Protecting the Privacy and Security of Confidential Information

Annual Compliance Training

Protecting the Privacy and Security of Confidential Information

Course Information

Course Title:	Protecting the Privacy and Security of Confidential Information
Regulations/Standards:	US Department of Health and Human Services Office for Civil Rights (OCR)
Approximate Time to Complete:	15 minutes
Intended Audience:	All LVHN employed staff
Technical Specifications:	Internet Explorer 11 or Microsoft Edge
Date Revised:	August 2021

Contact Information

Please forward any content questions or concerns to the Subject Matter Expert:	Compliance Department

Please call the Technology Support Center at 610-402-8303 with any technical issues.

This course does not contain audio.

Objectives

After completing this course, you should be able to:

- Explain the fundamental purpose of Lehigh Valley Health Network's Privacy & Information Security Programs
- Describe key actions every employee is expected to take to safeguard patient health information, other confidential information, and all Technology resources
- Know where to locate network privacy and information security policies on our intranet

Protecting the Privacy and Security of Confidential Information

Why?	What?	How?	When?	Where?

Questions asked and answered during this course:

- **WHY** is this Privacy and Security course required?
- **WHAT** confidential information must I safeguard?
- **HOW** can I keep confidential information and information systems resources secure?
- **WHEN** should I report concerns about information privacy and/or security?
- **WHERE** do I find privacy and information security policies on our intranet?

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

Why comply with HIPAA?

Our patients depend on us to protect the **Privacy and Security** of their **Confidential Information.**

We must comply:

- To show LVHN's commitment to protect privacy
- Because we are obligated to follow LVHN's policies and procedures
- Because patients are trusting us with their personal information

Compliance is mandatory. It is not optional. If you choose not to follow the rules, you could be at risk and you could put LVHN at risk.

HIPAA Privacy and Security Rules

The **Health Insurance Portability and Accountability Act (HIPAA)** provides a framework for nation-wide protection of patient confidentiality and security of electronic systems.

- Privacy rule – 2003
- Security rule – 2005
- HITECH – 2009
- Omnibus - 2013

What Confidential Information Must I Safeguard?

All Confidential Information must be protected.

This includes:

- Patients' Protected Health Information (PHI)
- Personnel information
- Strategic, financial or other business information

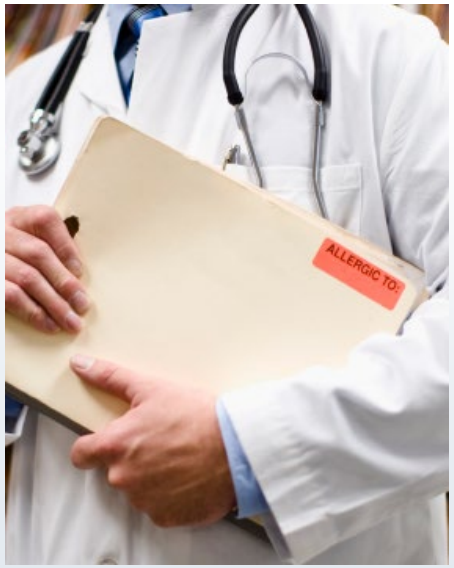
The information can be maintained in *any* format:

- Verbal discussion
- Written
- Computer applications/ software
- Computer hardware

Protecting the Privacy and Security of Confidential Information

PHI

Protected Health Information is health information, including demographic information, collected from an individual that:



- Is created or received by LVHN and
- Relates to the past, present, or future physical or mental health or condition of an individual; providing health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- Could be used to identify the individual

PHI Identifiers

Under HIPAA, a patient's health information that contains any of the following identifiers must be protected and treated with special care:

1. Names
2. Geographical identifiers (smaller than state; for example, a street address)
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. Email Addresses
7. Social Security Numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web addresses
15. Internet Protocol (IP) addresses
16. Biometric identifiers (including finger, retinal and voice prints)
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code

Protecting the Privacy and Security of Confidential Information

How do I safeguard confidential information and resources?

Access to information systems and applications is granted based on an employee's current job duties.

- You've been assigned a unique "User ID" to access the information you need to perform your current job duties.
- Your supervisor's approval is required to change your access level.
- You are responsible for anything and everything that happens under your User ID.
- Do NOT share your password.

Protecting the Privacy and Security of Confidential Information

How do I safeguard confidential information and resources?

DO access only the information you need to perform your job at the time of the access.

DO always lock or logoff your account once finished and whenever you step away from the computer.

DO always request visitors to step out of the room prior to discussing patient information.

DO verify accuracy of all documents before handing to another person or faxing/mailing.

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

How do I safeguard confidential information and resources?

DON'T access information for immediate family members, unless a signed consent form is on file. The consent form is located on the web page for HIM (Medical Records) on the employee intranet. The consent form is only applicable to immediate family members.

DON'T access more information than you need to perform your job. YOU have a DUTY to NOT review or obtain confidential information that you have access to if you do NOT have a specific need to know that information to perform your job!

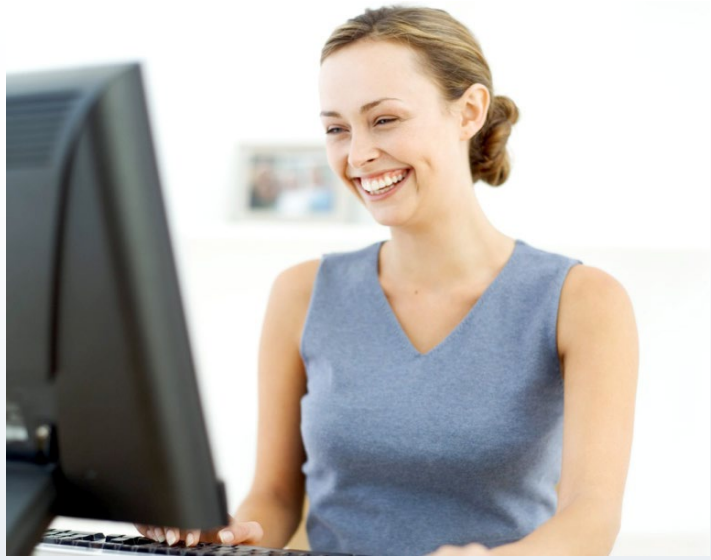
DON'T print your own medical record information.

DON'T post patient or confidential information on social media sites.

LVHN colleagues may sign up to access their own medical information through myLVHN portal.

Accessing confidential information without a business or clinical need to do so may result in *termination*.

Accessing Information Remotely



LVHN remote access is authorized for business use only.
All users must be uniquely identified.

When working from a "remote" location (not a LVHN site):

- **DO** practice safe "physical" security to safeguard equipment and protect confidential information.
- **DO** only print from remote locations when it is urgent or necessary to support patient care or LVHN business.
- **DO NOT** discard confidential information in public places (such as garbage cans or recycle bins)

Protecting the Privacy and Security of Confidential Information

Protect your passwords!

You are not allowed to share your password or use someone else's password under ANY circumstances.

DO change your password if:

- You have accidentally or inadvertently shared it.
- Any device you use is misplaced, lost, or stolen.
- You believe your password may have been compromised.

- **DON'T** record your password in a readable format (by writing it on paper or typing it on a computer or other device) where someone else can access it.
- **DON'T** enable the "remember me" or "save password" option, even if prompted.

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

Encryption

What is Encryption?

How Does it Work?

Encryption is a process used to keep confidential information safe & secure.

Lehigh Valley Health Network "encrypts" its computers and all files transferred to USB devices.

Always encrypt emails and other documents when sending confidential information outside LVHN. Type encrypt# or Encrypt# anywhere in the e-mail message body.

Additional information for email encryption can be found on the Technology Security and Risk Management Intranet page.

Protecting the Privacy and Security of Confidential Information

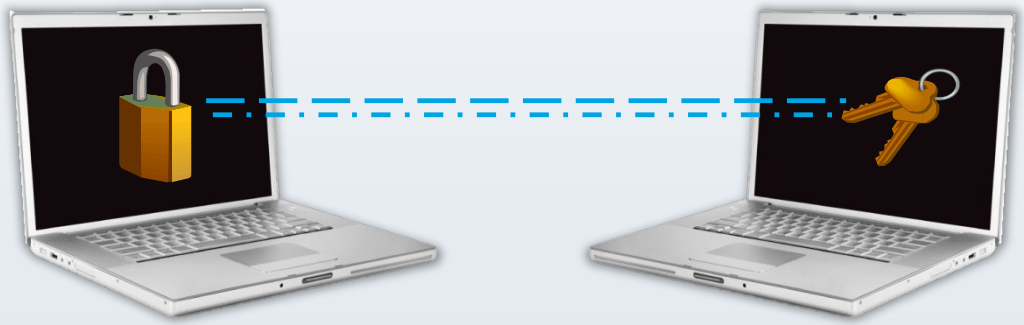
Why? | What? | How? | When? | Where?

Encryption

What is Encryption?

How Does it Work?

When you Encrypt data or text, it is "scrambled" into an unreadable form (like a code) and you - or the person or company receiving it - must have a way (a "key" or password) to unscramble it.



Use internet, email and instant messaging appropriately

These are communication tools intended for business use.

Acceptable use of the internet, email and instant messaging is monitored to ensure that these tools are not misused or overused.

If you need to send confidential information for business purposes only, use approved secured method to ensure that it is encrypted and sent securely. For assistance, please contact the Technology Support Center at 610-402-8303.

NEVER forward a message containing PHI to your personal email account, because your own account is NOT properly encrypted.

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

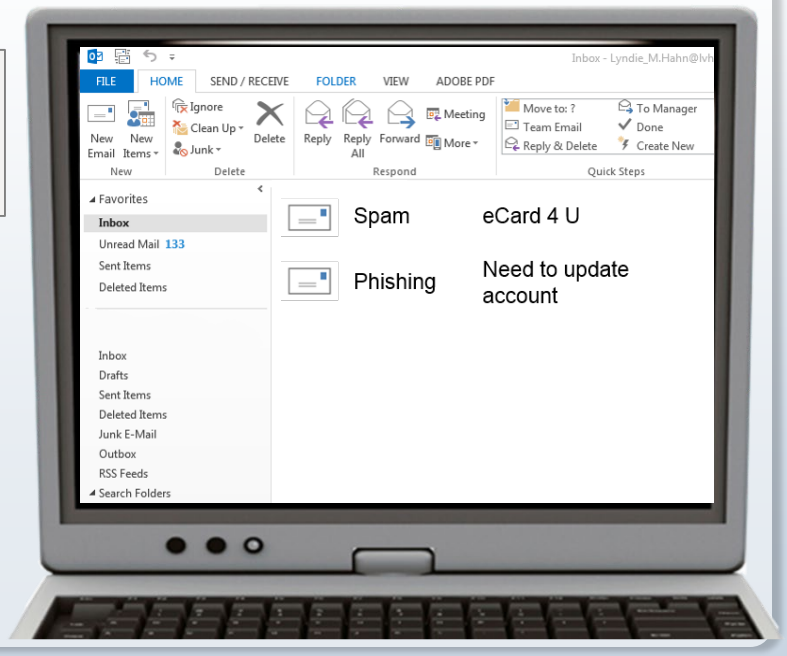
Email Safety

Spam | Phishing

Criminals often use email scams in an attempt to trick users, steal information, and infect computers with viruses. LVHN Technology Support Center staff will never ask you for your password. **DO NOT** share your passwords with anyone, even if asked.

If you receive a suspicious email, the preferred method is to click on the "**Report Suspicious Email**" button, found in the Outlook "Home" toolbar.

If you do not have this button, you can forward suspicious emails to spam@lvhn.org, and delete the email from your inbox. Two examples of email scams are Spam and Phishing.



Protecting the Privacy and Security of Confidential Information

Email Safety

Spam | Phishing

Spam emails are junk mail messages that will often ask you to click on a link or open an attachment. Clicking the link or opening the attachment will provide a pathway for your computer to become infected with a virus or spyware. Criminals may then be able to steal your password and access information stored on your computer.

You should never open attachments or click links in emails from senders you do not know. Do not open attachments that you are not expecting or that seem suspicious.

If you do inadvertently click on a link in a spam message, notify the LVHN Technology Support Center immediately. (610-402-8303)

Protecting the Privacy and Security of Confidential Information

Email Safety

Spam | Phishing

In **phishing scams**, criminals try to trick you into providing secure information such as your Social Security number or bank account number. For example, it might be an email or phone call from a trusted entity such as your bank or government agency that appears to be official.

You should never respond to emails or phone calls that ask you to provide any type of information. Businesses do not request this type of information through email or phone calls.

If you do inadvertently respond to a phishing message, notify the LVHN Technology Support Center immediately. (610-402-8303)

Protecting the Privacy and Security of Confidential Information

You MUST secure information and resources!

You are responsible for the safety and security of any computer you are using, regardless of your location (including software and confidential information within it).

This means that you must protect it from:

- Loss, theft, damage or unauthorized access
- Displaying Confidential Information to unauthorized viewers
- Malicious software (i.e. viruses)

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

Security tips:

DOs

- Dispose of paper in designated locked bins.
- If you must travel with LVHN computer equipment, confidential papers, or mobile devices, take them into your residence (home, hotel, etc…) every night.
- Change your password frequently.
- Lock or Logoff when you step away from your workstation.
- Protect our patients', our colleagues', and our network's confidential information by NEVER posting it on the internet, including social media sites.

DON'Ts

- Don't ever leave a laptop, mobile device, or confidential information in plain sight inside a vehicle.
- Don't share your password with anyone, even if asked to do so.
- Don't share personal information through the internet, email or instant messaging.
- Don't respond to spam emails (unsolicited emails from a source you don't know and trust) or phishing scams.
- Don't use another person's logon or user ID under <u>any</u> circumstances.

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

Report a concern about a potential breach of privacy or security of confidential information as soon as it is brought to your attention.

To report concerns related to misplaced, lost, or stolen devices:

- Report to your Supervisor, or
- Call the LVHN Technology Support Center (610-402-8303)

To report concerns related to how PHI is accessed, used, shared or disposed of:

- Report to your Supervisor, or
- Call the LVHN Privacy Officer (610-402-9100)
- Report through the Compliance Hotline (877-895-2905 or lvhn.ethicspoint.com)

To report security concerns contact IS_SecAdministration@lvhn.org

Report ANY concerns about a potential breach of information privacy or security immediately!

Protecting the Privacy and Security of Confidential Information

Where can I find important policies on the intranet?

- **Code of Conduct**
- **Compliance Policies and Procedures**
- **Security Risk Management**

Code of Conduct

Each year, you (electronically) sign a Confidentiality Agreement that outlines some of your key responsibilities for safeguarding confidential information.

You also (electronically) sign a Code of Conduct Acknowledgement to indicate that you have read or will read the **LVHN Code of Conduct** AND that you agree to follow the Code.

The **LVHN Code of Conduct** can be found in the Corporate Compliance folder in Policy Tech.

Protecting the Privacy and Security of Confidential Information

Where can I find important policies on the intranet?

- Code of Conduct
- Compliance Policies and Procedures
- Security Risk Management

To find the LVHN Compliance and HIPAA policies open Policy Tech from your SSO Toolbar, and navigate to the Corporate Compliance folder.

- Policies that pertain to protecting the privacy and security of our patients' protected health information begin with "**HIPAA**".

Protecting the Privacy and Security of Confidential Information

Where can I find important policies on the intranet?

- Code of Conduct
- Compliance Policies and Procedures
- Security Risk Management

Additional information and FAQs pertaining to Security Management can be found on the Technology Security and Risk Management Intranet Page.

Protecting the Privacy and Security of Confidential Information

Why? | What? | How? | When? | Where?

Reviewing the Compliance Policies (including HIPAA Policies)

REMEMBER, these policies are updated when the laws and regulations change.

You are responsible for reading these policies, reviewing them on a regular basis, and referring to them whenever you have a need to do so!

Protecting the Privacy and Security of Confidential Information

You should now be able to:

- Explain the fundamental purpose of Lehigh Valley Health Network's Privacy & Information Security Program
- Describe key actions every employee is expected to take to safeguard confidential information and all resources
- Know where to locate network privacy and information security policies on our intranet