AHS HIPAA Awareness Training

***IMPORTANT Once finished with this training, please visit completion link on last page to receive credit.**

Introduction

***IMPORTANT Once finished with this training, please visit completion link on last page to receive credit.**

This Course is intended for all members of the AHS workforce, including AHS employees, interns, volunteers, and temporary employees of:

- **AHS Central Office (AHS CO)**
- **Vermont Department of Health (VDH)**
- **Department of Mental Health (DMH)**
- **Department of Vermont Health Access (DVHA)**
- **Department for Children and Families (DCF)**
- **Department of Disabilities, Aging and Independent Living (DAIL)**
- **Department of Corrections (DOC)**

This course also is intended for members of AHS' State of Vermont Business Associates' workforces whose work directly supports AHS, including employees, interns, volunteers, and temporary employees of:

- **Agency of Digital Service (ADS)**

We are professionals working together to serve individuals respectfully.

Course Index

- NOTE: It will take most people between 30 minutes to one hour to complete this course.

How this course works

For this training and for general reference you may wish to open and view from the AHS HIPAA Site, the following:

Glossary of HIPAA Terms

Acronyms

HIPAA Top Tips

What is the purpose of this course?

The purpose of this course is to train the AHS workforce to keep private and secure the health information of the individuals we serve. Because of the very nature of our work, human services, we all come across sensitive information, even if "health information" is not our focus or responsibility.

This course focuses on the federal Health Insurance Portability and Accountability Act of 1996, known as "HIPAA," and its federal regulations, known as "the HIPAA Privacy Rule" and "the HIPAA Security Rule." This course is required by law. If you work for a department that regularly handles health information, this electronic course may be accompanied by more in-depth and job-specific HIPAA training.

If you have questions about how HIPAA applies to your job duties, you can talk with your supervisor and/or HIPAA Departmental Liaisons. You can visit the AHS HIPAA Site to find more resources, forms and links to HIPAA related information.

Why should you be concerned about the privacy and security of health information?

Almost daily, there are stories in the news about the mistaken disclosure of personal information by state agencies, non-profit organizations, or private businesses.

The individuals we serve trust us with highly personal information about themselves and their families. We must be deserving of their trust and keep their information private. This is a basic tenet that guides our work and ensures that we work together to serve individuals respectfully.

Examples of mistaken disclosures of personal information:

November 2019

The Centers for Medicare & Medicaid Services (CMS) Office of Civil Rights (OCR) imposed a $1,600,000 civil money penalty against the Texas Health and Human Services Commission (TX HHSC), for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules between 2013 and 2017. (ePHI) of 6,617 individuals was viewable over the internet, including names, addresses, social security numbers, and treatment information. The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials.

"Covered entities need to know who can access protected health information in their custody at all times," said OCR Director Roger Severino. "No one should have to worry about their private health information being discoverable through a Google search."

October 2019

Elite Dental Associates, Dallas ("Elite") has agreed to pay $10,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Elite is a privately-owned dental practice located in Dallas, Texas, providing general, implant, and cosmetic dentistry. OCR's investigation found that Elite had impermissibly disclosed the protected health information (PHI) of multiple patients in response to patient reviews on the Elite Yelp review page. Additionally, Elite did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protect the PHI of its patients or a Notice of Privacy Practices that complied with the HIPAA Privacy Rule.

"Social media is not the place for providers to discuss a patient's care," said OCR Director, Roger Severino. "Doctors and dentists must think carefully about patient privacy before responding to online reviews."

November 2019

In an agreement with the Office for Civil Rights (OCR) at the U.S Department of Health and Human Services (HHS), Sentara Hospitals (Sentara) have agreed to take corrective actions and pay $2.175 million to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification and Privacy Rules. OCR's investigation determined that Sentara mailed 577 patients' PHI to wrong addresses that included patient names, account numbers, and dates of services. Sentara reported this incident as a breach affecting 8 individuals, because Sentara concluded, incorrectly, that unless the disclosure included patient diagnosis, treatment information or other medical information, no reportable breach of PHI had occurred. Sentara persisted in its refusal to properly report the breach even after being explicitly advised of their duty to do so by OCR.

"HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed." said Roger Severino, OCR Director. "When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."

Recent enforcement action reported by OCR: https://www.hhs.gov/ocr/newsroom/index.html

1

HIPAA BASICS

This lesson addresses the importance of all members of the AHS workforce being respectful of the personal and confidential information regarding the individuals we serve. This lesson introduces the federal law entitled HIPAA and provides an overview of other laws that govern privacy.

The goal of this lesson is to enable you to:

- Understand what HIPAA is.
- Understand the importance of being respectful of the personal information of the individuals we serve.
- Understand why AHS is required to comply with the HIPAA Privacy and Security Rules.
- Recognize that there are other laws, both state and federal, and agency rules that you need to review and comply with when doing your work.

What is HIPAA?

HIPAA stands for *Health Insurance Portability and Accountability Act of 1996*. It is a federal law. The United States Congress enacted HIPAA to make sure that an individual's health information is kept private and secure.

All of AHS is considered a covered entity under HIPAA, which means that all members of the AHS workforce must have a basic understanding of this law.

What is Respectful Service?

The individuals we serve trust us with highly personal information about themselves and their families. As members of the AHS workforce, it is very important that we keep this information confidential and that consumers trust that we will do so.

We may only share personal information when it is necessary for us to perform our jobs or in special situations which will be covered in this course.

Why is AHS a "Covered Entity" under HIPAA?

HIPAA covers three types of organizations:

1. A health care provider such as a physician, dentist, pharmacist, or hospital when it provides health care and electronically transfers patient information.
2. A health plan, organization or individual that pays for or authorizes payment for health care, such as Medicare and Medicaid programs, insurance companies and health management organizations.
3. A health care clearinghouse or organization that facilitates the processing of health information such as transcription or billing services.

AHS is a covered entity because AHS provides health care and health care coverage. Although not every department and division provides direct health services or payment for health services, the entire Agency is considered a covered entity. Therefore all members of the AHS workforce must comply with HIPAA.

What is the HIPAA Privacy Rule and the HIPAA Security Rule?

The *HIPAA Privacy Rule* and the *HIPAA Security Rule* are federal regulations that implement HIPAA. You need to understand how these rules affect your work and what you need to do to follow them.

The *HIPAA Privacy Rule* relates to the ways we use and disclose **all health information**, whether the health information is in written, spoken, or electronic form. It creates minimum nationwide standards for making sure an individual's health information is kept private.

The *HIPAA Security Rule* specifically applies to health information in electronic form. It relates to the ways we protect and control access to an individual's **electronic health information**.

Do other federal and state laws govern privacy?

In addition to HIPAA, there are a number of federal and state laws and agency rules that govern the way we must handle the personal information entrusted to us.

Examples of these laws and rules are:

- AHS Consumer Information and Privacy Rule (AHS rule 08-048) establishes a basic presumption of confidentiality of the information of those applying for and receiving services from us.
- 18 VSA 1881 adopts HIPAA as the Vermont standard for confidentiality of protected health information.
- 18 VSA 7103 regulates the disclosure of certain mental health records.
- 9 VSA Chapter 062 regulates the protection of personally identifiable information such as Social Security numbers and financial information.
- 42 C.F.R. Part 2 applies to information about substance use disorder treatment.

If you have questions regarding federal and state confidentiality laws that apply to your work, talk with your supervisor or an attorney for your department.

What is 42 CFR Part 2 and How Does it Relate to HIPAA?

Part 2 refers to the federal law and regulation protecting the privacy of substance use disorder (SUD) treatment records. Part 2 protects records with patient-identifying information that identifies an individual as having sought, received, or applied for substance use disorder services from a Part 2 program.

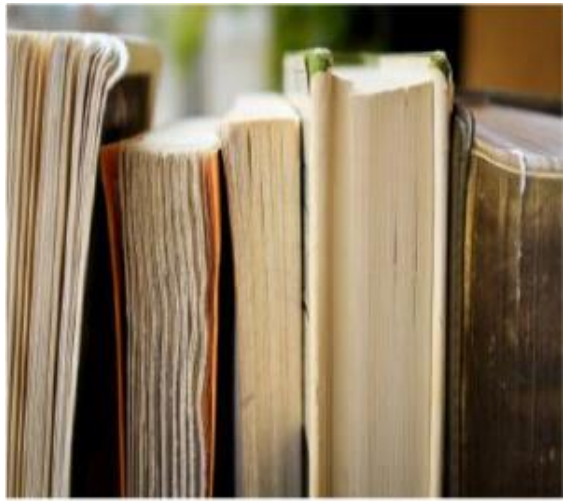
Part 2 is more protective of privacy than HIPAA in many ways, and when it is more protective, then Part 2 controls. For example, HIPAA allows sharing of health information for treatment, payment, or health care operations without the consent of the individual, but Part 2 does not and requires consent to disclose the records. All SUD treatment records are protected by HIPAA, but they are only covered also by Part 2 if they were created by a Part 2 program.

Not every provider of SUD treatment meets the federal definition of a Part 2 program, so it may take a specific analysis to determine whether HIPAA or Part 2 applies to the records.

If you need to share, or are asked to share, SUD treatment records of someone receiving services from AHS for your work, *talk with your supervisor or an attorney for your department to be sure you know what laws apply to those records before sharing them.*

What happens when other federal or state laws are more protective of an individual's privacy than HIPAA?

When Vermont or federal law is stricter than HIPAA in protecting the privacy of an individual's health information, we need to follow the stricter law. That is to say, we need to follow the law that affords more privacy protections for an individual's health information.



For example, Part 2 is more protective of privacy for substance use disorder (SUD) treatment records than HIPAA in many ways. When working with SUD treatment records, always check the Part 2 requirements, in addition to HIPAA.

Let’s Review Some Concepts

Protect Privacy

HIPAA is a federal law enacted to protect the privacy of an individual's health information. Vermont adopted HIPAA as the standard for confidentiality of protected health information.

Confidential

As members of the AHS workforce we must keep the information about the individuals we serve confidential.

Governs

The HIPAA Privacy Rule governs how we use and disclose the health information of the individuals we serve.

Other Rules

There are other federal and state laws and rules that protect the privacy of protected health information. If these laws or rules protect the privacy of an individual's health information even more than HIPAA, we must follow them.

Protects Access

The HIPAA Security Rule governs how we protect and control access to the electronic health information of the individuals we serve.

When to Share

We may share certain information when it is necessary for us to perform our jobs.

2

PRIVACY BASICS

This lesson introduces the AHS HIPAA Privacy Standards and Guidelines. The lesson examines the definition of "health information" under these Standards and Guidelines.

The goal of this lesson is to enable you to:

- Understand the AHS HIPAA Privacy Standards and Guidelines and how to access them.
- Identify what personal information of an individual we serve is "protected health information" under HIPAA.

What are the AHS Standards and Guidelines?

The HIPAA Privacy Rule requires AHS to implement policies and procedures to safeguard the privacy of the health information entrusted to us. AHS calls these policies and procedures the "AHS HIPAA Privacy Standards and Guidelines." As members of the AHS workforce, we must know how the Standards and Guidelines apply to our work and how to follow them.

Lesson 3 explains these Standards and Guidelines.

Show me the AHS HIPAA Privacy Standards and Guidelines

What is health information?

HIPAA defines "**individually identifiable health information**" as:

- Any information, whether oral or recorded in any form, that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual; and
- is created or received by a health care provider, health plan, employer or health care clearinghouse; and
- that identifies the individual; or
- there is a reasonable basis to believe the information can be used to identify the individual.

The term "PHI," stands for "protected health information." PHI is individually identifiable health information that is maintained or transmitted in electronic or any other form or medium.

Let’s Review Some Concepts

Policies & Procedures

The HIPAA Privacy Rule requires that AHS adopt policies and procedures to carry out the Privacy Rule. AHS calls these policies and procedures the AHS HIPAA Privacy Standards and Guidelines.

You are Responsible

As a member of the AHS workforce you are responsible for being familiar with the Standards and Guidelines and following them when you perform your work.

Disclosing Health Information

The Standards and Guidelines define "health information" and dictate how AHS may use and disclose health information of the individuals we serve.

Questions?

If you do not understand how the Standards and Guidelines apply to your work, it is your responsibility to talk with your supervisor.

3

STANDARDS & GUIDELINES

This lesson focuses on four of the Standards and Guidelines that members of the AHS workforce who use and disclose health information will encounter on a regular basis: Minimum Necessary, Authorization, Breach Reporting, and Business Associates.

The goal of this lesson is to enable you to:

- Understand how the Minimum Necessary Rule guides our use and disclosure of health information.
- Understand when an authorization is necessary prior to disclosure of protected health information.
- Understand how to report a possible or actual violation of HIPAA.
- Understand the term Business Associate.

What is Minimum Necessary?

The Minimum Necessary Rule requires that members of the AHS workforce make reasonable efforts to use, disclose or request only the minimum amount of health information that is necessary to accomplish the purpose of the use, disclosure, or request. This rule does not apply when the disclosure is to a health care provider for the purpose of providing treatment, or when the use or disclosure is authorized in writing by the individual.

You should only use, disclose, or request health information that you need to perform your job duties.

What is Authorization?

An Authorization is a form that, in most instances, must be signed by an individual before AHS may disclose PHI about that individual.

Authorization is required for sharing PHI with individuals and entities outside of AHS. Authorization may even be required, in certain circumstances, to share PHI with employees in other departments and divisions within AHS.

Ask your supervisor or HIPAA liaison where you can find authorization forms for your program.

Generally, authorizations are not required for AHS to use and disclose an individual's health information for purposes of treatment, payment, or health care operations; however, authorizations are required for use and disclosure if the information is SUD treatment records under Part 2.

What is Breach Reporting?

A breach occurs when a member of the AHS workforce improperly accesses, uses or discloses PHI. If you think you or a co-worker has not complied with HIPAA, then you must complete and submit a Privacy/Security Event Report form as soon as possible. If you have any questions, you should talk with your supervisor or your division's HIPAA Liaison.

If it is an emergency situation involving the disclosure of electronic protected health information and/or the security of AHS computer systems, you must contact the AHS Security Officer immediately.

The Privacy/Security Event Report Form is posted on the AHS internet page here.

What is a Business Associate?

A Business Associate is an individual or organization that performs a service for or on behalf of AHS which involves disclosure or use of protected health information. Examples of services Business Associates provide for AHS are claims processing, data analysis, and call center services. The Agency of Digital Services is a Business Associate for the services they provide for AHS.

An individual or organization that provides treatment services on behalf of AHS is not a Business Associate.

AHS must have a written agreement, called a Business Associate Agreement, with its Business Associates. By signing the Business Associate Agreement the individual or organization agrees to comply with the terms of the HIPAA Privacy and Security Rule when performing the services on behalf of AHS.

Let's Review Some Concepts

Minimum Necessary Rule

The Minimum Necessary Rule requires that you only use, disclose, or request health information that you need to perform your job duties. In some cases, the Minimum Necessary Rule does not apply. For example, the rule does not apply when the disclosure is to a health care provider for the purpose of providing treatment to the individual or when the use or disclosure is authorized in writing by the individual.

Individual Authorization

Generally, an individual's Authorization is not required for treatment, payment of health care operations but is required before an AHS employee may disclose that individual's PHI to someone else.

Business Associate Agreements

AHS must have Business Associate Agreements with those that perform services on its behalf which involve protected health information. In the agreement the individual or organization who will perform the service agrees to comply with the terms of the HIPAA Privacy and Security Rule.

Reporting the Breach

When you improperly access, use, or disclose an individual's PHI, either intentionally or inadvertently, you must promptly report the Breach.

4

NOTICE OF PRIVACY PRACTICES

This lesson examines the AHS Notice of Privacy Practices (NPP).

The goal of this lesson is to enable, you to:

- Understand the NPP.
- Know when an individual we serve should receive a NPP.

What is the Notice of Privacy Practices?

HIPAA requires all covered entities to have a NPP that tells the individuals they serve what will happen to health information they share with the covered entity.

The AHS NPP tells the individuals we serve:

- How AHS or a specific program of AHS may use or disclose their health information,
- What rights they have regarding their health information, and
- How they can complain if they believe AHS or a specific program of AHS has violated those rights.

What disclosure of health information does the Notice of Privacy Practices allow?

The NPP provides that AHS may use and disclose health information ***without an individual's written permission*** regarding:

- Treatment,
- Payment for treatment,
- Health care operations, and
- Specific circumstances, allowed by HIPAA, including reports of child abuse, certain law enforcement purposes, and health oversight activities.

Example of disclosure for:

Treatment Purposes:

AHS discloses an individual's health information to the individual's doctors to help determine a course of care for the individual.

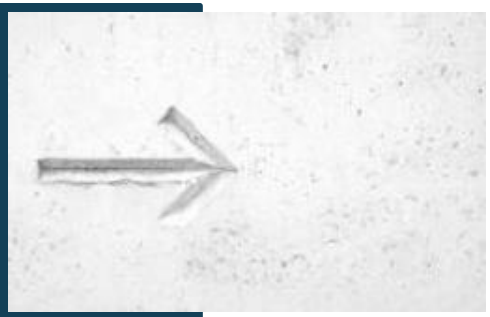
Payment Purposes:

AHS receives health information from the individual's doctor so that it can pay the doctor for their services.

Health Care Operations:

AHS shares an individual's health information with a contractor who evaluates the care and services that an individual receives to ensure that quality care was provided.

What rights do individuals have regarding health information under NPP?



The notice informs individuals of their rights with respect to their health information such as:

- Reviewing their health information,
- Obtaining an accounting of disclosures of their health information by AHS, and
- Written notification in the event of a breach of their health information.

Does the NPP include a process for filing a complaint if an individual believes AHS has violated his/her rights?

The NPP explains the process for filing a complaint with the Agency of Health and Human Services, Office of Civil Rights (OCR) if an individual believes AHS has violated his/her rights.

Who receives a Notice of Privacy Practices?

1. Individuals who enroll for health plan benefits, such as Medicaid, Dr. Dynasaur, and WIC.
2. Individuals who receive direct health services from AHS, such as children served by the Children with Special Health Needs program, patients at the Vermont Psychiatric Care Hospital, and individuals receiving chronic care case management services.

AHS must give the Notice of Privacy Practices to individuals at the time of enrollment in a health plan, or at the time they receive direct health services.

Show me The Notice of Privacy Practices

In accordance with the AHS Standards for Translation of Vital Documents for Persons with Limited English Proficiency, the NPP has been translated into the following languages: Bosnian, Burmese, French, Nepali, Somali, Spanish, and Swahili

Let's Review Some Concepts

AHS Notice of Privacy Practices (NPP)

A NPP is a document that outlines how AHS, and its programs, may use or disclose an individual's health information, what rights the individual has regarding their health information, and how the individual can file a complaint if he/she believes AHS, or its programs, violated the individual's rights set forth in the AHS HIPAA Privacy Standards and Guidelines.

When do Individuals Receive NPP

Individuals receive an AHS NPP when:

- An individual is enrolled in an AHS health plan.
- An individual is receiving direct health care from an AHS program.

5

COMMUNICATIONS

This lesson explains the manner and methods for properly communicating protected health information.

The Goal Of This Lesson is to Enable You To :

- Talk with your co-workers and external entities about health information of the individuals we serve.
- Recognize how to properly use the phone, fax, and email to communicate this information.

May I talk about health information with my co-workers?

Yes

Yes, when you need to talk about an individual's health information with co-workers, in most instances you may.

When you need to discuss the PHI of an individual you must:

- Limit the discussion to the minimum amount of health information necessary to do your job;
- Only discuss the health information in a private place; and.
- Never discuss health information in public places where it can be easily overheard by others, such as in the hallway or the cafeteria.

May I Communicate PHI By Phone, Fax, Or Email?

Yes

You may communicate PHI by phone , fax or email AFTER confirming the privacy protection and security of the communication method you plan to use to communicate the minimum amount of health information necessary to do your job.

- When you need to talk on the phone about an individual's health information in order to perform your job duties, you may.
- When you need to fax an individual's health information in order to perform your job duties, you may.
- When you need to send an individual's health information by email in order to perform your job duties, you may.

May I Communicate PHI By Text Messaging?

No

Currently text messaging is not a secure means to comminate protected health information. If you have questions about how to remotely communicate protected health information as part of your job function contact your department's IT staff.

How to Communicate PHI

Phone

Speak quietly and in as private a space as possible. Before communicating protected health information, you must first verify the identity of the person you are talking with and his/her authority to have access to the protected health information.

Fax

Before you fax protected health information, you must verify the fax number of the person or entity to whom you are faxing. You must also confirm that you entered the recipient's fax number correctly. If you do not know if the receiving fax is in a secure location, you must call the intended recipient to notify them you are sending a fax.

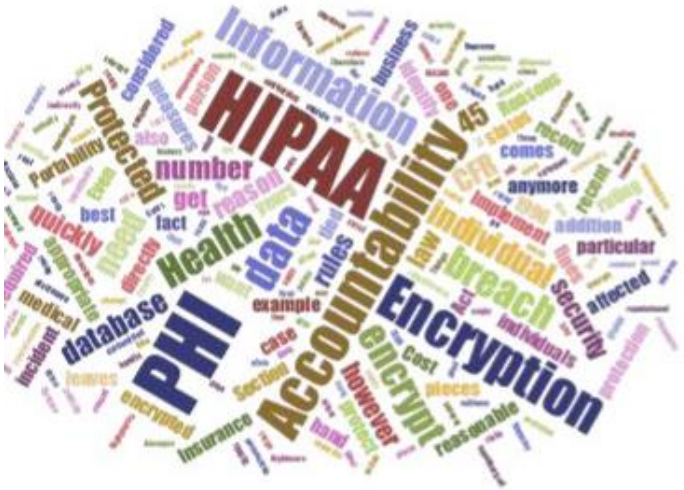
Email

Proceed with extreme caution when doing so. Whenever you are sending protected health information by email you must confirm that the addressee is the intended recipient. You must also confirm that you have not unintentionally selected the wrong recipient from the email autocomplete function.

What Should I Do If I Have An Accidental Disclosure?

Accidental disclosures of protected health information can occur when you use the phone, fax, or email.

If you believe you have accidentally disclosed protected health information, you must contact your Department's HIPAA liaison and complete a HIPAA Privacy/Security Event Report Form found on the AHS website.



Let’s Review Some Concepts

When to Discuss PHI

You may discuss protected health information with your co-workers only when necessary to fulfill your job responsibilities. You must be careful about how and where you talk about this information.

How to Communicate PHI

You may communicate protected health information by phone, fax and email. When you do communicate by these methods, you must ensure that the information is only communicated to the intended recipient and cannot be heard or seen by others.

Use Caution

Use of email requires extreme caution due to the ease with which mistakes can be made.

Text Messaging

Do not communicate protected health information via text message.

6

SECURITY BASICS

This lesson examines the safety measures you must take to keep electronic protected health information secure.

The goal of this lesson is to enable you to:

- Maintain a safe computer workstation.
- Keep state electronic equipment safe and secure.
- Take precautions to protect against phishing, viruses and other malicious software.
- Protect your passwords.
- Securely send email.
- Protect documents that you print.

What safety measures should I take to protect my computer workstation?

We all must do our part to ensure the confidentiality of protected electronic health information. Our computer workstations are access points to protected electronic health information.

If you have a computer workstation (or share a workstation with others), you must follow these safety measures to protect your workstation:

1. Do not store protected electronic health information on the hard drive (usually called the "C" drive) of your workstation unless you are authorized to do so.
2. Do not download protected electronic health information onto unauthorized electronic storage devices.
3. Position your computer screen so others cannot casually view it.
4. Never allow someone else to use your username or password and never use someone else's username or password.
5. Lock or logoff from your workstation when you leave it unattended.

How do I keep state electronic equipment safe and secure?

State issued electronic equipment may include laptops, tablets, and phones. It is very important to protect them from loss and theft. When not using them, keep electronic devices locked up and out of sight. This is especially important when you are working remotely and traveling. Do not allow anyone else, including coworkers, to use your electronic devices.

If your state-issued electronic equipment is lost or stolen immediately contact your supervisor or the AHS Privacy Officer at AHS.PrivacyAndSecurity@Vermont.gov

What precautions must I take to protect against viruses and other malicious software?

Malicious software or "malware" is used as a catch-all term to refer to any software that causes damage to a single computer, server, or computer network. Malware might expose or alter confidential information; delete or remove important files; disable your and other AHS network computers; email everyone in your email address book; and/or spread quickly to other machines.

You must take these precautions to protect against malware:

- Always follow AHS, and state policies and guidelines on email and internet use.
- Never open an email attachment from someone you don't know or whose identity you cannot verify.
- Never disable or attempt to disable antivirus and other protective software.
- Never attempt to install any software without first contacting your Information Technology (IT) support staff.
- Never download or execute a file from a source you cannot trust or verify.

How should I protect my password?

<u>You must protect your password by taking these steps</u>:

- Do not write it where it may be seen, such as on a post-it note near your computer.
- Do not share your password with anyone!

Change your password **immediately** if another person learns your password.

When I use email, how can I safeguard protected electronic health information?

You may only use state email to conduct AHS business. Sometimes email will contain protected health information.

AHS internal email is secure and encrypted. If you are emailing outside of AHS, email is not automatically secure. When sending protected health information to an external entity you must use the secure method approved by ADS. Click here to review the approved ADS secure email method.

For additional instructions about the approved method to safeguard this information, contact your supervisor or AHS Privacy and Security staff at AHS.PrivacyAndSecurity@Vermont.gov

A large number of AHS HIPAA violations are caused by people sending email to unintended recipients. This can happen when:

- You select the wrong recipient using the “autocomplete” function;
- You select the wrong recipient from the global address book; or
- You send email to a distribution list.

If you suspect email containing protected electronic health information has been accidentally or improperly distributed:

- Immediately try to recall the email message; and
- Inform your supervisor and the AHS Privacy Officer.

When I use a printer, how can I safeguard electronic health information?

When you print electronic health information, you should take measures to protect it. Follow these steps:

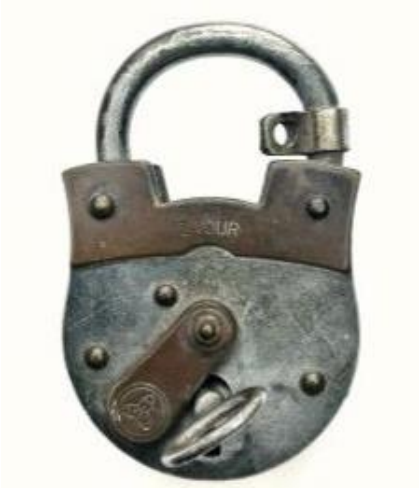
1. Confirm which printer you are printing to.
2. Promptly remove documents containing protected health information from the printer.
3. If you accidentally send protected health information to a printer, cancel the print job. Then check to make sure that the document did not print.

Let's Review Some Concepts

Security Basics

HIPAA requires that AHS protect and control access to electronic health information. If you work with electronic health information, you must use safety measures to help protect and control access to it. You must:

- Maintain a safe computer workstation.
- Keep state electronic devices safe and secure.
- Take precautions to protect against viruses and other malware.
- Keep your account passwords protected.
- Send email securely.
- Safeguard electronic health information when printing.



7

COMPLAINTS, INVESTIGATIONS & SANCTIONS

This lesson describes how an AHS employee or member of the public may file a complaint when he/she believes that AHS has violated the privacy of an individual's health information. This lesson outlines the investigation process and explains the sanctions and penalties for failing to comply with HIPAA.

The goal of this lesson is to enable you to:

- Recognize when you or another member of the AHS workforce has, or might have, violated HIPAA
- Recognize when you should inform the AHS Privacy Officer of a potential HIPAA violation
- Understand that if you are informing the Privacy Officer that another member of the AHS workforce has, or might have, violated HIPAA, you will be protected from retaliation by State and Federal whistleblower laws.
- Be aware that members of the public can file a HIPAA privacy complaint with the AHS Privacy Officer or the United States Department of Health and Human Services (HHS) when they believe AHS has violated their HIPAA rights.
- Understand the process for making and investigating HIPAA complaints.
- Understand that a member of the AHS workforce can face sanctions for failing to comply with HIPAA.
- Understand that there may be criminal and civil penalties that result from serious HIPAA violations.

What procedure do I follow if I think I have violated HIPAA, or another member of the AHS workforce has violated HIPAA?

If you think that you have violated HIPAA or another member of the AHS workforce has violated HIPAA, you must inform your supervisor, your department's HIPAA liaison, or the AHS Privacy Officer. If you are a supervisor, you must inform your department's HIPAA liaison or the AHS Privacy Officer.

When you or your supervisor are reporting a HIPAA violation use the Privacy/Security Event Report Form to report the event. This form can be found on the AHS website.

Here are examples of situations that indicates a potential HIPAA violation that you would need to report to your supervisor or the AHS Privacy Officer:

- A member of the AHS workforce accidentally or intentionally discloses protected health information to an unauthorized person.
- A member of the AHS workforce accesses protected health information for reasons other than performing his/her job duties.
- Documents containing protected health information are stolen or lost.
- Documents containing protected health information are not stored properly or are not disposed of properly.
- An unauthorized person is given access or asks for access to AHS information systems.
- Computer equipment (laptops and other portable devices or desktop workstations) containing protected health information is stolen.
- An unauthorized person is found in office space containing protected health information.

Are there whistleblower provisions in the Standards and Guidelines that protect me from retaliation for notifying the AHS Privacy Officer or HHS?

HIPAA includes whistleblower provisions that prohibit retaliation against members of the AHS workforce who reveal a privacy or security violation by another member of the workforce.

If you believe a fellow workforce member is not complying with HIPAA, it is essential that you inform the Privacy Officer. As members of the AHS workforce we have a duty to the individuals we serve to monitor our protection of their privacy.

Can members of the public file a complaint when they believe their HIPAA privacy rights have been violated?

Members of the public can file a complaint by using the AHS Health Information Privacy Complaint Form or by letter, email, or phone. Members of the public can locate the privacy complaint form and information on how to file a complaint on the AHS website.

Members of the public can also file a complaint with HHS. Members of the public can locate information about how to file a complaint on the HHS website.

What happens when I report a violation of HIPAA to the AHS Privacy Officer?

The AHS Privacy Officer will review the report to determine whether there was a HIPAA violation. If so, s/he will assess the level of risk of the violation. When making these determinations, the Privacy Officer will usually consult with the reporter, the supervisor and/or the department's liaison.

If the facts of the potential violation are in dispute, the Privacy Officer and the Personnel Unit will investigate the reported violation to determine the facts and whether HIPAA has been violated.

In most cases, violations are inadvertent. Whether intentional or inadvertent, the Privacy Officer will work with the department or division to create a plan to mitigate any harm resulting from the violation.

Are there sanctions for HIPAA violations?

AHS may impose sanctions against workforce members who do not comply with HIPAA.

AHS will consider the severity of the violation, including the type of protected health information that the workforce member disclosed and the intent of the disclosure, to determine the appropriate sanction.

Are there penalties for not complying with HIPAA?

The United States Department of Health and Human Services Office of Civil Rights can impose civil and criminal penalties for violating HIPAA.

Civil penalties range from $100 to $1,500,000 per year for repeated violations of the same infraction. Criminal penalties range from one year in prison and a $50,000 fine to ten years in prison and a $250,000 fine.

Let’s Review Some Concepts

Report!

A member of the AHS workforce must report any potential HIPAA violation.

Whistleblower Provisions

A member of the AHS workforce who reports violations by another member of the AHS workforce will be protected by HIPAA's whistleblower provisions.

Public Complaint

A member of the public can file a complaint when they believe that AHS has not protected the privacy of their health information.

Filing Complaints

Complaints can be filed directly with the AHS Privacy Officer and/or the United States Department of Health and Human Services.

Investigation

When a complaint is filed with AHS, the AHS Privacy Officer and other appropriate personnel will investigate the complaint.

Violations

If a member of the AHS workforce is found to have violated HIPAA, AHS may impose sanctions. The severity of the sanctions will be based upon the seriousness of the violation. HHS may impose criminal and civil penalties for HIPAA violations.

Test Your HIPAA Knowledge

As members of the Agency of Human Services (AHS) workforce, the individuals we serve trust us with health information about themselves. We must deserve their trust. We must be knowledgeable about HIPAA Privacy so that we can serve individuals respectfully and to the best of our abilities.

The following quiz is designed to test your HIPAA knowledge.

You may want to review individual sections before completing the quiz.

Lesson 1: HIPAA Basics

Lesson 2: Privacy Basics

Lesson 3: Four Standards and Guidelines

Lesson 4: Notice of Privacy Practices

Lesson 5: Communications

Lesson 6: Security Basics

Lesson 7: Complaints, Investigations & Sanctions

The Following 7 question quiz is designed to test your HIPAA knowledge

1. All of AHS is covered by the HIPAA Privacy and Security Rules even though not all divisions provide health care and health care coverage.

- A) True
- B) False

2. The HIPAA privacy rule applies only to electronic information.

- A) True
- B) False

3. The Notice of Privacy Practices outlines how AHS may use or disclose an individual's health information, what rights the individual has regarding his/her health information, and how he/she can file a complaint if he/she believes AHS has violated these rights.

- A) True
- B) False

4. The Minimum Necessary Rule applies in all uses and disclosures of an individual's health information.

- A) True
- B) False

5. I should never send sensitive identifiable health information by email or fax.

- A) True
- B) False

6. I may give a coworker my computer password, as long as I know and trust the person.

- A) True
- B) False

7. If I send or disclose an individual's health information to the wrong person, but it does not appear to have caused any harm, I do not have to report this to my supervisor or the AHS privacy officer.

- A) True
- B) False

Score Your Quiz Results

Your Answers	Correct Answer
1.	True
2.	False
3.	True
4.	False
5.	False
6.	False
7.	False

If you did not score 100% go back and review the question(s) you got wrong along with the section materials until you understand why you answered the question incorrectly.

VERMONT
AGENCY OF HUMAN SERVICES

CONGRATULATIONS! Thank you for Finishing the Training!!!

For credit and to complete the Confidentiality Statement please visit:
https://www.surveygizmo.com/s3/5830916/AHS-HIPAA-Awareness-Training-Completion-Link

AHS HIPAA Awareness Training

By Agency of Human Services (PDF/AHS Online)