



## Cybersecurity Awareness & Requirements Training

# CONTENTS

- Remote Work Security
- Types of Cybersecurity
- Cybersecurity Terms
- Top Cybersecurity Threats
- What Personal-Touch Does for Cybersecurity
- What You Should Do for Cybersecurity
- How to Access Compliance 360
- Who to Notify if you Suspect a Cybersecurity Issue

## Maintaining Security Practices While Working Remotely

PTHC work on your workstation/portable device, any paper documents/notes, and information on conference calls are subject to strict confidentiality and compliance guidelines ALWAYS.

- 1. Utilize appropriate physical safeguards to limit observation of your work content to you/other authorized users.** Work should be done in an area where confidentiality can be maintained. This includes when working from your own home or apartment.
  - Be sure confidential information on your screen is not visible to those around you, including family/friends.
  - Have conference calls/video calls in a location where confidential conversations cannot be overheard by ANYONE. It is ESPECIALLY important to be mindful of discussions about any type of identifiable health information, cybersecurity information, passwords, etc.

## Maintaining Security Practices While Working Remotely

### **2. Utilize appropriate physical safeguards to limit workstation access to you/other authorized users.**

- When not in use, workstations/portable devices must be stored in secured/locked locations.
- Workstations/portable devices must not be left unattended and visible to unauthorized users, including family/friends. Lock the screen before walking away from it.
- Workstations/portable devices must be logged off of applications requiring authentication and authorization at the conclusion of user sessions.
- Family members and friends are not permitted to use remote workstations or portable devices used for work.
- Remote workstations can only be utilized for approved functions.
- ePHI cannot be copied from workstations to removable media without specific authorization.

## Maintaining Security Practices While Working Remotely

- 3. Utilize appropriate safeguards in the disposal of hardware and confidential documents.**
- 4. Follow all HIPAA, FINRA, etc. and your company's cybersecurity compliance policies.**
- 5. Utilize company approved video conferencing solutions and procedures in any and all discussion of confidential information, particularly including, but not limited to PHI. (i.e. Do not use the free Zoom; ensure it is clear who joins a call; lock calls once attendees are present, etc.)**

### **BREACH EXAMPLES:**

- A child repeating a patient's name, that was seen on a parent's computer, to a friend.
- A home appliance technician seeing a password.

## Types of Cybersecurity\*

**Application** - Specific software/programs.

**Information** - Data stored locally, in the cloud or offsite.

**Network** - a set of computers connected together for the purpose of sharing resources.

**Database and infrastructure** - Hardware and software that enable network connectivity, communication, operations and management of a network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.\*\*

**Mobile** - Portable devices that can connect to and/or communicate with the network.

## Types of Cybersecurity\*

**Application** - Specific software/programs.



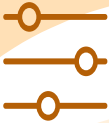


**Information** - Data stored locally, in the cloud or offsite.

**Network** - a set of computers connected together for the purpose of sharing resources.

**Database and infrastructure** - Hardware and software that enable network connectivity, communication, operations and management of a network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.\*\*






**Mobile** - Portable devices that can connect to and/or communicate with the network.

## Cybersecurity Terms\*






	<p><b>1. Cloud</b></p> <p>A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it's a collection of computers with large storage capabilities that remotely serve requests.</p>
	<p><b>2. Software</b></p> <p>A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.</p>
	<p><b>3. Domain</b></p> <p>A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.</p>
	<p><b>4. Virtual Private Network (VPN)</b></p> <p>A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.</p>
	<p><b>5. IP Address</b></p> <p>An internet version of a home address for your computer, which is identified when it communicates over a network. For example, connecting to the internet.</p>








## Cybersecurity Terms

	<b>6. Exploit</b> A malicious application or script that can be used to take advantage of a computer's vulnerability.
	<b>7. Breach</b> The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.
	<b>8. Firewall</b> A defensive technology designed to keep criminals out. Firewalls can be hardware or software-based.
	<b>9. Malware</b> An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
	<b>10. Virus</b> A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses have caused physical damage.

## Cybersecurity Terms

	<p><b>11. Ransomware</b></p> <p>A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.</p>
	<p><b>12. Trojan horse</b></p> <p>A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.</p>
	<p><b>13. Worm</b></p> <p>A piece of malware that can replicate itself in order to spread the infection to other connected computers.</p>
	<p><b>14. Bot/Botnet</b></p> <p>A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a “botnet” and is controlled by the hacker or “bot-herder”.</p>
	<p><b>15. DDoS</b></p> <p>An acronym that stands for distributed denial of service – a form of cyber attack. This attack aims to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).</p>

## Cybersecurity Terms

	<p><b>16. Phishing or Spear Phishing</b></p> <p>A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.</p>
	<p><b>17. Encryption</b></p> <p>The process of encoding data to prevent theft by ensuring the data can only be accessed with a key.</p>
	<p><b>18. BYOD (Bring Your Own Device)</b></p> <p>Refers to a company security policy that allows for employees' personal devices to be used in business. A BYOD policy sets limitations and restrictions on whether or not a personal phone or laptop can be connected over the corporate network.</p>
	<p><b>19. Pen-testing</b></p> <p>Short for "penetration testing," this practice is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws. This is done internally and by hired vendors.</p>
	<p><b>20. Clickjacking</b></p> <p>A hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element.</p>

# Top Cybersecurity Threats

1. Email
  - a. Untargeted phishing with malicious links
  - b. Spear-phishing/targeted phishing at organization or individual within
  - c. Impersonation or misrepresentation
  - d. Malicious macros in attachments
2. Ransomware / Data Hostage
3. Data Corruption
4. Data Theft
5. DDoS - Distributed Denial of Service  
& System Shut downs



Cybersecurity is a TEAM effort!



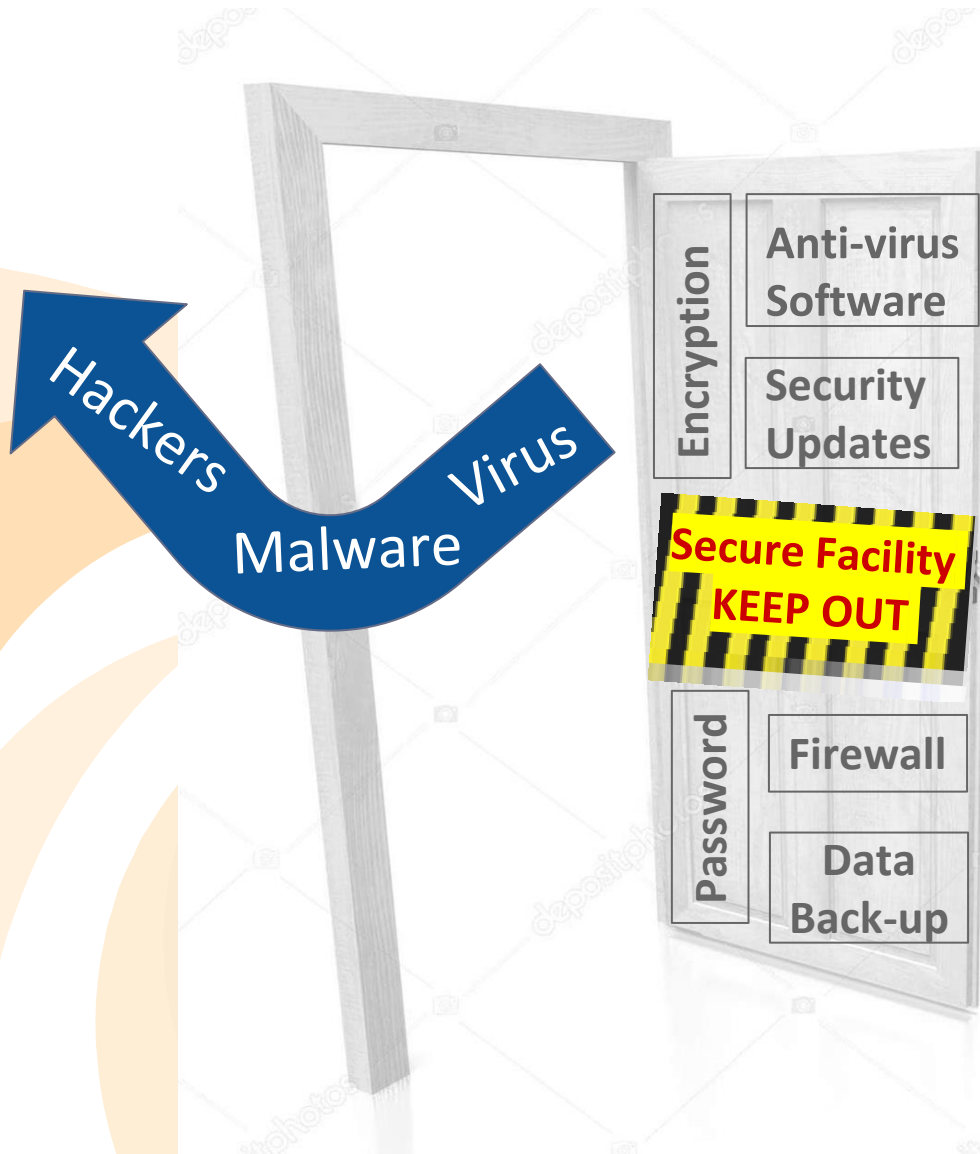
## What Personal-Touch Does for Cybersecurity

- ❑ Physical and technical safeguards to protect EPHI
  - ❑ Firewalls, encryption, anti-virus, secure data facility
- ❑ Collaborating/Consulting with IT Security Vendors to utilize best practices in data protection.
- ❑ Data Collection - Collecting and analyzing logs and installing endpoint monitoring solutions.
- ❑ Monitoring the entire attack/vulnerability surface - Securing endpoints and access to outside networks and applying advanced analytics to data for warnings and detection of attacks.
- ❑ Assessing vulnerability of data and/or systems due to events.
- ❑ Organizational collaboration - Coordination between IT, departments, vendors and key stakeholders.

## What Personal-Touch Does for Cybersecurity

- ❑ Analyzing the infrastructure & equipment and operational processes and procedures that could leave an opening for attackers:\*
  - Infiltration and persistence; Reconnaissance; Lateral movement; Mission target; Maintaining presence
- ❑ Understanding likely threats - Staying updated on current trends and specific industry and organizational cybersecurity and data/system loss risks (i.e. fire, flood, etc.).
- ❑ Organization-wide Workflow - Creating an Incident Response Plan (reviewing and revising it at least annually), testing workflows, and maintaining consistent policies.
- ❑ Maintaining independent redundancy of data and systems as possible and understanding amount of time needed to transfer to back-up systems and/or restore systems and/or data.
- ❑ Training and ongoing reminders and updates regarding policies and procedures

## What You Should Do for Cybersecurity



## Pause Before Clicking

All security measures are only as good as the degree to which they are utilized & enforced. An open door is an open door.





## What You Should Do for Cybersecurity

→ Strong password protection and authentication

- ◆ Complex Passwords
- ◆ Update Passwords
- ◆ Don't share your passwords or leave them posted

→ Avoid pop-ups

- ◆ Even/especially ones that say "URGENT"

→ ALWAYS use company email address for company correspondence

→ Inspect emails before opening them

- ◆ Look at who it is from - check the banner at the bottom of the email
- ◆ Does the subject make sense?

**CAUTION:** This email originated from outside of the PTHC email system. Do not click links, open attachments, or reply unless you trust the sender and know the content is safe. If you suspect this is a fraudulent email, please contact the IT service desk at [support@pthomecare.com](mailto:support@pthomecare.com) or call ext 1730

**NOTE:** It is extremely important to recognize the risk and inspect emails for potential impersonation to insure it is the person who they say they are. **VERIFY** the user - especially before sharing any confidential information.

## What You Should Do for Cybersecurity

- Don't click on unknown links
- Adhere to Mobile Device User Agreement/Policy
- Multi-factor authentication on ALL mobile devices that have access to potentially confidential information
- Do NOT use non-company issued USB thumb drives
- Ask when unsure
- Read, review and follow policies and procedures - (Compliance 360 - see page 19)
  - ◆ Stay updated
  - ◆ Read Memos that are sent out about security issues
- IMMEDIATELY notify the CISO if you suspect a cybersecurity issue  
(Info on page 20)

# How to Access Compliance 360

The screenshot shows the PTHC website with the URL [pthomecare.com/log-in](http://pthomecare.com/log-in) in the browser address bar. The website header includes the PTHC logo, the phone number **1-888-275-4147**, and a navigation menu with links: Home, About, Employment, Services, Locations, Contact, Bill Pay, Log In, and More. The 'Log In' link is highlighted with a blue circle and an arrow pointing to it from the instruction '1. From the PTHC website click "Log In"'. Below the navigation menu is the 'Employee Portal' section, which contains three buttons: 'EMPLOYEE EMAIL ACCESS', 'FORGOT YOUR EMAIL PASSWORD?', and 'CLICK HERE TO ACCESS COMPLIANCE 360'. The 'CLICK HERE TO ACCESS COMPLIANCE 360' button is highlighted with a yellow background and an arrow pointing to it from the instruction '2. Select "Access Compliance 360"'. Below this button is contact information for tech support: 'If you need further assistance contact tech support: Email: [support@pthomecare.com](mailto:support@pthomecare.com)', 'Phone: 718.468.4747 ext. 1610', 'Option 1 - Allscripts and ATL', 'Option 2 - PC, Printer, Fax, Phone, Copier, Email, Internet, Networking', and 'Option 3 - AS-400, HSS, Payroll Pickup'. To the right of the 'Employee Portal' section is the 'Guest Area' login form, which has the heading 'Guest Area', the instruction 'Please enter the password below.', a 'Password' label, a password input field, and a 'Go' button. An arrow points from the instruction '3. Enter Password' to the password input field.

1. From the PTHC website click "Log In"

2. Select "Access Compliance 360"

3. Enter Password

## Who to notify if you suspect a cybersecurity issue:

Notification List
<b>CISO / Sr. Telecom Engineer</b> Dan Erlichman  <b>Direct:</b> (718) 468-4747 ext. 1717  derlichman@pthomecare.com
<b>VP of IT Services and Support</b>  jcupp@pthomecare.com
<b>Service Desk</b>  support@pthomecare.com

- Immediately call the CISO - at (718)-468-4747, ext. 1717
- After call, email the CISO at [derlichman@pthomecare.com](mailto:derlichman@pthomecare.com) and cc all Notification List ([jcupp@pthomecare.com](mailto:jcupp@pthomecare.com) & [support@pthomecare.com](mailto:support@pthomecare.com)) with any attachments and pertinent information/explanation to be reviewed.
  - i.e. Screenshot, Suspected Phishing Email, etc.
- For email subject:  
**Suspected Cybersecurity Issue**