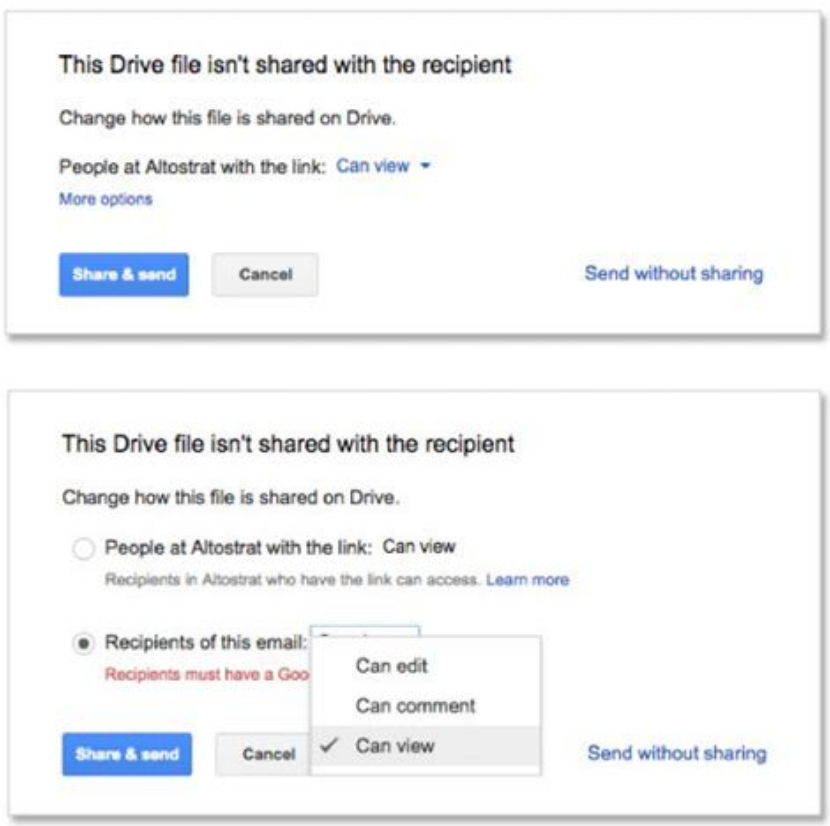
- **HIPAA Included Functionality** which all users can access. This includes Gmail, Google Drive, Google Calendar, Google Sites, and Google Apps Vault.
- **Core Services** where PHI is not permitted. Google Apps administrators can choose to turn off Hangouts, Contacts and Groups.
- Other **Non-Core Services** offered by Google where PHI is not permitted, such as Google+, YouTube, Blogger and Picasa Web Albums.

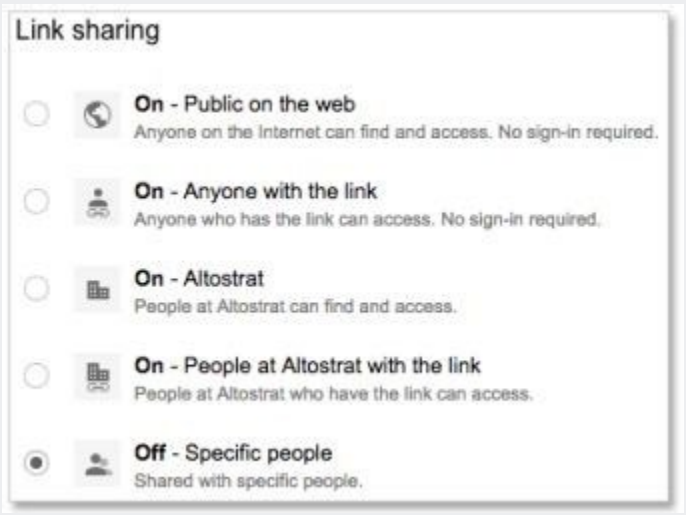
The admin has the ability to set up restrictions in Google Apps Core Services in the sharing of PHI.

Trainiay

HIPAA

Compliance & Data Protection with Google Apps

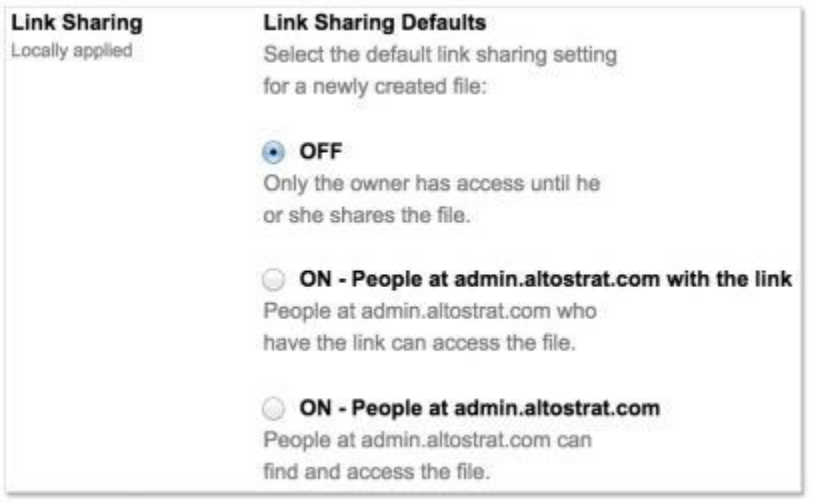




Training

HIPAA

Compliance & Data Protection with Google Apps



The Google Apps administrator can also set up specific user access within the organization based on whether the users handle PHI or not. This can be done by placing users into groups.

To keep data safe and secure, several security practices are recommended including the following:

- Set up 2-step verification to reduce the risk of unauthorized access in case a user's password is compromised.

Training

HIPAA

Compliance & Data Protection with Google Apps

- Configure enterprise sender identity technologies — sender policy framework, DomainKeys Identified Mail, and Domain-Based Message Authentication to — prevent spammers and phishers from “spoofing” your domain.

Also, it is the customer’s responsibility to ensure that appropriate HIPAA-compliant measures are in place with any third party (or third party application) before sharing or transmitting PHI.

A list of security and privacy controls available with Google Apps can be found on our Security and Privacy website.

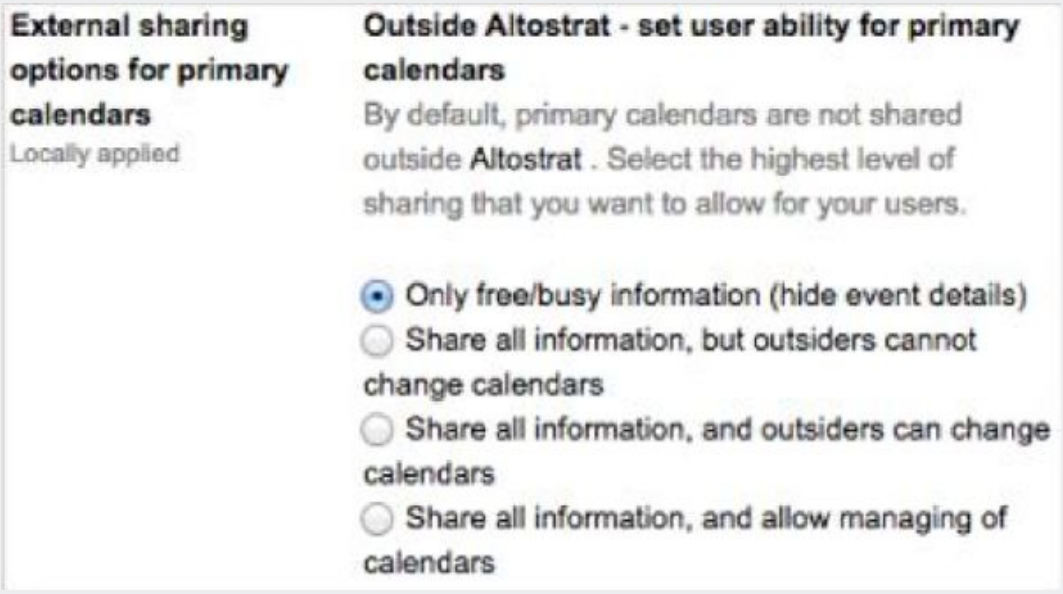
These additional resources may help you understand how Google services are designed with privacy, confidentiality, integrity, and availability of data in mind.

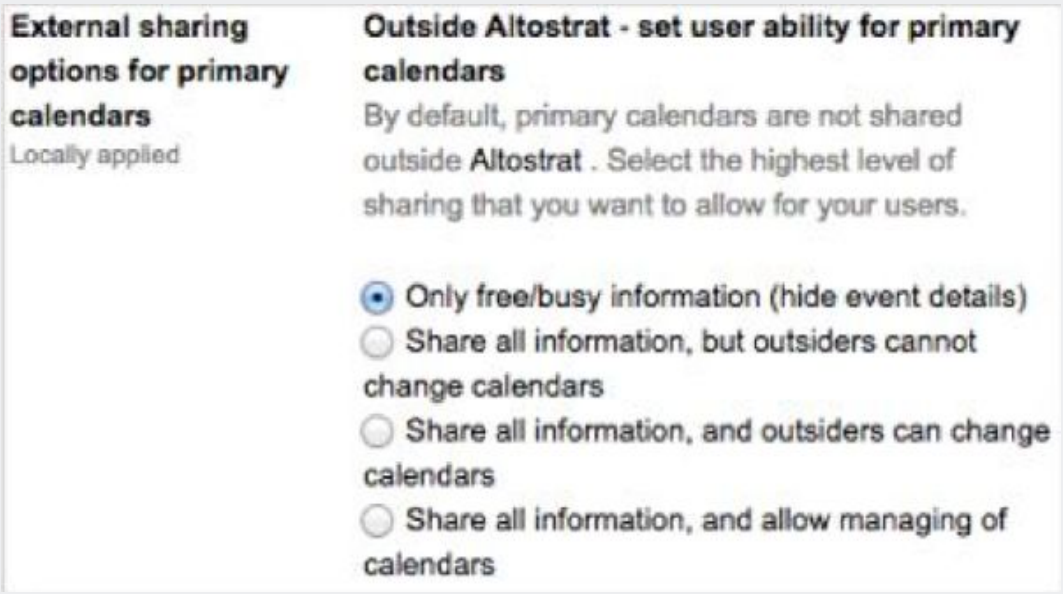
- Google Apps Help Center
- Google for Work security page
- HIPAA Compliance with Google Apps

Training

HIPAA

Compliance & Data Protection with Google Apps





Training

HIPAA

Compliance & Data Protection with Google Apps

Employees should consider setting sharing permissions appropriately, if inserting a
Google Calendar or content stored in Google Drive (including Docs, Sheets, Slides, and Forms) into a site. Administrators should consider setting the default visibility for sites to “Private”.

Training

HIPAA

How to be HIPAA compliant

As a MedSpecialized employee, what should you do to be HIPAA compliant?

- Always lock your computer every time you leave your station even if for a short while.
- Log out of computer systems after use.
- Avoid writing patient information on a piece of paper or sticky note. Any written information should be destroyed after intended use.
- Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites) and work areas. Do not access sites, such as Facebook, Twitter, etc., when accessing a client's computer remotely.
- Limit accidental disclosures. Do not talk about a patient's health information outside of the office or to any colleague or individual not directly related to the client's case.
- Access information only as necessary for your authorized job responsibilities.
- Passwords and access codes should never be shared to anyone.

Training

HIPAA

How to be HIPAA compliant

- Avoid using the same password in multiple programs or applications.
- Do not open email or click on embedded links from an unknown or untrusted site.
- Be doubtful of emails asking you to disclose passwords, name, and other sensitive information. Should you receive this kind of email, do not open it and discard it right away.
- Nowadays, many harmful websites already have security certification, so just relying on signs of a secured website may be problematic. The best way would be to verify any links, especially suspicious ones or those that came from emails you are not expecting.
- Do not open email attachments if the message looks suspicious, even if you recognize the sender. When in doubt, throw it out.
- Do not respond to “spam”. Simply discard or delete it, even if it has an “unsubscribe” feature.
- Do not forward messages containing PHI from your

HIPAA

How to be HIPAA compliant

company email to your personal email or to anyone for that matter.

- When sending an email, do not include PHI or other sensitive information such as Social Security numbers, unless you have proper written approval to store the information and use encryption.
- Be careful when sending email blasts. Know when to use CC and BCC. When sending emails containing PHI, limit it only to people who are directly related to the task or case. Do not CC or BCC everyone.
- Do not browse non-work-related sites. If the computer or mobile device you are using stores work-related sensitive information, personal use of the web is not recommended.
- Avoid video streaming. Streaming media websites might seem harmless, but watching or listening to streaming media may require downloading a special media player that may contain malware.
- Do not download programs, software, and other media using a work PC. If it is needed, have the IT guy assist you.

Training

HIPAA

How to be HIPAA compliant

- Using file sharing programs is prohibited as these frequently contain spyware and are used to share files that contain malware. Some may also expose sensitive information to unauthorized individuals if not configured correctly. Examples of P2P (Peer to peer) or file sharing programs are Limewire, BitTorrent, Ares, BearShare, eMule, among others.
- Encryption is required when you are accessing your company email or a client's computer remotely using your mobile phone, device, or laptop.
- When transmitting or accessing PHI on mobile devices (laptop, tablets, mobile phone), you must utilize the following security controls:
  - ❖ strong power-on password
  - ❖ automatic log-off
  - ❖ display screen lock at regular intervals while the device is inactive
  - ❖ encryption
- Never leave mobile devices unattended in unsecured areas. Remember, for any mobile device, encryption is the best defense.

Training

HIPAA

How to be HIPAA compliant

- Avoid storing sensitive information on mobile devices and portable media, but if you must, you must use encryption.
- Always keep portable devices physically secure to prevent theft and unauthorized access. Immediately report the loss or theft of any mobile computing device to your supervisor and the HR department.
- In a work-from-home setup, when you need to connect to a client's server, it must be done through the office's network.

HIPAA & COVID-19

Guidance on Disclosing Information about COVID-19 Patients to First Responders

The Office for Civil Rights (OCR) highlights several existing HIPAA provisions that allow healthcare providers to share PHI with emergency responders, law enforcement, and others in the context of COVID-19 **without** the authorization of the patient.

OCR reviews many of the provisions covered in its previous guidance document, but includes new examples of how these provision apply to COVID-19.

- PHI can be shared **when disclosure is needed to provide treatment**. For example, a nursing home can disclose health information about a resident who has COVID-19 so that emergency responders can provide treatment while transporting the resident to a hospital.
- PHI can be shared **when law enforcement or first responders may be at risk of infection**. OCR's examples include:
    - A county health department disclosing PHI to a police officer or other person who may come into

HIPAA & COVID-19

Guidance on Disclosing Information about COVID-19 Patients to First Responders

contact with a person who tested positive for COVID-19, and
    - A hospital providing a list of names and addresses of all individuals it knows to have tested positive, or received treatment, for COVID-19 to an EMS dispatch for use on a per-call basis.
- PHI can be shared **when necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public**. OCR indicates that PHI can be disclosed about patients who have tested positive for COVID-19 to fire department personnel, child welfare workers, mental health crisis services personnel, or others charged with protecting the health or safety of the public if the healthcare provider believes in good faith that the disclosure is necessary to prevent or lessen a serious and imminent threat to such individuals.

HIPAA gives healthcare providers leeway to make certain types of disclosures related to COVID-19 without the

HIPAA & COVID-19

Guidance on Disclosing Information about COVID-19 Patients to First Responders

patient's authorization, especially when it comes to protecting the health and safety of first responders.

At the same time, patient privacy should remain a priority and disclosures should be limited to the **minimum necessary** amount of information to accomplish the purpose of the disclosure.

HIPAA & COVID-19

HIPAA Compliance During the COVID-19 Pandemic

As the COVID-19 pandemic spreads throughout the world, more and more companies are asking their employees to work from home in light of new government-issued regulations and for their own well-being. This unprecedented health crisis has meant that many sectors have had to adapt to the new conditions and embrace remote work despite past misgivings.

HIPAA requirements relaxed for virtual healthcare

In response to the ongoing COVID-19 pandemic, the HHS recognized the need for healthcare providers to communicate and provide health services to patients virtually through remote communication technologies. This was not previously fully compliant with HIPAA Rules, but the HHS has announced that they are now permitted in response to current circumstances.

HIPAA requirements are still mandatory

While some rules have been relaxed due to the current emergency, it's worth noting that HIPAA requirements have not been waived.

Training

HIPAA & COVID-19

HIPAA Compliance During the COVID-19 Pandemic

This means that although healthcare organizations may have greater leeway in the tools, they use to continue conducting their business, the sensitive health data they collect, store, and process, must still be protected.

The HHS states that in an emergency situation, organizations falling under the scope of HIPAA must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. They must also apply the administrative, physical, and technical safeguards detailed in the HIPAA Security Rule.

Protecting health data while working remotely

Once healthcare providers decide to implement remote work plans, it is essential for them to ensure that health data will be protected even when it is taken outside the security of company networks. This starts from the devices employees will be using remotely: they must be encrypted, password-protected, and have updated firewalls and antivirus software installed.

Training

HIPAA & COVID-19

HIPAA Compliance During the COVID-19 Pandemic

Virtual Private Networks (VPNs) should be used to access the company network remotely. Employees should be required to disconnect at the end of each workday to ensure their computers don't stay connected longer than necessary to the company network.

Companies should use solutions like Data Loss Prevention (DLP) tools to ensure that health data cannot be copied to any external devices not approved by the organization. In this way, potential malicious devices cannot be connected to a computer, and data at rest cannot be stolen or stored in a way that is not HIPAA compliant.

Physical protection of files

Working from home may also mean that employees can print information or receive health information through the mail. It is essential, therefore, that they store it in a secure place, whether it's in a locked cabinet or a home office that no one other than themselves has access to.

Training

HIPAA & COVID-19

HIPAA Compliance During the COVID-19 Pandemic

When they are no longer needed for the original purpose they were collected for, physical files should be shredded or otherwise destroyed.

It is also important that employees work in a private space where no one can see or hear the information they are transmitting or working on. No other individuals, except the employees themselves, should be allowed to access computers on which protected health information is stored.

Monitoring and logging health information

Lastly, health data should be monitored at all times to ensure compliance and to help companies spot any risky practices their employees might be tempted to use while working from home. Logging the movements of health information is also a way for organizations to prove compliance in case the OCR requires it.


www.h.hospital.com
HOSPITAL
Home
About Us
Find a Doctor
Our Centers
Contact Us
Search
Hotline Center
Online Services

END