Identity Theft Prevention Program
FY17 Core Training
# Course Information

<table>
<thead>
<tr>
<th><strong>Course Title:</strong></th>
<th>Identity Theft Prevention Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulations/Standards:</strong></td>
<td>Federal Trade Commission (FTC) Identity Theft Training Requirements</td>
</tr>
<tr>
<td><strong>Approximate Time to Complete:</strong></td>
<td>15 minutes</td>
</tr>
<tr>
<td><strong>Intended Audience:</strong></td>
<td>All LVHN employed staff</td>
</tr>
<tr>
<td><strong>Technical Specifications:</strong></td>
<td>Flash player 11. Internet Explorer 11.</td>
</tr>
<tr>
<td><strong>Date Revised:</strong></td>
<td>August 2016</td>
</tr>
</tbody>
</table>

## Contact Information

**Please forward any content questions or concerns to the Subject Matter Expert:** Janet Palmer 484-884-0131

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

*This course does not contain audio.*
Objectives

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

• Explain the purpose of the LVHN Identity Theft Program
• Define medical identity theft
• List three consequences of identity theft
• List precautions that individuals can take to avoid identity theft
• Identify the appropriate information that should be obtained to verify patient identity and four acceptable forms of identification
• Identify the four categories of red flags for identity theft in healthcare
In January 2008, the Federal Trade Commission (FTC) issued a set of regulations requiring certain organizations to develop a written program to identify the warning signs – or red flags – of identity theft.

The purpose of the Identity Theft Prevention Program at Lehigh Valley Health Network is to detect, prevent, decrease, and respond to identity theft.

LVHN’s Identity Theft Prevention Program follows the guidelines issued by the FTC and the Fair and Accurate Credit Transactions (FACT) act.
Identity Theft:
Fraud committed or attempted using the identifying information of another person. Identity theft can cause severe consequences for its victims.

Identity theft can be broken down into sub-categories:
1. Financial Identity Theft
2. Medical Identity Theft

According to the FTC, identity theft is the #1 consumer complaint.
Medical Identity Theft

The World Privacy Organization defines medical identity theft as **theft that occurs when someone uses another person’s name and other parts of their identity** (such as insurance information or social security number) without the victim’s knowledge or consent to:

- Receive medical services or goods
- Make false claims for money

In the process, false information is added to the victim’s medical record.
Mr. Miller is the unknowing victim of medical identity theft.

Claims for procedures which were never performed on Mr. Miller were submitted to his insurance company.

How do you think this will impact Mr. Miller?
Consequences of Identity Theft

Because false claims have been submitted in Mr. Miller’s name, his medical record shows information that is false.

As a result Mr. Miller could:
- Be denied insurance coverage
- Receive unsafe medical care and false diagnoses
- Have credit and financial problems

Identity theft can impact:
- Insurance Coverage
- Medical Care
- Credit and Finances
Avoiding Identity Theft

Take these precautions to protect yourself:

- Share personal health information only with trusted providers
- Review each Explanation of Benefits you receive to monitor claims submitted in your name
- Request an annual summary of benefits paid from the insurer
- Review your credit history
To help prevent identity theft, LVHN has:

• Established a verification process
• Minimized the use of social security numbers
• Created safeguards for all identifiable health information
• Implemented procedures for the disposal and destruction of health information
Why is the Program Important?

The LVHN Identity Theft Prevention Program is required by the government and incorporates the requirements of the Federal Trade Commission (FTC). The FTC requires a written program to identify warning signs of identity theft.

The LVHN Identity Theft Prevention Program is designed to identify and correct any potential identity risks.
A "Red Flag" is a pattern, practice, or specific activity that indicates the possibility of identity theft. Red flags fall into one of four categories for healthcare.

Click each of the buttons to learn about the four types of "red flags".
Red Flags

Suspicious Documents

Examples:
- Patient's identification documents appear to have been altered
- Expired Driver's License or Insurance Card

Suspicious Identifying Information
Suspicious Activity to an Account
Alerts from Others
Red Flags

Suspicious Documents

Suspicious Identifying Information

Examples:
- Driver's License picture does not match the patient
- Patient has an insurance number but no Insurance Card and you cannot find active coverage
- Information differs from that previously provided
- Invalid telephone number or address

Suspicious Activity to an Account

Alerts from Others
Red Flags

<table>
<thead>
<tr>
<th>Suspicious Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious Identifying Information</td>
</tr>
<tr>
<td>Suspicious Activity to an Account</td>
</tr>
<tr>
<td>Alerts from Others</td>
</tr>
</tbody>
</table>

Suspicious Activity to an Account

Examples:
- Mail is undeliverable, but patient presents for treatment
- Non-payment for services when there is no history of a late payment
- Frequent address changes
- Multiple alias names
Red Flags

Suspicious Documents

Suspicious Identifying Information

Suspicious Activity to an Account

Alerts from Others

Others, including law enforcement, patients, the identity theft victim, etc., could alert you to possible identity theft.

Examples:
- Family members call patient by a different name
- Notification by other healthcare organizations or insurance carriers
To help prevent identity theft, LVHN has implemented a verification process for both new and existing patients.

Obtain the appropriate demographic and insurance information from your patient. This includes:
- Full name
- Date of birth
- Address
- Social Security Number
- Photo ID/Driver’s License
- Insurance card

You should also verify electronic insurance eligibility for all carriers.
Acceptable forms of identification include:
- Driver’s License
- Birth Certificate
- Passport
- Military ID
- Social Security Card
- School ID
- Work ID
- Permanent Residence Card (Green Card)
- Voter Registration Card

If you have any concerns or questions regarding a patient’s identity, ask for a second form of identification to verify the patient’s identity.
If You Suspect Identity Theft

When you suspect identity theft:

1. **Gather information** – DO NOT confront the patient

2. **Provide Care** – NEVER turn a patient away!

3. **Notify** your supervisor/manager

4. **Notify Security** (610-402-8220)

5. Complete a **Patient Safety Report**
   Click the icon on your SSO Toolbar
You should now be able to:

• Explain the purpose of the LVHN Identity Theft Program
• Define medical identity theft
• List three consequences of identity theft
• List precautions that individuals can take to avoid identity theft
• Identify the appropriate information that should be obtained to verify patient identity and four acceptable forms of identification
• Identify the four categories of red flags for identity theft in healthcare