HIPAA

Health Insurance Portability and Accountability Act

FY13 Core Training

The **Health Insurance Portability and Accountability Act**, or HIPAA, is a federal law that regulates the privacy and security of health information.

The law focuses on maintaining confidentiality, respecting a patient's rights to privacy, and protecting patient information.

Click next to continue

Course Information

Course Title:	HIPAA
Regulations / Standards:	HIPAA
Approximate Time to Complete:	25 minutes
Intended Audience:	All LVHN employed staff
Technical Specifications:	Flash player 9. Internet Explorer 6.
Date Revised:	August 2012

Contact Information

Please forward any content questions or concerns to the Subject Matter Expert:	Carol Kriebel at 610-969-0501

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

This course does not contain audio.

Objectives

Lehigh Valley Health Network is committed to protecting the health information of our patients.

As an LVHN employee, you should be familiar with the HIPAA requirements. It is the responsibility of all LVHN employees to protect our patients' privacy and confidentiality and maintain network security.

Upon completion of this course, you should be able to:

- Describe three ways in which you can protect a patient's PHI
- Identify four examples of PHI
- Describe two measures you can take to enhance network security

Are you ready to test your knowledge?

To test your knowledge, you can click the **"Demonstrate Knowledge"** button to move to the final test.

Demonstrate Knowledge

Consent and Privacy

HIPAA does not require the patient's consent *to allow healthcare providers and plans to use health information* ***for ordinary treatment purposes.***

All patients must sign the "Consent to Treatment" form

This form gives permission to the hospital and staff to use health information to care and treat the patient.

As a general rule, HIPAA does not require the patient's consent to allow healthcare providers and plans to use health information for ordinary treatment purposes. Most people understand and expect that health information will be shared in order to provide treatment and care.

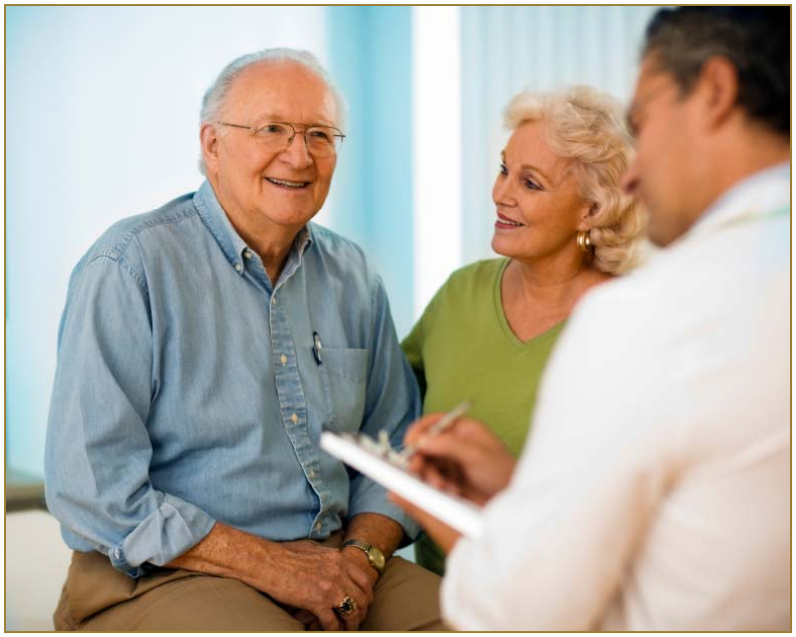
Privacy Rule

HIPAA restricts how health information can be used and disclosed.

Healthcare providers must take reasonable measures to protect the privacy and security of patients' health information. The Privacy Rule gives patients and personal representatives rights concerning their health information and outlines the requirements for the use and disclosure of protected health information (PHI).

LVHN is required to explain to patients how their protected health information is used and disclosed. The "Health Information Privacy Notice", which is given to all patients, summarizes how protected health information is used and disclosed.

The Privacy Rule also requires that LVHN provide training to all staff on good privacy practices. This training fulfills that requirement.



Personal Representative:

A personal representative is a person who is able to inspect and receive a copy of your Protected Health Information. Examples of personal representatives include a parent of a child, a person who has health care power of attorney for you, etc.

Protected Health Information

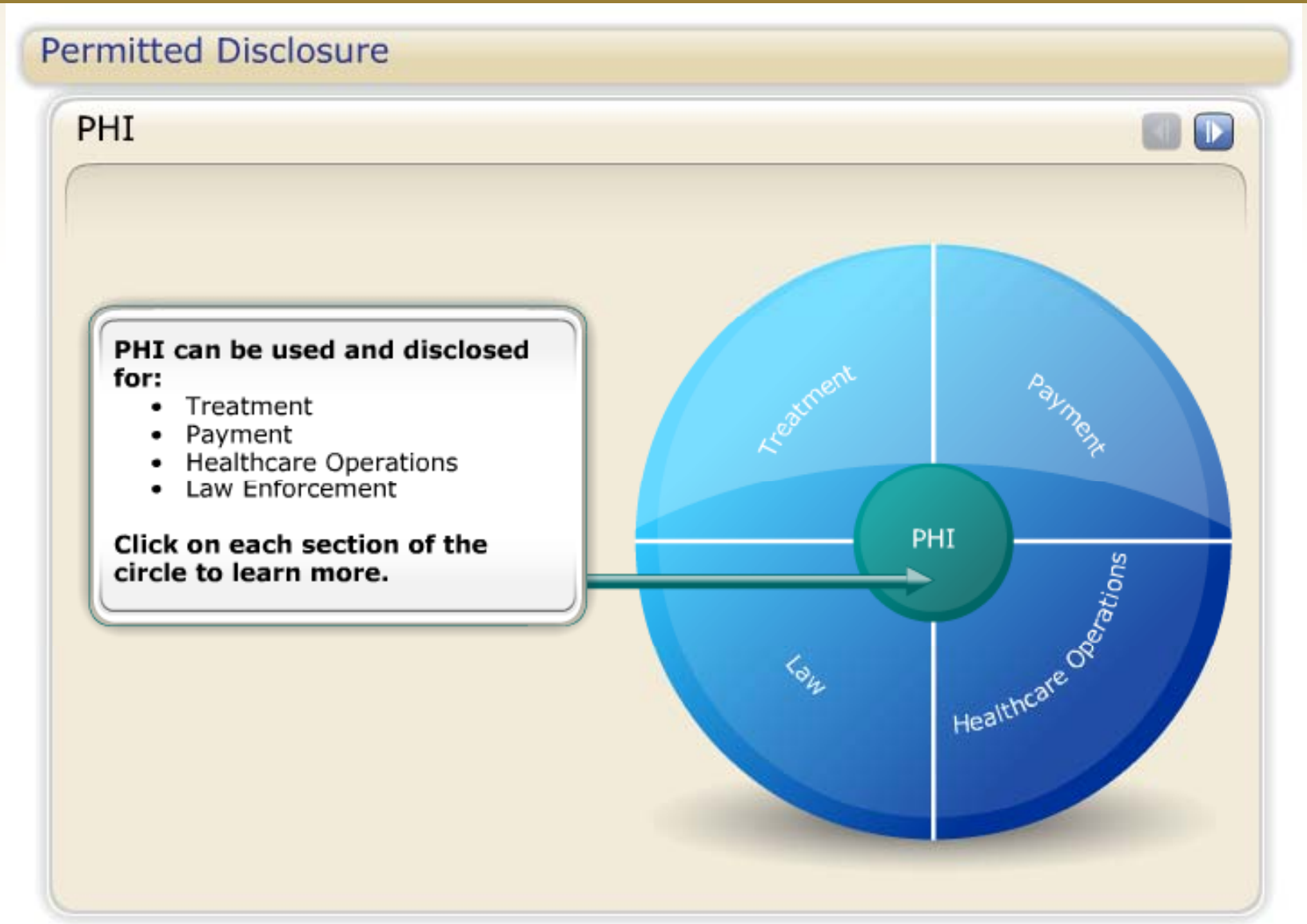
Protected Health Information (PHI) -

PHI is any information that can be used to identify an individual or any information that can be used with other available information to identify an individual. Protected Health Information is information about a person's health condition or care, including billing and payment information. This information may be in written format, may be electronic, or may be spoken.

Examples of PHI:

- Census sheet
- Billing information
- Medical records
- Mail identifying patient rooms
- Information in the computer systems
- Conversations related to patient care and treatment
- Photographs

Permitted Disclosure



Treatment

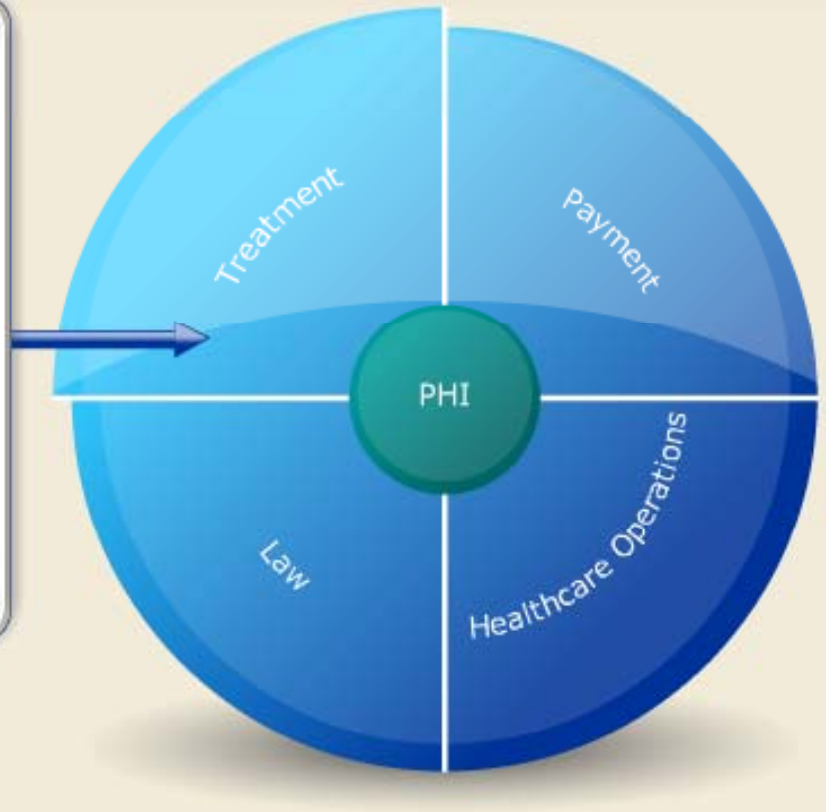
Permitted Disclosure

Treatment

Health information may be shared and used for **treatment and care**.

- A physician may access the medical record to treat a patient
- A nurse may consult with another nurse related to a patient's care

HIPAA does not restrict the amount of information that can be disclosed as long as the information is being used for treatment purposes.

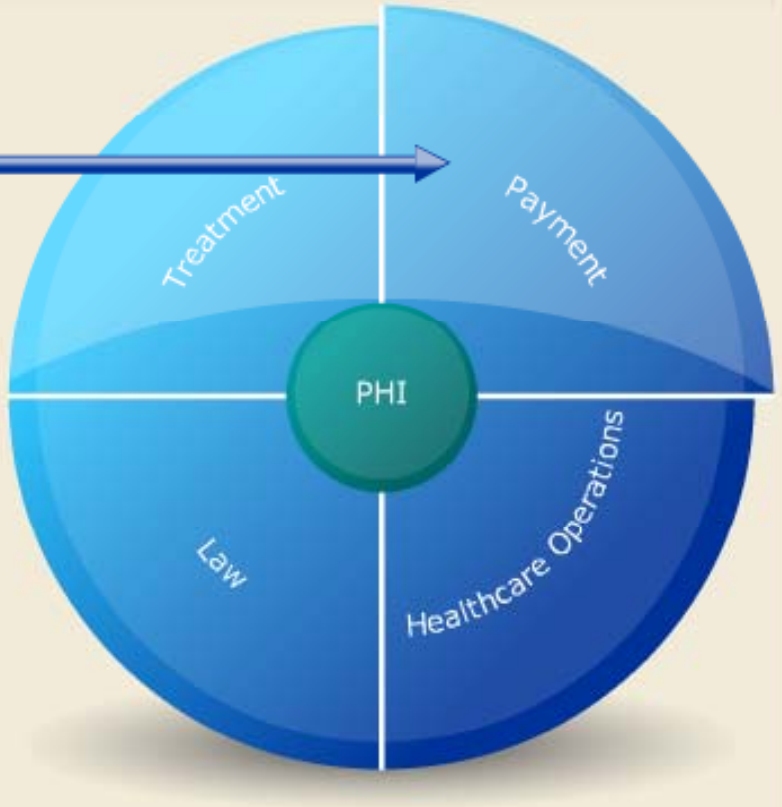


Payment

Permitted Disclosure

Payment

Lehigh Valley Health Network may use and disclose Protected Health Information to obtain or make **payment** for healthcare without the permission of the patient.



Healthcare Operations

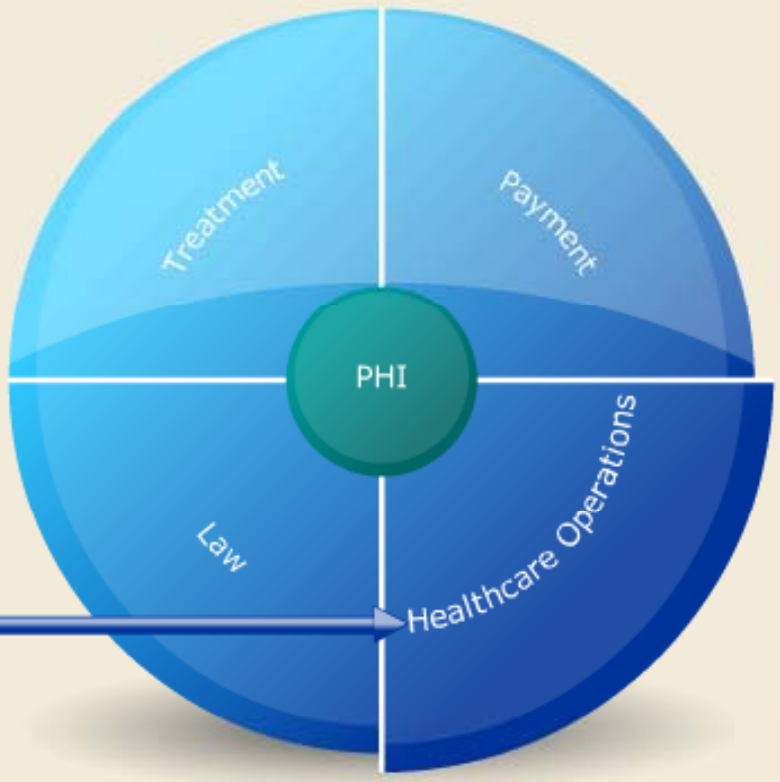
Permitted Disclosure

Healthcare Operations

Lehigh Valley Health Network may use and disclose PHI for healthcare operations.

Healthcare operations include:

- billing
- accounting
- quality assessment and improvement
- business planning



Law

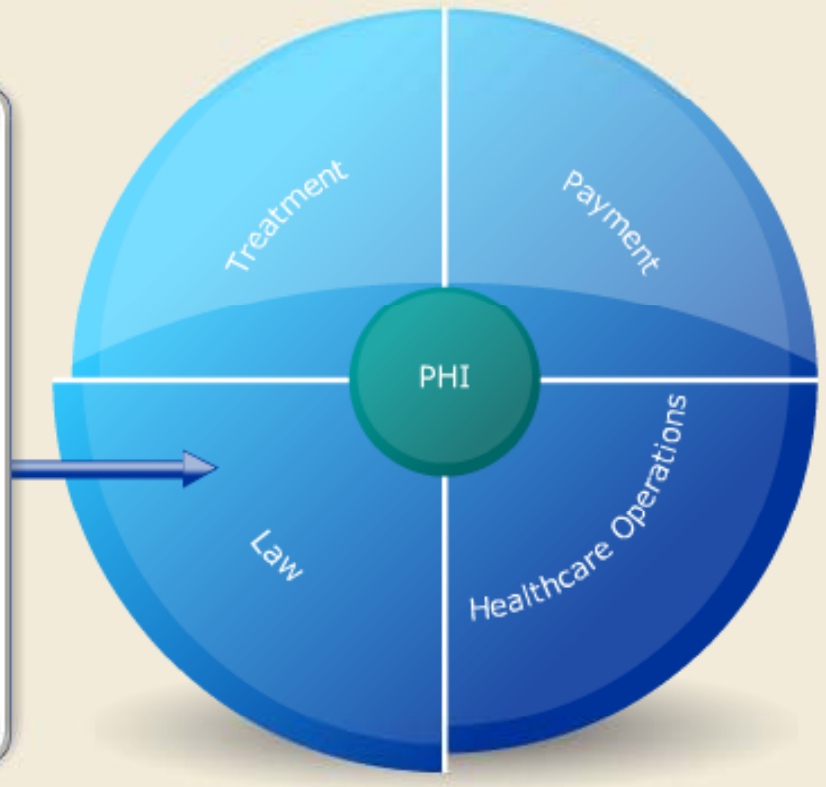
Permitted Disclosure

Law

Protected Health Information may also be used when **required or permitted by law**.

This includes:

- Disclosures of information to participate in a government payment program, such as Medicare
- Disclosures about victims of domestic abuse or domestic violence
- Disclosures required by a court or grand jury or for administrative proceedings
- Disclosure for law enforcement purposes



Disclosure to Family and Friends

Health information is often shared with the patient's family and friends involved in the patient's healthcare.

Before health information can be shared, the patient must have the chance to object to the disclosure. If the patient is not present or is unconscious, the provider may make the disclosure if he or she believes that it is in the patient's best interest.

Information should be limited to what the family or friends need to know.

Examples:

- A pharmacist gives a prescription to a patient's husband
- Family members waiting outside the ER are told about a patient's condition
- Parents are given information about their ill child

Authorization

PHI can't be used for:

- Marketing
- Research
  - PHI can only be used for research if authorization is waived by an Institutional Review Board.

If you are unsure whether or not PHI can be disclosed, **ask the patient to sign an authorization form**. PHI can be used for treatment, payment, healthcare operations and when required by law. Any other use or disclosure of PHI requires a written authorization form.

Authorization form:

The authorization form must include:

- A description of the information to be used or disclosed
- Who may use or disclose the protected health information
- To whom the PHI may be disclosed
- The purpose of the use or disclosure

The authorization form must be signed and dated and it must expire on a specific date or event. The patient may decide to revoke authorization at any time.

What Do You Think?

A doctor shares health information with a nurse so she can provide care to the patient.

Is this an acceptable use of protected health information?

Yes

No

What Do You Think?

A doctor shares health information with a nurse so she can provide care to the patient.

Is this an acceptable use of protected health information?

Yes

No

Yes - Protected health information can be used to care and treat patients. This is an acceptable use of PHI.

Continue

What Do You Think?

A nurse tells a nurse who works on another unit that her neighbor is in the hospital for surgery.

Is this an acceptable use of protected health information?

Yes

No

What Do You Think?

A nurse tells a nurse who works on another unit that her neighbor is in the hospital for surgery.

Is this an acceptable use of protected health information?

Yes

No

No – This is not an acceptable use of the patient's health information. The other nurse is not part of the patient's care.

Continue

What Do You Think?

A pharmacist gives a patient's husband her prescription.

Is this an acceptable use of protected health information?

Yes

No

What Do You Think?

A pharmacist gives a patient's husband her prescription.

Is this an acceptable use of protected health information?

Yes

No

Yes – This is acceptable. The pharmacist can give the patient's husband her prescription.

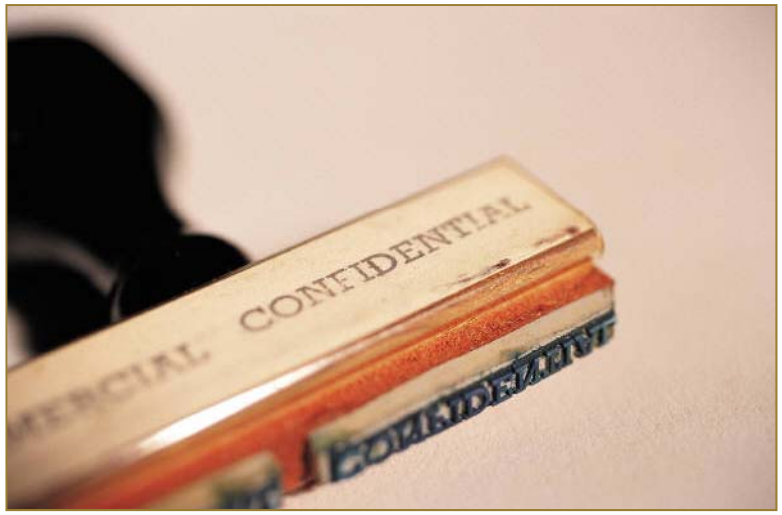
Continue

Confidentiality

At LVHN every employee, member of the medical staff, volunteer, intern, student, contractor and vendor must sign a confidentiality statement.

This statement is signed upon employment and is then signed annually.

You need to be aware of what this agreement says and what is expected of you. It is the policy of LVHN to protect confidential information. Unauthorized disclosure of confidential information is not allowed. By signing the acknowledgement of confidentiality statement, you are promising to protect patient information.



To read more about LVHN's confidentiality policy click here

As part of this training bundle you will be asked to read and electronically sign the Acknowledgement of Confidentiality.

Maintaining Confidentiality

Sharing information inappropriately can result in suspension or termination!

You must take reasonable measures to protect health information of our patients. Do not share patient information with anyone outside of work regardless of the situation. Work related activities should stay at work.

Employees should NOT:

- Disclose, discuss or release patient information to anyone at or outside work EXCEPT to carry out regular duties assigned. The fact that a patient is here at LVHN is confidential.
- Share or disclose any computer systems username or password to anyone.
- Seek or use confidential information for personal gain or pass it on to any person outside LVHN, including family and friends, or even to other employees who do not need to know such information to carry out their duties.
- Remove confidential data from the facility.

Accessing Information

Confidential information can only be accessed:

- If it is required to perform your job
- If you are accessing your own Protected Health Information (PHI)
  - If your own medical records contain sensitive information (such as behavioral health or mental health issues) you must contact health information management to get physician approval before accessing your records.
- If you are accessing PHI of an immediate family member with their permission by having a signed HIPAA consent form on file

You may NOT access information for other employees.

You may NOT print or transfer your own or your family member's health information.

Violating the Policy

Disciplinary Actions:

- If you print, download, or transfer your own medical record out of the Network database, you will receive a final warning for the first offense.
  - **If the offense occurs again you will be fired.**
- If you access an immediate family member's record without a signed Consent form on file, you will receive a warning for the first offense if the family member verifies you had permission to access the information.
  - **If the offense occurs again you will be fired.**
  - **If the family member states they did not give permission for you to access their medical record, you will be fired on the first offense.**
- If you access third party (non-immediate family, friends, neighbors, co-workers, etc.) health information without a job or treatment reason you will be fired.

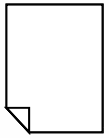
Any offense may also result in loss of medical staff or Allied Health Professional Privileges.

Do Not Announce

The Do Not Announce Policy refers to **excluding information regarding a patient's presence at LVHN** from the public information patient directory, either by request of the patient or by their medical condition.

The patient's presence will not be acknowledged to the public, including family and friends. Mail, flowers and visitors will all be refused.

Do Not Announce is established during the admission process. If the patient elects not to authorize the release of information, the "Do Not Announce" flag is denoted as a "Y" in the clinical census screen. A patient can request discontinuation of the "Do Not Announce" status at any time.



Click here to read the "Do Not Announce" Policy

The Do Not Announce Policy can also be found in the Administrative Policy Manual on the LVHN intranet

It is important to determine whether the patient is a "Do Not Announce" before releasing any information to the public or family and friends.

Security Rule

Electronic information must be secure and confidential.

We use computers to store electronic patient records, billing information, operational data and other confidential LVHN information.

All users must follow computer security measures to maintain the privacy of electronic information.

The **HIPAA Security Rule** controls how we maintain the privacy of electronic healthcare information. The HIPAA Security Rule contains rules for user accounts, computer passwords and network security.

User Accounts

You are forbidden to share computer accounts with others.
Only under very rare circumstances and emergency situations is the sharing of user account information acceptable.

Every person at LVHN has a unique user account.

User accounts help to secure information by ensuring that only certain people have access to our computer network. User accounts also enable us to track account activity. HIPAA requires tracking of who sees medical data.

Passwords

Passwords

Don't

Do

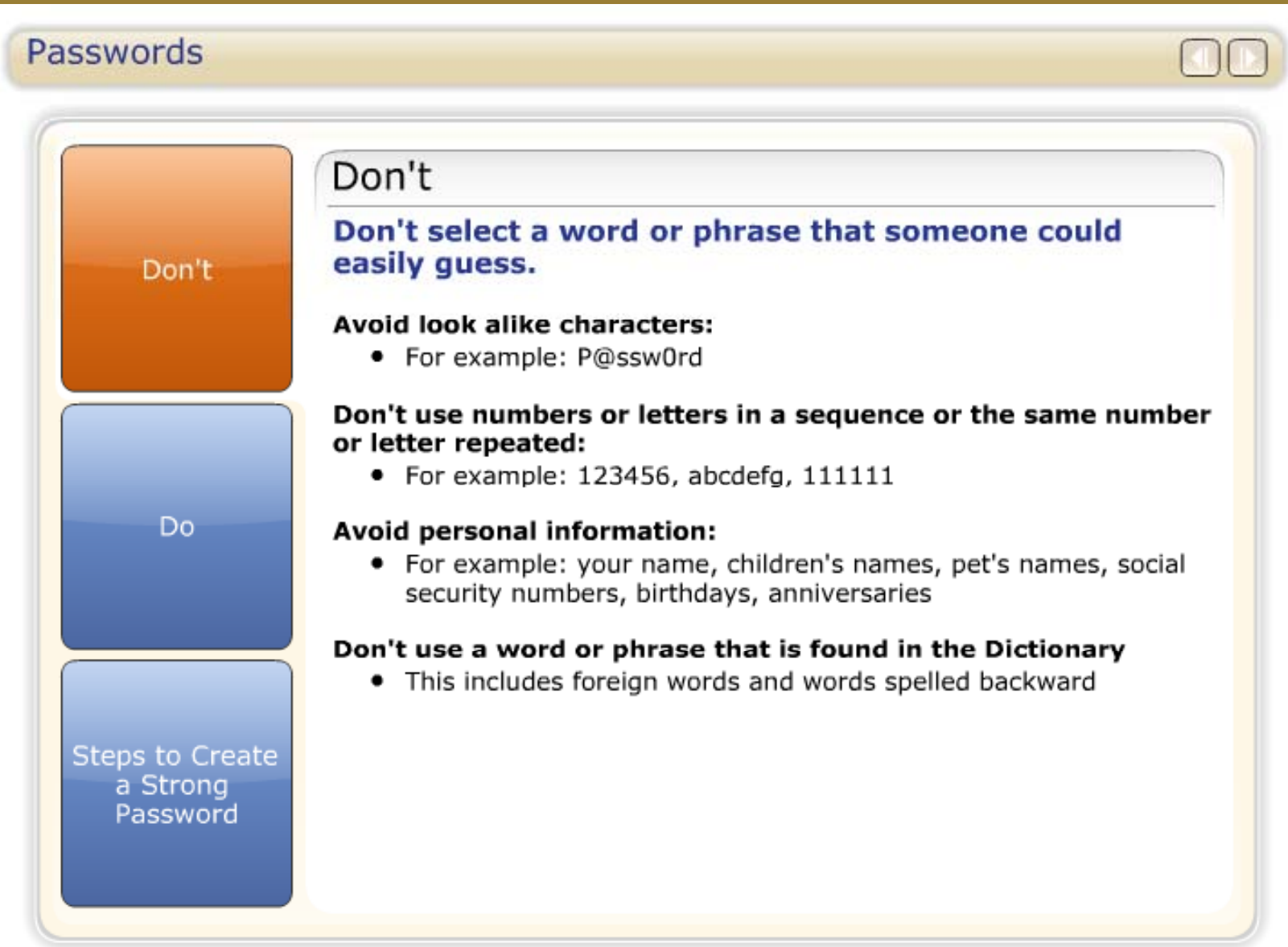
Steps to Create a Strong Password

Passwords

Passwords help to keep other users and computer criminals out of your computer account. To be sure that your account is secure, you need to create good passwords.

What is a good password? **Click the buttons** to learn more about creating passwords.

Don’t


Passwords
Don't
Do
Steps to Create a Strong Password
Don't
Don't select a word or phrase that someone could easily guess.
Avoid look alike characters:
For example: P@ssw0rd
Don't use numbers or letters in a sequence or the same number or letter repeated:
For example: 123456, abcdefg, 111111
Avoid personal information:
For example: your name, children's names, pet's names, social security numbers, birthdays, anniversaries
Don't use a word or phrase that is found in the Dictionary
This includes foreign words and words spelled backward

Do

Passwords

Don't

Do

Steps to Create a Strong Password

Do

The more complex a password is, the more difficult it will be for someone to guess.

Do use a combination of:

- Letters
- Upper and lower case letters
- Numbers
- Symbols

Create a Strong Password

Passwords

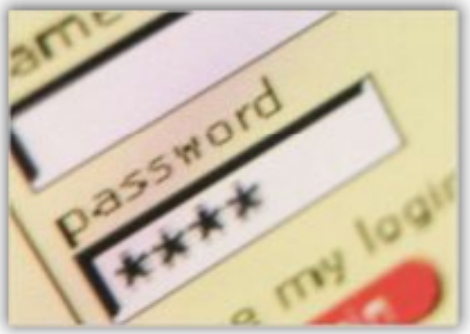
Don't

Do

Steps to Create a Strong Password

Steps to Create a Strong Password

1. Think of a sentence or phrase.
   Hint: Choose something that is easy for you to remember, but difficult for someone else to guess. Think of your favorite book, movie or hobby.
2. Turn the phrase into a password.
3. Use upper and lower case letters.
4. Add complexity with numbers and symbols



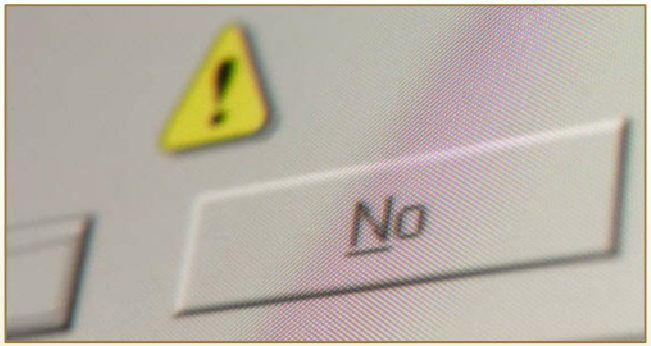
Computer Security Tips

Do:

- Change passwords frequently
- Lock your computer when you are away from your desk.
  - Set a screensaver to automatically lock your computer after the computer has been inactive for a certain length of time.
- Log off from your computer when you are done using it.
- Use different passwords for different applications.

Don't:

- Don't write down passwords. If you must write down your passwords, make sure that they are stored in a secure location. Never leave the passwords in a location where others could easily see them or find them! Don't store your passwords electronically either. If a hacker does get into your computer, then they will be able to find all of your passwords.
- Don't share passwords with others.
- Do not allow others to use your account.



Network Security

Lehigh Valley Health Network has put into practice computer network security measures to protect our computers from viruses, spyware and criminals.

Security prevents users from accessing websites that frequently contain harmful software and content that is inappropriate for the workplace.

Records are kept of all computer activity and alarms are triggered when bad activity is detected.

LVHN computers are for work purposes only!

While logged into the network do not visit sites that are inappropriate for the workplace. This includes personal shopping websites.

Email

Email

Introduction

Email should only be used for business purposes. You should be aware that criminals often use email scams in an attempt to trick users, steal information, and infect computers with viruses.

Two examples of email scams are **Spam** and **Phishing**.

Click the bars to learn more about these scams and email safety.

Spam

Phishing

Email Safety Tips

Spam

Email

Introduction

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 infect your computer with a virus or spyware. Criminals may then be able to steal your passwords and access information stored on your computer.

You should never open attachments from senders you do not know or open attachments that you are not expecting.

Phishing

Email Safety Tips

Phishing

Email

Introduction

Spam

Phishing

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 them with any type of information. Businesses do not request this type of information through email.

Email Safety Tips

Email Safety Tips

Email

Introduction

Spam

Phishing

Email Safety Tips

To protect your information and patient information, remember these email safety tips:

- Never email patient information without IS review of the security
- Never give out personal information
- Call banks to confirm email requests
- Do not click links in emails from unknown senders
- Do not open email attachments that you are not expecting

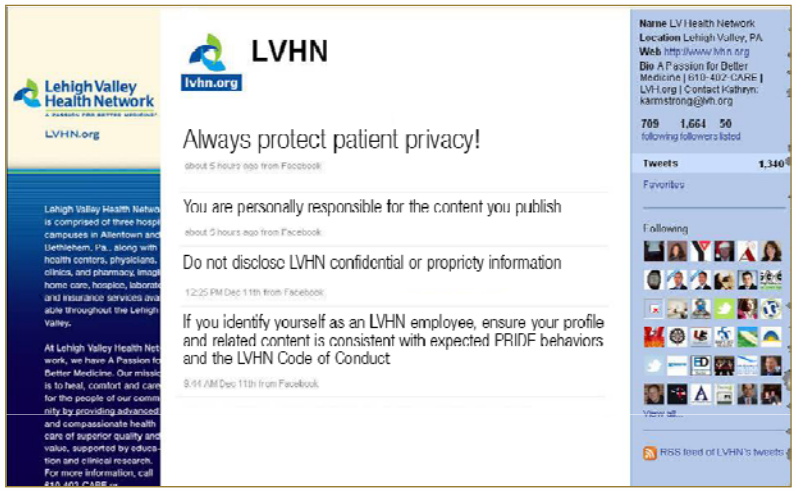
Social Media

Social media is used to share professional opinions, insights, experiences and perspectives. Some popular examples include:

- Facebook
- Flickr
- Twitter
- YouTube

Along with the many benefits of these technologies also comes a greater need to use these tools responsibly, respectfully and safely.

Social Media Behavior



If your behavior or conduct is inconsistent with LVHN standards, it reflects poorly on our Network and disciplinary action will be taken.

Click here to review the LVHN
"Social Media Participation" policy

When you send messages electronically, you are being judged solely on your written word.

It is important to be very careful of the contents of the message you are sending.

- You must always protect patient privacy
- You are personally responsible for the content you publish
- Do not disclose LVHN confidential or proprietary information
- If you identify yourself as an LVHN employee, ensure your profile and related content is consistent with expected PRIDE behaviors and the LVHN Code of Conduct

Termination Offenses

Inappropriate use of LVHN's computer network may result in termination.

Employees CAN NOT:

- View pornographic websites
- Download or use computer hacking tools
- View patient records without authorization

If an employee is caught doing any of these activities, he or she may be disciplined and/or terminated. Other inappropriate uses of LVHN computers may also result in employee termination.

Ready to Test Your Knowledge?

You should now be able to:

- Describe three ways in which you can protect a patient's PHI
- Identify four examples of PHI
- Describe two measures you can take to protect network security

If you are ready to take the final test, click the test button below.

You must earn a score of at least 80% to successfully complete the course.

Test