Protecting the Privacy and Security of Confidential Information
Annual Compliance Training
## Course Information

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Protecting the Privacy and Security of Confidential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulations/Standards</td>
<td>US Department of Health and Human Services Office for Civil Rights (OCR)</td>
</tr>
<tr>
<td>Approximate Time to Complete</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Intended Audience</td>
<td>All LVHN employed staff</td>
</tr>
<tr>
<td>Technical Specifications</td>
<td>Flash player 11, Internet Explorer 11.</td>
</tr>
<tr>
<td>Date Revised</td>
<td>August 2016</td>
</tr>
</tbody>
</table>

## Contact Information

Please forward any content questions or concerns to the Subject Matter Expert: Melissa Blihar 484-884-1410

Please call the Help Desk at 610-402-8303 with any technical issues.

This course does not contain audio.
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 Information Systems (IS) resources
- Know where to locate network privacy and information security policies on our intranet
Protecting the Privacy and Security of Confidential Information

- **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?

Questions asked and answered during this course:
Protecting the Privacy and Security of Confidential Information

Why is this Privacy & Security Course required?

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

Government regulations require healthcare organizations to have Privacy and Security policies and procedures in place and to provide training to all employees on a regular basis.

Not only is it important to protect our patients' confidential information, but it's the law!
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect sensitive patient information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened when the American Recovery and Reinvestment Act was passed. This law is referred to as the HITECH Act (Health Information Technology for Economic and Clinical Health).

In 2013, the Omnibus Final Rule made significant changes to enhance the HIPAA privacy and security rules.
Protecting the Privacy and Security of Confidential Information

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
Protected Health Information (PHI)

PHI can be verbal (spoken) or written (either on paper or in electronic form).

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

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

**Why?**
- Protecting personal information is a legal requirement (HIPAA).

**What?**
- Protecting the privacy and security of Confidential Information.

**How?**
- **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.

**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.

**How do I safeguard confidential information and IS 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.

**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.

**Accessing confidential information without a business or clinical need to do so will result in termination.**
Protecting the Privacy and Security of Confidential Information

Accessing Information Remotely

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** print confidential information from remote locations.
- **DO NOT** discard confidential information in public places (such as garbage cans or recycle bins).

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

Contact the IS department if you use devices that are not owned or issued to you by LVHN to access, process, save or relocate confidential information. They can assist you with options to safeguard the information stored on those devices.
Encryption

**What is Encryption?**

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.

**How does it work?**

For more information, see the IS Security Management intranet page.
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 information services.

NEVER forward a message containing PHI to your personal email account, because your own account is NOT properly encrypted.
Criminals often use email scams in an attempt to trick users, steal information, and infect computers with viruses. LVHN technical support staff will never ask you for your password. **DO NOT** share your passwords with anyone, even if asked.

If you receive a suspicious email you should forward the email to Spam@lvh.com and delete the suspicious email from your inbox.

Two examples of email scams are Spam and Phishing. Click on the tabs above to learn more.
Email Safety

**Spam**

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 help desk immediately. (610-402-8303)
In phishing scams, you will receive an email that appears to be official. For example, it may look like an email sent from your bank, or some other type of account, or even from the government. However, the email is not real.

In phishing scams, criminals try to trick you into providing secure information, such as your social security number or bank account number.

You should never reply to an email like this or provide any type of information. Businesses do not request this type of information through email.

If you do inadvertently respond to a phishing message, notify the LVHN help desk immediately. (610-402-8303)
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?**
- 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.

**What?**

**How?**

<table>
<thead>
<tr>
<th>Security tips:</th>
<th>DOs</th>
<th>DON'Ts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dispose of paper in designated locked bins.</td>
<td>Don’t ever leave a laptop, mobile device, or confidential information in plain sight inside a vehicle.</td>
</tr>
<tr>
<td></td>
<td>If you must travel with LVHN computer equipment, confidential papers, or mobile devices, take them into your residence (home, hotel, etc...) every night.</td>
<td>Don’t share your password with anyone, even if asked to do so.</td>
</tr>
<tr>
<td></td>
<td>Change your password frequently.</td>
<td>Don’t share personal information through the internet, email or instant messaging.</td>
</tr>
<tr>
<td></td>
<td>Lock or Logoff when you step away from your workstation.</td>
<td>Don’t respond to spam emails (unsolicited emails from a source you don’t know and trust) or phishing scams.</td>
</tr>
<tr>
<td></td>
<td>Protect our patients', our colleagues', and our network’s confidential information by NEVER posting it on the internet, including social media sites.</td>
<td>Don’t use another person’s logon or user ID under any circumstances.</td>
</tr>
</tbody>
</table>
Protecting the Privacy and Security of Confidential Information

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 Help Desk (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)

To report security concerns contact IS_Securityadmin@lvhn.org

Report ANY concerns about a potential breach of information privacy or security immediately!
Protecting the Privacy and Security of Confidential Information

Why?
What?
How?
When?
Where?

Where can I find important policies on the intranet?

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 Code of Conduct can be found in Policy Tech.
Where can I find important policies on the intranet?

To find the LVHN Compliance and HIPAA policies open Policy Tech from your SSO Toolbar.
- Policies that pertain to protecting the privacy and security of our patients' protected health information begin with "HIPAA".
Where can I find important policies on the intranet?

For additional information and FAQs pertaining to Security Management:
1. Select the "Technology" tab on the intranet home page
2. Click "IS Security Management"
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!
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 Information Systems (IS) resources
- Know where to locate network privacy and information security policies on our intranet

Ready to test your knowledge?
You have successfully completed
Protecting the Privacy and Security of Confidential Information
You can close the window to exit the course.