

HPN Cybersecurity Awareness Training



Objective: Understand how daily actions protect patient information, devices, and company systems. Gain the skills to identify cyber threats, maintain secure practices, and report incidents promptly and responsibly.

Cybersecurity Awareness Training



- How to Protect Our Patients, Data, and Organization
- This self-paced training explains how your daily actions help keep systems and information secure.



How to Use This Training



- This is a self-paced course.
- Read each slide carefully and think about how it applies to your role.
- There is no presenter.
- You will complete a knowledge check at the end.

What Cybersecurity Means for You



- Cybersecurity is about protecting information, systems, and devices.
- Your daily actions directly impact patient safety and data protection.
- You do not need technical expertise to make a difference.



Why Cybersecurity Matters in Healthcare



- Cyber incidents can:
 - Delay or disrupt patient care
 - Expose patient or employee information
 - Shut down systems needed for daily work
- Every role plays a part in prevention.



Common Cybersecurity Risks



- Healthcare organizations face risks such as:
 - Ransomware and malware
 - Accidental data exposure
 - Insider mistakes
 - Lost or stolen devices
 - Physical security gaps



Ransomware Explained



- Ransomware is malicious software that locks systems or files.
- This can stop access to patient records and schedules.
- Early reporting helps limit damage.



Malware Explained



- Malware is software designed to harm or spy on systems.
- It can slow devices, steal information, or spread silently.
- Unsafe downloads are a common cause.



How Ransomware and Malware Are Introduced



Ransomware and malware are often introduced through everyday activities such as:

- Clicking suspicious links in emails or text messages
- Opening unsafe attachments or downloads
- Visiting compromised or untrusted websites
- Using infected USB drives or external devices
- Installing unauthorized software or applications



Examples of Ransomware and Malware



- **Phishing Email:** An employee clicks a fake invoice attachment that installs ransomware.
- **Malicious Download:** Downloading free software from an unapproved website infects a computer with malware.
- **Fake Pop-Up Alert:** A user clicks a “system update” pop-up that secretly installs harmful software.
- **Infected USB Device:** Plugging in an unknown USB drive spreads malware to the network.

Key Reminder:

Always verify emails, downloads, and websites before interacting with them. Report anything suspicious immediately.



Insider Threats



- Insider threats are often accidental.
- Examples include:
 - Sharing passwords
 - Accessing data you do not need
- Awareness helps prevent mistakes.



Protecting Patient and Company Data



- You are responsible for handling sensitive data carefully.
 - Access only what you need
 - Follow HIPAA and company policies
 - Be mindful of screens, conversations, and printed materials



Passwords and Authentication



- Strong authentication protects accounts.
 - Use strong, unique passwords
 - Do not use the same password for multiple accounts, since a breach of one account can compromise others
 - Never share credentials
 - Multi-Factor Authentication adds protection



Email and Communication Safety



- Be cautious when communicating digitally.
 - Verify senders before responding
 - Be careful with unexpected attachments
 - Do not share sensitive data through unsecured channels
 - A separate training on phishing is available. Please review it to familiarize yourself with common phishing techniques used by malicious actors.



Internet and Application Use



- Work devices should be used responsibly.
 - Use approved websites and software only
 - Avoid untrusted downloads
 - Limit personal browsing on work devices

Remote Work Security



1. Use Company Devices in a Private and Secure Area

- Work in a private location whenever possible.
- Ensure screens and conversations are not visible or audible to roommates, guests, or co-tenants.
- Prevent unauthorized individuals from accessing patient or company information.

2. Secure Company Devices at All Times

- Lock your screen whenever you leave your device unattended
- Store laptops and mobile devices securely when not in use.
- Do not allow family members or others to use company devices.

3. Protect Your Home Network and Connections

- Use a password-protected Wi-Fi network with strong encryption at all times.
- Do not use public or unsecured Wi-Fi for work activities.
- Use the VPN and approved security tools when accessing company systems remotely.

Device Security



- Protect the devices you use every day.
 - Lock your screen when away
 - Keep devices updated
 - Report lost or stolen devices immediately



Remote Work Security



- Working remotely requires extra care.
 - Use secure Wi-Fi
 - Avoid public Wi-Fi when possible
 - Use VPN if required
 - Keep conversations private



Physical Security Matters



- Cybersecurity also includes physical protection.
 - Wear your badge
 - Do not allow tailgating
 - Secure paper records
 - Follow clear desk practices



Data Handling and Disposal



- Handle data safely from start to finish.
 - Print only when necessary
 - Secure printed documents
 - Shred sensitive information
 - Do not store work data on personal devices



Security Incidents Can Happen



- Even careful people can make mistakes.
- Early reporting reduces harm.
- The organization supports a no-blame reporting culture.



How to Report a Security Incident



- Report immediately if something feels wrong.
- Contact IT or the Security team.
- Provide details, even if you are unsure.



Your Role in Cybersecurity



- Cybersecurity is a shared responsibility.
- Small actions make a big difference.
- Staying alert helps protect everyone.



Key Takeaways



Think Before You Click

Cyberattacks often start with suspicious emails, links, attachments, or pop-ups. If you are unsure, pause and verify before proceeding.

Protect Patient and Company Information

Access only the information necessary for your role, comply with HIPAA requirements, and refrain from discussing sensitive information in public or shared areas.

Secure Your Devices Everywhere

Lock your screen when away, keep devices updated, and never leave company laptops or phones unattended, particularly when working remotely.

Work Securely From Home

Use company devices in a private area, away from others, and always connect through secure Wi-Fi or VPN as needed.

Report Problems Immediately

If something feels suspicious - such as a phishing email, lost device, or accidental mistake - report it right away. Early reporting helps protect everyone.