HIPAA COMPLIANCE FOR REMOTE WORKERS

PRESENTED BY
PAUL R. HALES, J.D.

Welcome!

August 17, 2022

HIPAA Compliance for Remote Workers

PAUL R. HALES
ATTORNEY AT LAW

Health Information – HIPAA

The HIPAA E-Tool®

Protecting Patient Privacy is Our Job®

Legal Education – Not Legal Advice

AttorneyHales.com @hipaaetool 314-534-3534

Paul.Hales@AttorneyHales.com

HALESLAWGROUP HEALTH INFORMATION PRIVACY

HIPAA Compliance for Remote Workers

Who Must Comply With HIPAA?

Covered Entity

Health Care Provider – Health Plan – Health Care Clearinghouse

Business Associate

On behalf of a Covered Entity

- Creates, Receives, Maintains or Transmits Protected Health Information (PHI) for a function or activity regulated by the HIPAA Rules
- Provides Services involving disclosure of PHI from a Covered Entity or from another Business Associate

Subcontractor Business Associate

On behalf of a Business Associate

- Creates, Receives, Maintains or Transmits PHI for function or activity regulated by the HIPAA Rules

HIPAA Compliance for Remote Workers

What Are We Going to Cover?

- Impact of the Pandemic
- Remote Work – the New Normal
- Why Protecting PHI Privacy is Essential
- HIPAA Rules and Remote Work Protocols
  - Privacy
  - Security
  - Breach Notification
- Remote Work Guidelines
- Conclusion, Discussion, Questions, Comments

HIPAA Compliance for Remote Workers

PANDEMIC!

SUDDENLY ALMOST EVERYONE IS WORKING FROM HOME

HIPAA Compliance for Remote Workers

HIPAA Compliance for Remote Workers

HIPAA Compliance for Remote Workers

Safety – Every aircraft has Checklists

HIPAA Compliance for Remote Workers

REMOTE WORK – THE NEW NORMAL

REMOTE AND HYBRID WORKFORCE SOLUTIONS

HIPAA Compliance for Remote Workers

HIPAA Rules – Compliance Checklists for *Every* Workplace

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

AT EVERY WORKPLACE

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

Cyber criminals are selling the information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

https://oig.hhs.gov/fraud/consumer-alerts/medical-identity-theft/

Medical Identity Theft

What is Medical Identity Theft?

Medical identity theft is when someone steals or uses your personal information (like your name, Social Security number, or Medicare number), to submit fraudulent claims to Medicare and other health insurers without your authorization. You should protect your personal information, check medical bills and statements, and report questionable charges or fraud.

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

PHI = The GOLD Standard

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

HHS OIG Medical Identity Theft Video

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

HHS OIG Medical Identity Theft Video

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

Medical Identity Theft is the fastest growing form of Identity Theft

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

Only two things are needed for Medical Identity Theft:
Identity of a Patient – Identity of a Provider

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

I got a call one evening – I gave him my Medicare Number and my Debit Card Number

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

Criminals Attack People of All Ages & All Walks of Life

- Social Engineering
  Clever Scripts & Messages
- Coronavirus Scams
- Vishing
- Phishing
- Smishing
- Email – Cell Phone Number Harvesting

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Criminal Black Market

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

Medical Identity Theft – Patient Safety

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

EQUIFAX DATA BREACH

September 7, 2017

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

September 9, 2017

Equifax data breach could create lifelong identity theft threat

September 17, 2017

Key Equifax executives departing after huge data breach

September 26, 2017

Equifax dumps CEO in wake of damaging data breach

HIPAA Compliance for Remote Workers

Why Protecting PHI Privacy is Essential

EQUIFAX DATA BREACH

Equifax Breach Caused by *Lone Employee's Error* Former CEO Says

The company said unpatched software had been to blame
but Mr. Smith went further, describing how
"human error and technology failures"
turned a single oversight into a data breach
allowing attackers to obtain personal details
on nearly half of America's population

HIPAA Compliance for Remote Workers

HIPAA Rules and Remote Work Protocols

Privacy – Security – Breach Notification

HIPAA Rules are the basis for Remote Work Checklists

HIPAA Compliance for Remote Workers

HIPAA Rules

Are Easy to Follow

Step-by-Step

When You Know the Steps

HIPAA Compliance for Remote Workers

HIPAA Rules

Are a Blueprint

To Protect

Your Organization

HIPAA Compliance for Remote Workers

HIPAA for Remote Workers

Is about Fundamentals

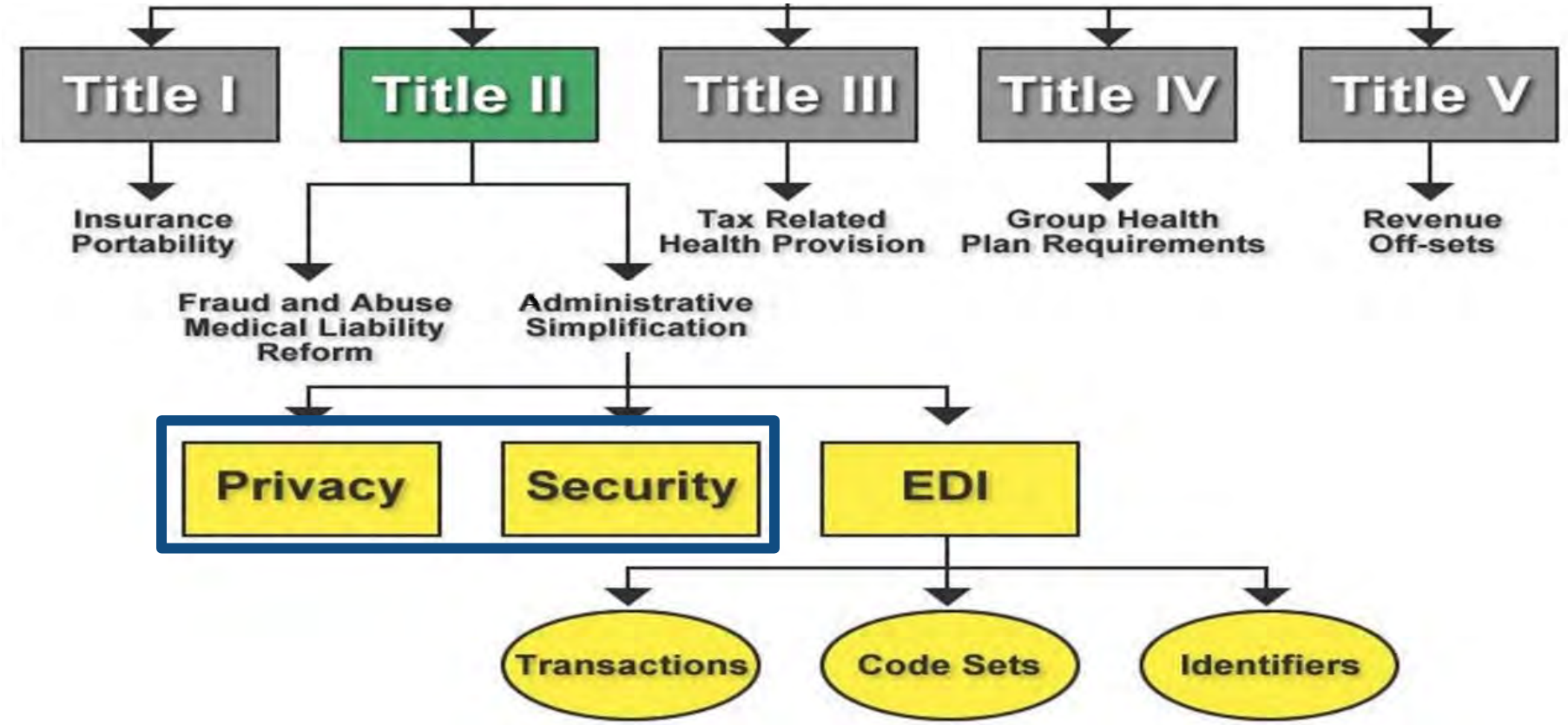
Policies – Procedures – Training

Risk Analysis and Risk Management

HIPAA Compliance for Remote Workers

HIPAA Rules

Health Insurance Portability and Accountability Act of 1996



HIPAA Compliance for Remote Workers

HIPAA Rules

Health Insurance Portability and Accountability Act of 1996

Privacy Rule – Security Rule – Enforcement Rule

Health Information Technology for Economic and Clinical Health Act

HITECH Act

Breach Notification Rule

HIPAA and HITECH apply to Covered Entities and Business Associates of all sizes that handle PHI

The HIPAA Rules are flexible – to be achievable by all types and sizes of Covered Entities and Business Associates

– designed to guide – not prescribe precise compliance

HIPAA Compliance for Remote Workers

HIPAA Rules

Health Insurance Portability and Accountability Act of 1996

Telephone Consumer Protection Act of 1991

1991 TCPA

Subject: Telecommunications Sent Automatically – Landline, Fax, Cell, Text
by Automatic Telephone Dialing System (ATDS) – "Autodialer" ***1991 Technology***

Purpose: **Protect Consumers from Nuisance & Invasion of Privacy**

Exception – "Safe Harbor" – Consumer's **Prior Express Consent**

Enforcement: FCC, State Attorneys General, Civil Fines, **Private Lawsuits**

2019 TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act)

2021 FCC Regulation

addresses prior consent exemption for certain healthcare-related calls to a wireless number given by a patient to a healthcare provider

Exempted calls may not include accounting, billing or debt-collection content and must comply with HIPAA Privacy Rules

HIPAA Compliance for Remote Workers

HIPAA Rules

Health Insurance Portability and Accountability Act of 1996

Telephone Consumer Protection Act of 1991

"Healthcare Provider Exemption"

Voice and Text Messages by or on behalf of Healthcare Provider to a Wireless Number must comply with HIPAA privacy rules

HIPAA Privacy & Security Rules – 3 Steps – Unencrypted Text Messages

"**Duty to Warn**"

Warning – Agreement – Documentation

Documents **Prior Express Consent** *in writing*

TCPA "Safe Harbor"

HIPAA Compliance for Remote Workers

HIPAA Rules

Privacy Rule – the Fundamental Rule – All PHI

- Administrative Requirements
- Uses and Disclosures of Protected Health Information (PHI)
- PHI Privacy Rights of an Individual

Security Rule – ePHI – PHI transmitted or maintained Electronically

- Administrative, Physical and Technical Safeguards to prevent Uses and Disclosures of ePHI that violate the **Privacy Rule**

Breach Notification Rule

- Defines "Breach" – Access, Acquisition, Use or Disclosure of PHI that violate the **Privacy Rule**
- Steps to identify a Breach
- Steps to make Required Notifications of a Breach

HIPAA Compliance for Remote Workers

HIPAA Rules

Privacy Rule – the Fundamental Rule – All PHI

- Requires appropriate Administrative, Technical, and Physical safeguards to protect the privacy of PHI – flexible – achievable – not precise

  Examples of specified safeguards:

  - Written Policies and Procedures – specific to entity's PHI activities
  - Training – specific to staff member's PHI-related work
  - Sanctions – discipline for violating Policy or Procedure

  Example from OCR Enforcement

  - Lincare Inc. judgment – in-home health services – no Policies and Procedures to protect PHI removed from office – paper records
    - Lincare *office* procedure – PHI in secure filing cabinets

HIPAA Compliance for Remote Workers

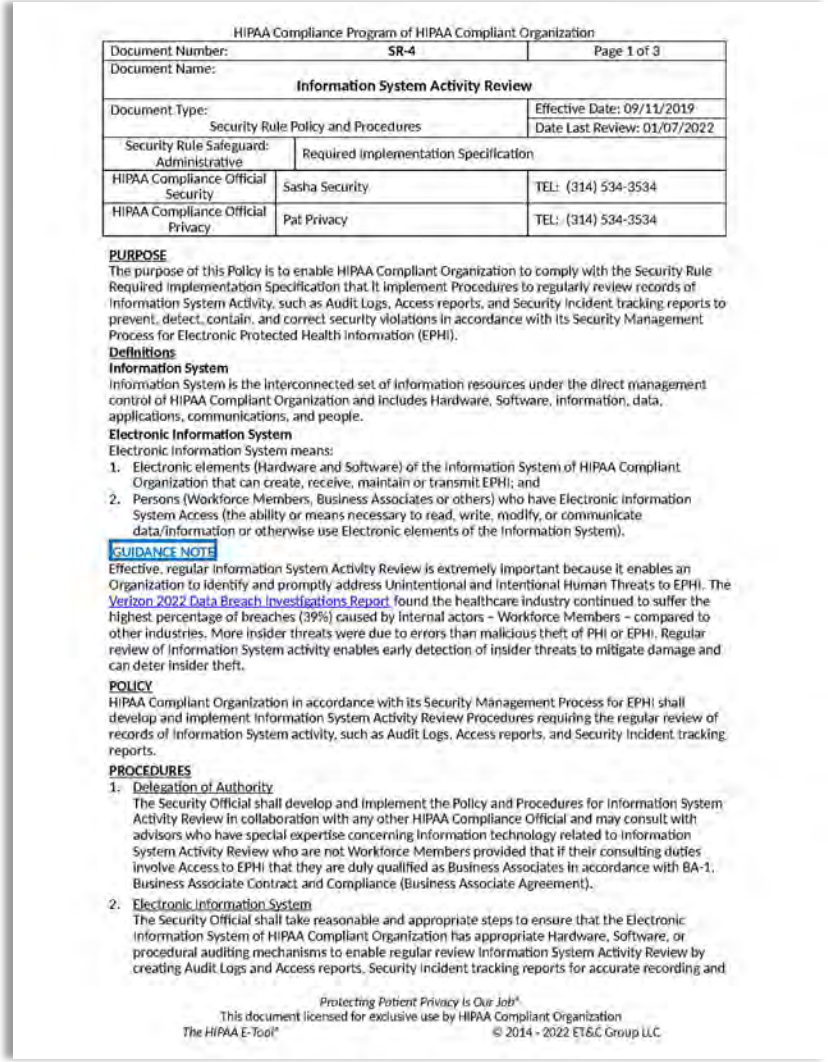
HIPAA Rules

Security Rule – ePHI – PHI transmitted or maintained Electronically

- Security Rule Standards and Implementation Specifications
  Written Policies and Procedures
  - Administrative Safeguards
    Example
    - Information System Activity Review
  - Physical Safeguards
    Examples
    - Device and Media Controls – BYOD Policy
  - Technical Safeguards
    Example
    - Access Control

HIPAA Compliance for Remote Workers

Information System Activity Review Policy and Procedures



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: SR-4		Page 1 of 3
Document Name: **Information System Activity Review**		
Document Type: Security Rule Policy and Procedures		Effective Date: 09/11/2019 Date Last Review: 01/07/2022
Security Rule Safeguard: Administrative	Required Implementation Specification	
HIPAA Compliance Official Security	Sasha Security	TEL: (314) 534-3534
HIPAA Compliance Official Privacy	Pat Privacy	TEL: (314) 534-3534

PURPOSE
The purpose of this Policy is to enable HIPAA Compliant Organization to comply with the Security Rule Required Implementation Specification that it implement Procedures to regularly review records of Information System Activity, such as Audit Logs, Access reports, and Security Incident tracking reports to prevent, detect, contain, and correct security violations in accordance with its Security Management Process for Electronic Protected Health Information (EPHI).

Definitions

Information System
Information System is the interconnected set of information resources under the direct management control of HIPAA Compliant Organization and includes Hardware, Software, information, data, applications, communications, and people.

Electronic Information System
Electronic Information System means:
1. Electronic elements (Hardware and Software) of the Information System of HIPAA Compliant Organization that can create, receive, maintain or transmit EPHI; and
2. Persons (Workforce Members, Business Associates or others) who have Electronic Information System Access (the ability or means necessary to read, write, modify, or communicate data/information or otherwise use Electronic elements of the Information System).

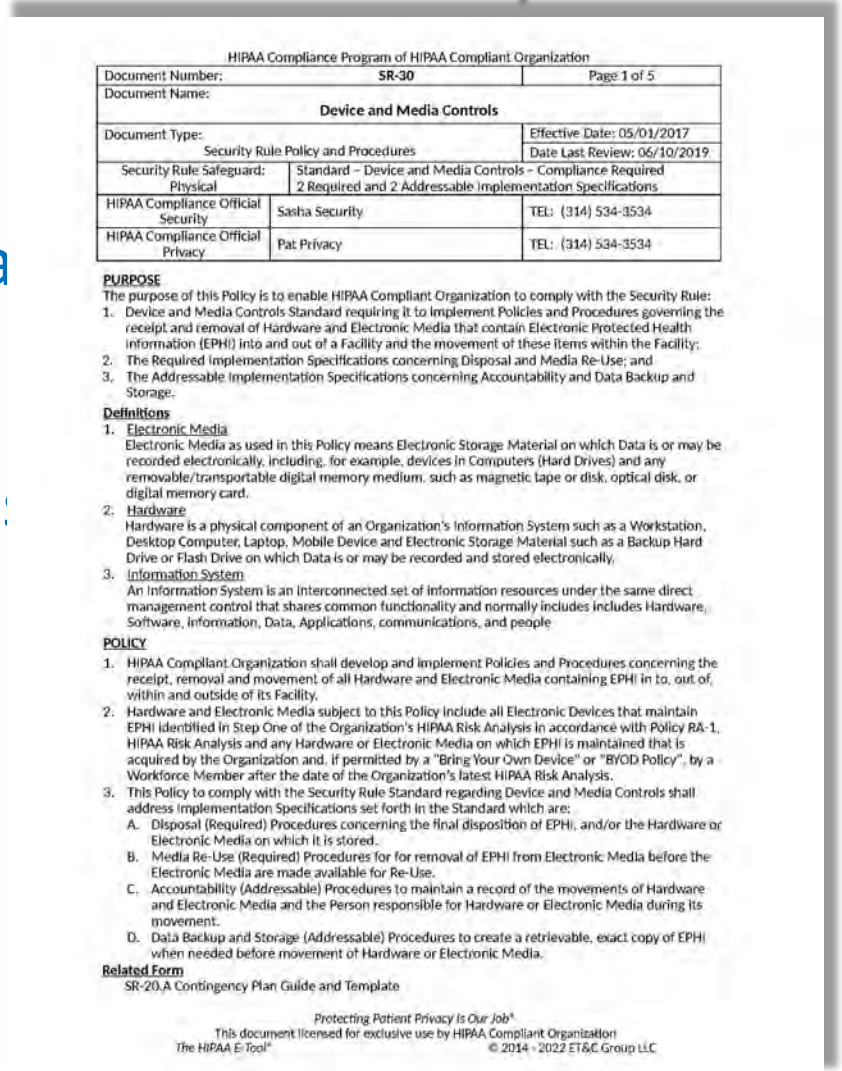
GUIDANCE NOTE
Effective, regular Information System Activity Review is extremely important because it enables an Organization to identify and promptly address Unintentional and Intentional Human Threats to EPHI. The Verizon 2022 Data Breach Investigations Report found the healthcare industry continued to suffer the highest percentage of breaches (39%) caused by internal actors – Workforce Members – compared to other industries. More insider threats were due to errors than malicious theft of PHI or EPHI. Regular review of Information System activity enables early detection of insider threats to mitigate damage and can deter insider theft.

POLICY
HIPAA Compliant Organization in accordance with its Security Management Process for EPHI shall develop and implement Information System Activity Review Procedures requiring the regular review of records of Information System activity, such as Audit Logs, Access reports, and Security Incident tracking reports.

PROCEDURES
1. Delegation of Authority
   The Security Official shall develop and implement the Policy and Procedures for Information System Activity Review in collaboration with any other HIPAA Compliance Official and may consult with advisors who have special expertise concerning Information technology related to Information System Activity Review who are not Workforce Members provided that if their consulting duties involve Access to EPHI that they are duly qualified as Business Associates in accordance with BA-1. Business Associate Contract and Compliance (Business Associate Agreement).
2. Electronic Information System
   The Security Official shall take reasonable and appropriate steps to ensure that the Electronic Information System of HIPAA Compliant Organization has appropriate Hardware, Software, or procedural auditing mechanisms to enable regular review Information System Activity Review by creating Audit Logs and Access reports. Security Incident tracking reports for accurate recording and

HIPAA Compliance for Remote Workers

Device and Media Controls Policy and Procedure



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: SR-30		Page 1 of 5
Document Name: Device and Media Controls		
Document Type: Security Rule Policy and Procedures		Effective Date: 05/01/2017 Date Last Review: 06/10/2019
Security Rule Safeguard: Physical	Standard – Device and Media Controls – Compliance Required 2 Required and 2 Addressable Implementation Specifications	
HIPAA Compliance Official Security	Sasha Security	TEL: (314) 534-3534
HIPAA Compliance Official Privacy	Pat Privacy	TEL: (314) 534-3534

PURPOSE

The purpose of this Policy is to enable HIPAA Compliant Organization to comply with the Security Rule:

1. Device and Media Controls Standard requiring it to implement Policies and Procedures governing the receipt and removal of Hardware and Electronic Media that contain Electronic Protected Health Information (EPHI) into and out of a Facility and the movement of these items within the Facility;
2. The Required Implementation Specifications concerning Disposal and Media Re-Use; and
3. The Addressable Implementation Specifications concerning Accountability and Data Backup and Storage.

Definitions

1. Electronic Media
   Electronic Media as used in this Policy means Electronic Storage Material on which Data is or may be recorded electronically, including, for example, devices in Computers (Hard Drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
2. Hardware
   Hardware is a physical component of an Organization's Information System such as a Workstation, Desktop Computer, Laptop, Mobile Device and Electronic Storage Material such as a Backup Hard Drive or Flash Drive on which Data is or may be recorded and stored electronically.
3. Information System
   An Information System is an interconnected set of information resources under the same direct management control that shares common functionality and normally includes includes Hardware, Software, Information, Data, Applications, communications, and people

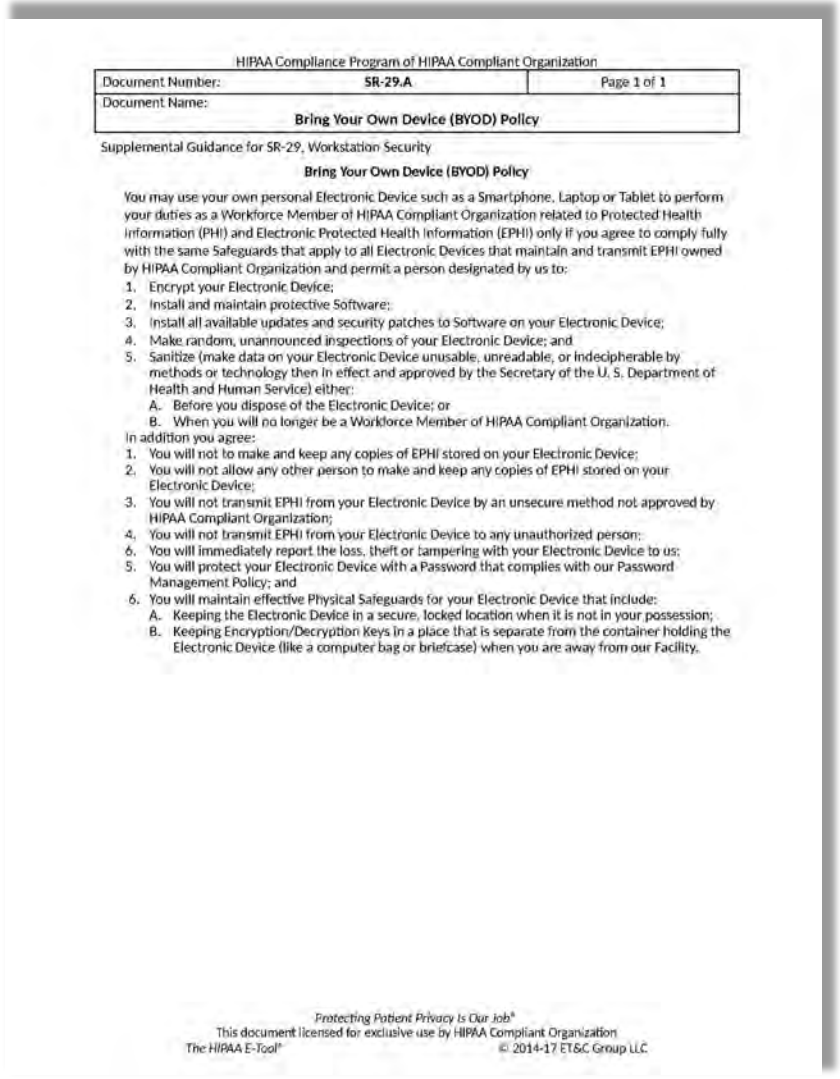
POLICY

1. HIPAA Compliant Organization shall develop and implement Policies and Procedures concerning the receipt, removal and movement of all Hardware and Electronic Media containing EPHI in to, out of, within and outside of its Facility.
2. Hardware and Electronic Media subject to this Policy include all Electronic Devices that maintain EPHI identified in Step One of the Organization's HIPAA Risk Analysis in accordance with Policy RA-1, HIPAA Risk Analysis and any Hardware or Electronic Media on which EPHI is maintained that is acquired by the Organization and, if permitted by a "Bring Your Own Device" or "BYOD Policy", by a Workforce Member after the date of the Organization's latest HIPAA Risk Analysis.
3. This Policy to comply with the Security Rule Standard regarding Device and Media Controls shall address Implementation Specifications set forth in the Standard which are:
   A. Disposal (Required) Procedures concerning the final disposition of EPHI, and/or the Hardware or Electronic Media on which it is stored.
   B. Media Re-Use (Required) Procedures for for removal of EPHI from Electronic Media before the Electronic Media are made available for Re-Use.
   C. Accountability (Addressable) Procedures to maintain a record of the movements of Hardware and Electronic Media and the Person responsible for Hardware or Electronic Media during its movement.
   D. Data Backup and Storage (Addressable) Procedures to create a retrievable, exact copy of EPHI when needed before movement of Hardware or Electronic Media.

Related Form

SR-20.A Contingency Plan Guide and Template

Protecting Patient Privacy is Our Job®
This document licensed for exclusive use by HIPAA Compliant Organization
The HIPAA E-Tool® © 2014 - 2022 ET&C Group LLC



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: SR-29.A	Page 1 of 1
Document Name: Bring Your Own Device (BYOD) Policy	

Supplemental Guidance for SR-29, Workstation Security

Bring Your Own Device (BYOD) Policy

You may use your own personal Electronic Device such as a Smartphone, Laptop or Tablet to perform your duties as a Workforce Member of HIPAA Compliant Organization related to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) only if you agree to comply fully with the same Safeguards that apply to all Electronic Devices that maintain and transmit EPHI owned by HIPAA Compliant Organization and permit a person designated by us to:

1. Encrypt your Electronic Device;
2. Install and maintain protective Software;
3. Install all available updates and security patches to Software on your Electronic Device;
4. Make random, unannounced inspections of your Electronic Device; and
5. Sanitize (make data on your Electronic Device unusable, unreadable, or indecipherable by methods or technology then in effect and approved by the Secretary of the U. S. Department of Health and Human Service) either:
   A. Before you dispose of the Electronic Device; or
   B. When you will no longer be a Workforce Member of HIPAA Compliant Organization.

In addition you agree:

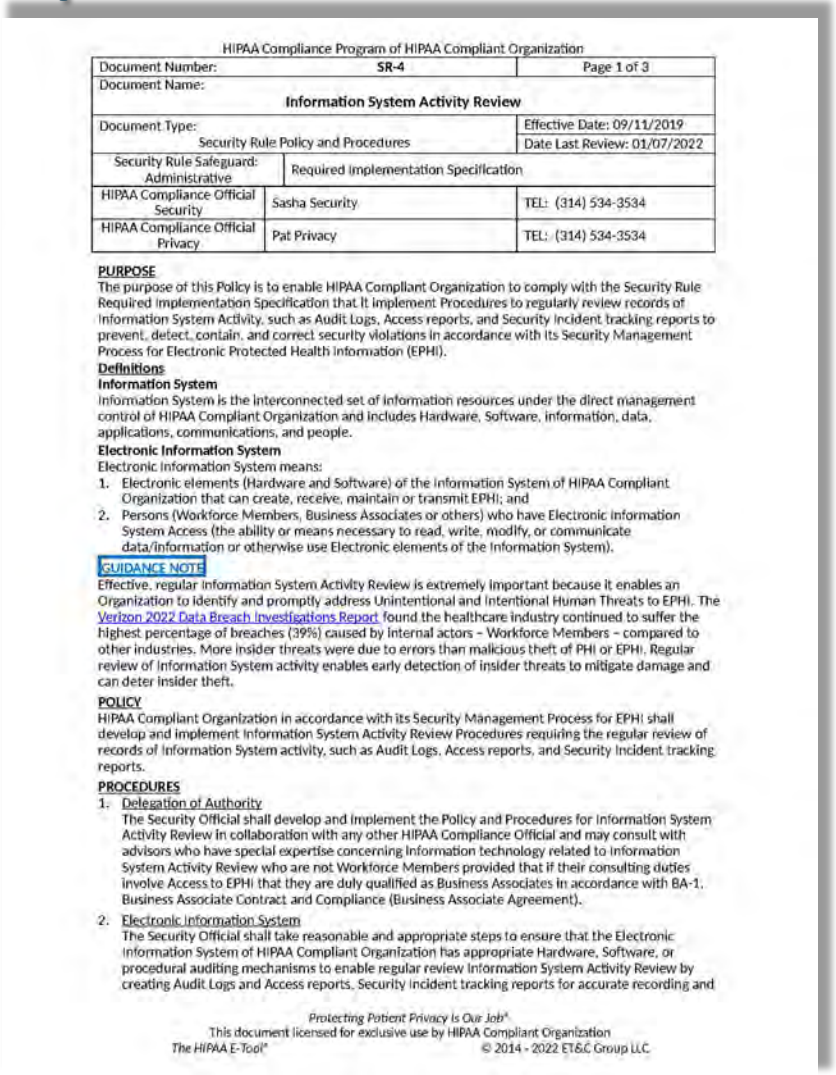
1. You will not to make and keep any copies of EPHI stored on your Electronic Device;
2. You will not allow any other person to make and keep any copies of EPHI stored on your Electronic Device;
3. You will not transmit EPHI from your Electronic Device by an unsecure method not approved by HIPAA Compliant Organization;
4. You will not transmit EPHI from your Electronic Device to any unauthorized person;
6. You will immediately report the loss, theft or tampering with your Electronic Device to us;
5. You will protect your Electronic Device with a Password that complies with our Password Management Policy; and
6. You will maintain effective Physical Safeguards for your Electronic Device that include:
   A. Keeping the Electronic Device in a secure, locked location when it is not in your possession;
   B. Keeping Encryption/Decryption Keys in a place that is separate from the container holding the Electronic Device (like a computer bag or briefcase) when you are away from our Facility.

Protecting Patient Privacy is Our Job®
This document licensed for exclusive use by HIPAA Compliant Organization
The HIPAA E-Tool® © 2014-17 ET&C Group LLC

BYOD Policy

HIPAA Compliance for Remote Workers

Access Control
Policy and Procedures



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: SR-4		Page 1 of 3
Document Name: **Information System Activity Review**		
Document Type: Security Rule Policy and Procedures		Effective Date: 09/11/2019 Date Last Review: 01/07/2022
Security Rule Safeguard: Administrative	Required Implementation Specification	
HIPAA Compliance Official Security	Sasha Security	TEL: (314) 534-3534
HIPAA Compliance Official Privacy	Pat Privacy	TEL: (314) 534-3534

PURPOSE
The purpose of this Policy is to enable HIPAA Compliant Organization to comply with the Security Rule Required Implementation Specification that it implement Procedures to regularly review records of Information System Activity, such as Audit Logs, Access reports, and Security Incident tracking reports to prevent, detect, contain, and correct security violations in accordance with its Security Management Process for Electronic Protected Health Information (EPHI).

Definitions

Information System
Information System is the interconnected set of information resources under the direct management control of HIPAA Compliant Organization and includes Hardware, Software, information, data, applications, communications, and people.

Electronic Information System
Electronic Information System means:
1. Electronic elements (Hardware and Software) of the Information System of HIPAA Compliant Organization that can create, receive, maintain or transmit EPHI; and
2. Persons (Workforce Members, Business Associates or others) who have Electronic Information System Access (the ability or means necessary to read, write, modify, or communicate data/information or otherwise use Electronic elements of the Information System).

GUIDANCE NOTE
Effective, regular Information System Activity Review is extremely important because it enables an Organization to identify and promptly address Unintentional and Intentional Human Threats to EPHI. The Verizon 2022 Data Breach Investigations Report found the healthcare industry continued to suffer the highest percentage of breaches (39%) caused by internal actors – Workforce Members – compared to other industries. More insider threats were due to errors than malicious theft of PHI or EPHI. Regular review of Information System activity enables early detection of insider threats to mitigate damage and can deter insider theft.

POLICY
HIPAA Compliant Organization in accordance with its Security Management Process for EPHI shall develop and implement Information System Activity Review Procedures requiring the regular review of records of Information System activity, such as Audit Logs, Access reports, and Security Incident tracking reports.

PROCEDURES
1. Delegation of Authority
   The Security Official shall develop and implement the Policy and Procedures for Information System Activity Review in collaboration with any other HIPAA Compliance Official and may consult with advisors who have special expertise concerning Information technology related to Information System Activity Review who are not Workforce Members provided that if their consulting duties involve Access to EPHI that they are duly qualified as Business Associates in accordance with BA-1. Business Associate Contract and Compliance (Business Associate Agreement).
2. Electronic Information System
   The Security Official shall take reasonable and appropriate steps to ensure that the Electronic Information System of HIPAA Compliant Organization has appropriate Hardware, Software, or procedural auditing mechanisms to enable regular review Information System Activity Review by creating Audit Logs and Access reports. Security Incident tracking reports for accurate recording and

Protecting Patient Privacy is Our Job®
This document licensed for exclusive use by HIPAA Compliant Organization
The HIPAA E-Tool® © 2014 - 2022 ET&C Group LLC

HIPAA Compliance for Remote Workers

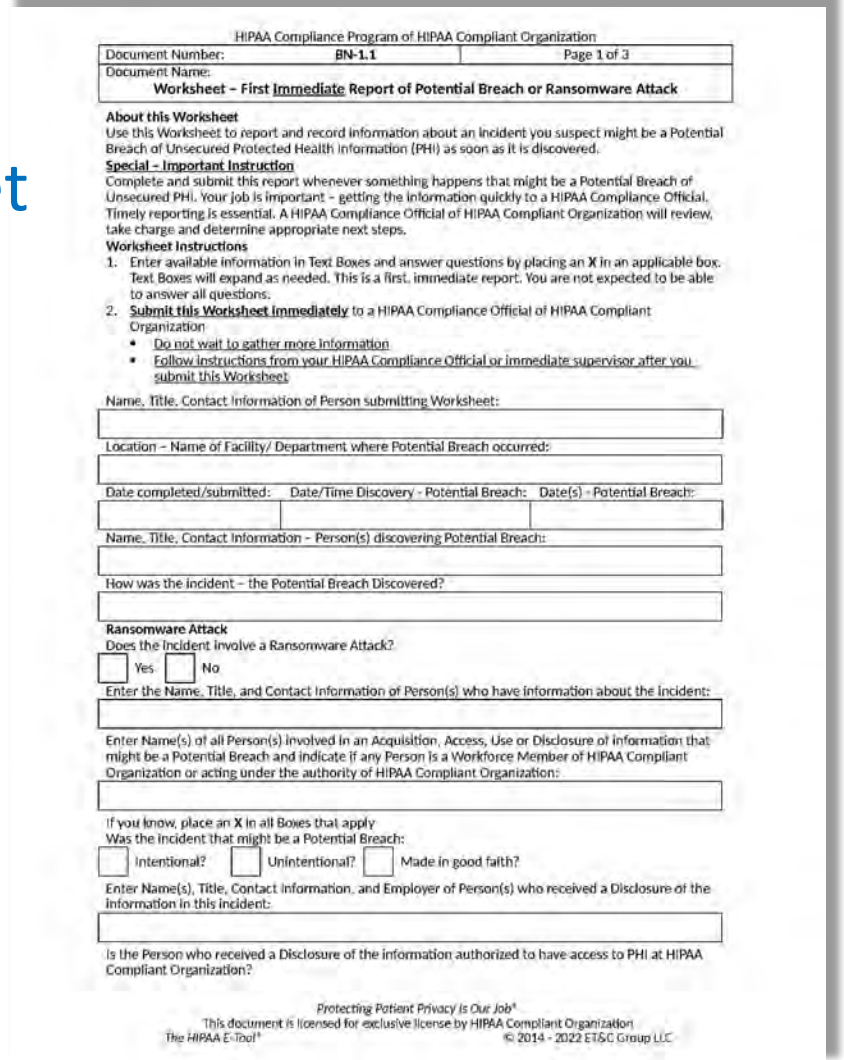
HIPAA Rules

Breach Notification Rule

- Written Policies and Procedures
  - Identify a Breach
  - Document an Incident was not a Breach
  - Breach Notification Content and Delivery Requirements
  - Document all required Breach Notifications were made
  - Special Circumstances
    - Law Enforcement Delay
  - Mitigate harm
  - Protect against further Breaches

HIPAA Compliance for Remote Workers

Worksheet Potential Breach Report



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number:	BN-1.1	Page 1 of 3
Document Name:	Worksheet – First Immediate Report of Potential Breach or Ransomware Attack	

About this Worksheet
Use this Worksheet to report and record information about an incident you suspect might be a Potential Breach of Unsecured Protected Health Information (PHI) as soon as it is discovered.

Special – Important Instruction
Complete and submit this report whenever something happens that might be a Potential Breach of Unsecured PHI. Your job is important – getting the information quickly to a HIPAA Compliance Official. Timely reporting is essential. A HIPAA Compliance Official of HIPAA Compliant Organization will review, take charge and determine appropriate next steps.

Worksheet Instructions
1. Enter available information in Text Boxes and answer questions by placing an **X** in an applicable box. Text Boxes will expand as needed. This is a first, immediate report. You are not expected to be able to answer all questions.
2. **Submit this Worksheet immediately** to a HIPAA Compliance Official of HIPAA Compliant Organization
   - Do not wait to gather more information
   - Follow instructions from your HIPAA Compliance Official or immediate supervisor after you submit this Worksheet

Name, Title, Contact Information of Person submitting Worksheet:

Location – Name of Facility/ Department where Potential Breach occurred:

Date completed/submitted: | Date/Time Discovery - Potential Breach: | Date(s) - Potential Breach:

Name, Title, Contact Information – Person(s) discovering Potential Breach:

How was the incident – the Potential Breach Discovered?

Ransomware Attack
Does the incident involve a Ransomware Attack?
☐ Yes ☐ No

Enter the Name, Title, and Contact Information of Person(s) who have information about the incident:

Enter Name(s) of all Person(s) involved in an Acquisition, Access, Use or Disclosure of information that might be a Potential Breach and indicate if any Person is a Workforce Member of HIPAA Compliant Organization or acting under the authority of HIPAA Compliant Organization:

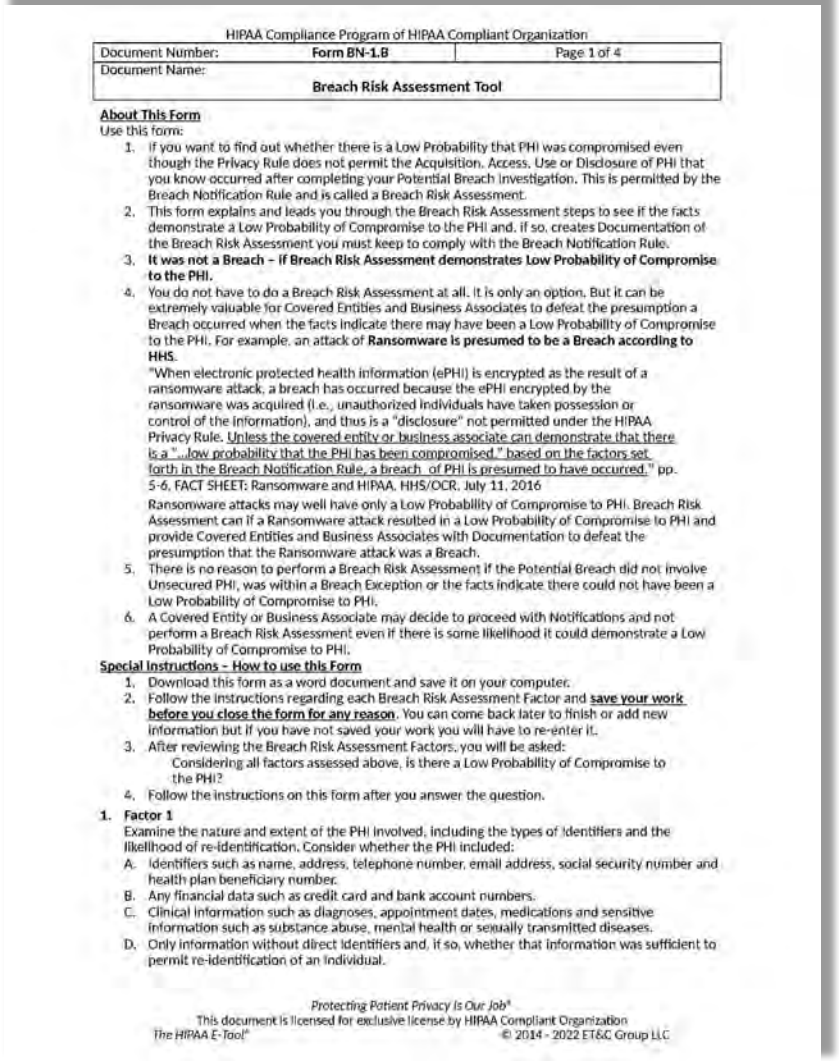
If you know, place an **X** in all Boxes that apply
Was the incident that might be a Potential Breach:
☐ Intentional? ☐ Unintentional? ☐ Made in good faith?

Enter Name(s), Title, Contact Information, and Employer of Person(s) who received a Disclosure of the information in this incident:

Is the Person who received a Disclosure of the information authorized to have access to PHI at HIPAA Compliant Organization?

Protecting Patient Privacy is Our Job®
This document is licensed for exclusive license by HIPAA Compliant Organization
The HIPAA E-Tool® © 2014 - 2022 ET&C Group LLC

Breach Risk Assessment Tool



HIPAA Compliance Program of HIPAA Compliant Organization

Document Number:	Form BN-1.B	Page 1 of 4
Document Name:	Breach Risk Assessment Tool	

About This Form
Use this form:
1. If you want to find out whether there is a Low Probability that PHI was compromised even though the Privacy Rule does not permit the Acquisition, Access, Use or Disclosure of PHI that you know occurred after completing your Potential Breach investigation. This is permitted by the Breach Notification Rule and is called a Breach Risk Assessment.
2. This form explains and leads you through the Breach Risk Assessment steps to see if the facts demonstrate a Low Probability of Compromise to the PHI and, if so, creates Documentation of the Breach Risk Assessment you must keep to comply with the Breach Notification Rule.
3. **It was not a Breach – if Breach Risk Assessment demonstrates Low Probability of Compromise to the PHI.**
4. You do not have to do a Breach Risk Assessment at all. It is only an option. But it can be extremely valuable for Covered Entities and Business Associates to defeat the presumption a Breach occurred when the facts indicate there may have been a Low Probability of Compromise to the PHI. For example, an attack of **Ransomware is presumed to be a Breach according to HHS.**
   "When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule. Unless the covered entity or business associate can demonstrate that there is a "...low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred." pp. 5-6, FACT SHEET: Ransomware and HIPAA, HHS/OCR, July 11, 2016
   Ransomware attacks may well have only a Low Probability of Compromise to PHI. Breach Risk Assessment can if a Ransomware attack resulted in a Low Probability of Compromise to PHI and provide Covered Entities and Business Associates with Documentation to defeat the presumption that the Ransomware attack was a Breach.
5. There is no reason to perform a Breach Risk Assessment if the Potential Breach did not involve Unsecured PHI, was within a Breach Exception or the facts indicate there could not have been a Low Probability of Compromise to PHI.
6. A Covered Entity or Business Associate may decide to proceed with Notifications and not perform a Breach Risk Assessment even if there is some likelihood it could demonstrate a Low Probability of Compromise to PHI.

Special Instructions – How to use this Form
1. Download this form as a word document and save it on your computer.
2. Follow the instructions regarding each Breach Risk Assessment Factor and **save your work before you close the form for any reason**. You can come back later to finish or add new information but if you have not saved your work you will have to re-enter it.
3. After reviewing the Breach Risk Assessment Factors, you will be asked:
   Considering all factors assessed above, is there a Low Probability of Compromise to the PHI?
4. Follow the instructions on this form after you answer the question.

1. Factor 1
Examine the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider whether the PHI included:
A. Identifiers such as name, address, telephone number, email address, social security number and health plan beneficiary number.
B. Any financial data such as credit card and bank account numbers.
C. Clinical information such as diagnoses, appointment dates, medications and sensitive information such as substance abuse, mental health or sexually transmitted diseases.
D. Only information without direct identifiers and, if so, whether that information was sufficient to permit re-identification of an individual.

Protecting Patient Privacy is Our Job®
This document is licensed for exclusive license by HIPAA Compliant Organization
The HIPAA E-Tool® © 2014 - 2022 ET&C Group LLC

HIPAA Compliance for Remote Workers

REMOTE WORK GUIDELINES

CREATING A REMOTE WORK CHECKLIST FOR YOUR ACTIVITIES

HIPAA Compliance for Remote Workers

Remote Work Checklist

Risk Analysis – PHI at Remote Location

- Where do you maintain PHI
- In what form or format do you maintain PHI
- Who has access to your workspace
- How do you protect the Privacy and Security of PHI
- How do you dispose of PHI when it is no longer needed
- How do you transmit PHI
- How do you protect the Privacy and Security of PHI during transmission

HIPAA Compliance for Remote Workers

Remote Work Checklist

Risk Management – PHI at Remote Location

Home Office

- Private Workspace
- Locked – and used – File Cabinet for Paper Records
- Encrypted Single Use – Single User Computer
- Virtual Private Network (VPN)
- Encrypted Single Use Portable Devices – Thumb & Backup
- Encrypted Single Use – Single User Mobile Devices
- Encrypt Emails and Text Messages
- Crosscut Shredder – Sanitize Electronic Devices before Disposal

HIPAA Compliance for Remote Workers

Remote Work Checklist

Risk Management – PHI at Remote Location

On the Road

- Encrypted Electronic Devices
- Keep Encryption Key safely separate from Encrypted Device
- Never Use Public Wi-Fi
- Virtual Private Network (VPN)
- Take care to prevent being overheard
- Manage Paper – Keep your Eyes and Hands on it
  - Locked Document Case
  - Bring home to shred

HIPAA Compliance for Remote Workers

Remote Work Checklist

Enterprise Risk Management – PHI at Remote Location

Remote Work Policy and Procedures

- Provide, Maintain and Update all Electronic Devices
- Encrypt, Install Protective Software and all Software Updates
- Remotely Monitor Electronic Device Activity
- Establish Organization Secure Virtual Private Network
- Maintain PHI in the Organization's secure cloud storage
- Use Encrypted Email and Text Message Services
- Provide Regular Training – Remote Work Privacy & Security
- Establish Procedures for Destruction of PHI

HIPAA Compliance for Remote Workers

Concluding Discussion, Questions, Comments

It's Your Turn

Questions, Comments, Suggestions

HIPAA Compliance for Remote Workers

We have reviewed

- Impact of the Pandemic
- Remote Work – the New Normal
- Why Protecting PHI Privacy is Essential
- HIPAA Rules and Remote Work Protocols
  - Privacy
  - Security
  - Breach Notification
- Remote Work Guidelines
- Conclusion, Discussion, Questions, Comments

HIPAA Compliance for Remote Workers

Thank You

Paul Hales, J. D.
HALESLAWGROUP
HEALTH INFORMATION PRIVACY
Paul.Hales@AttorneyHales.com
314-534-3534

ILLINOIS AAHAM American Association of Healthcare Administrative Management

The HIPAA E-Tool®

