



HIPAA Security Rule Training Materials



INTRODUCTION TO INFORMATION SECURITY

In April 2003 the HIPAA Privacy Rule went into effect. This introduced the idea of administrative, technical and physical “safeguards” for protected health information (PHI)- which came to be known as the “mini-security rule.” **On April 21, 2005 the HIPAA Security Rule takes effect** and develops the idea of the mini-security rule more fully. The Security Rule focuses specifically on PHI that is maintained or transmitted in electronic media (ePHI) and requires the implementation of appropriate security safeguards to protect ePHI against the risk of unauthorized use or disclosure, while permitting the appropriate access and use of that information.

Definition of ePHI

ePHI is patient health information that is created, received, stored or maintained, processed and/or transmitted in electronic media. Electronic media is defined broadly to include storage devices, such as computer hard drives, disks, optical disks and digital memory cards, and tools used in transmitting information, such as the internet, extranet, dialup lines, private networks. Also included is the physical transportation of electronic storage media (e.g. when disks may be moved from one location to another.).

Security Rule General Requirements

The General Requirements of the Security Rule identify the primary goals of the Standard. They require the practice to:

1. Ensure the confidentiality, integrity and availability (“CIA”) of all ePHI that we create, receive, maintain, or transmit.
2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI (e.g. hackers, virus, worms, etc.).
3. Protect against unauthorized disclosures.
4. Ensure awareness of workforce members through training. The purpose of this document is to provide you with a fundamental understanding and awareness of the importance of protecting PHI and the means by which it is done. Well trained employees are the key to ensuring the protection of PHI.

The Security Rule requires that we identify a Security Officer who is responsible for the development and implementation of appropriate security policies and procedures as well as ensuring compliance by all members of the practice.

Security Officer: Anthony Fraioli
Director of Information Technology
Phone: (914) 333-5886



Consequences of Poor Security

Failure to follow security measures puts our business at risk in several ways.

- Risk to integrity of confidential information, e.g. data corruption, destruction, unavailability of patient information
- Risk of security to personal information, e.g. identity theft
- Loss of valuable business information
- Added costs to our practice (increased work for the IT Department)
- Embarrassment, poor publicity, media coverage, news reports

- Internal disciplinary actions, termination of employment
- Penalties, prosecution and potential for sanctions / lawsuits
 - o Wrongful disclosure of individually identifiable health information can result in penalties of \$50,000 - \$250,000 and imprisonment of up to 10 years depending on the intent.

Adhering to good security practices will minimize the risk of any of the above consequences. Do your part by incorporating the following 10 Security Safeguards into your everyday routine, and encouraging others to do so as well.

10 Security Safeguards

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. Your Responsibility 2. Access Controls & Unique User ID 3. Password Security & Management 4. Workstation & Portable Device 5. Data Management | <ol style="list-style-type: none"> 6. Remote Access 7. Be Aware of Malicious Programs 8. Email Security 9. Safe Surfing and Internet Use 10. Reporting Security Incidents |
|---|---|

Safeguard #1: YOUR RESPONSIBILITY

Good security standards follow the “90/10 Rule” – 10% of the security safeguards are technical; 90% of security safeguards rely on the computer user (**YOU**) to adhere to good computing practices.

For example: A lock on a door is the 10%. You remembering to lock it, checking to see if it is closed, keeping control of the keys is the 90%. 10% security is worthless without YOU!

Adherence to good computing practices is done by familiarizing yourself with the policies and procedures and standards relating to information security. This paired with some common sense will maintain the confidentiality and integrity of the PHI we create and maintain electronically.

All workforce members are responsible for bringing potential security incidents to the attention of your supervisor or the Security Officer so that the concern may be addressed and mitigated. (See *Safeguard #10*)

Safeguard #2: USER ACCESS CONTROLS / UNIQUE USER LOG-IN

Access controls are policies and procedures that assure that reasonable measures are taken to protect ePHI. Users are assigned a unique “User ID” for purposes of logging into the network as well as NextGen and Medical Manager. Each User ID is linked to a specific amount of system access. This access is “**role-based**” which means that access is limited to the minimum information needed to perform your job. If you share your User ID with someone else, not only are you potentially giving that person access to information that they are not entitled to, you become responsible for anything that person does under your name.

The IT Department is responsible for the assignment of role-based access and subsequent auditing for inappropriate use or access. Ask for User IDs for all new employees by accessing the IT Department Support Page on our website. Do not share yours!

Safeguard #3 PASSWORD PROTECTION

Importance of Passwords

Your unique username and password is your key to access the system. Every time you log on, you must prove you're who you say you are by supplying your password. Should someone else guess or steal your password, that person can access the system and its file masquerading as you. This intruder will have the power to modify or destroy your files, and/or access protected health information (PHI). This is why it is important to select a secure password.



Creating a Better Password

When creating your password, think of it as an access code rather than a "word". Here are some important dos and don'ts when creating a secure password.

<u>Do's</u>	<u>Don'ts</u>
<ol style="list-style-type: none">1. Use a password with non-alphabetic characters, i.e.: digits or punctuation2. Make your password easy for you to remember but hard for someone else to guess3. Use a password with mixed-case alphabetic4. Pick the first letter of each word from a phrase that is meaningful to you (e.g. Mc1F&NaW! = My car is Filthy and Needs a Wash!)5. Use a password with at least 6-8 characters (letters, numbers & symbols).	<ol style="list-style-type: none">1. Never write your password down; someone else might see it2. Don't use your spouse's or child's name3. Don't use your name in any combination4. Don't use other information easily obtained about you, i.e.: DOB, license plate, telephone numbers, etc5. Don't use easily guessed password like the name of a city, or an alphabet or number sequence.6. Do not pick a word that can be found in the dictionary.

Password Management

After you have created a strong and secure password, protect it as your personal secret. If you believe your password has been compromised, change it immediately. Procedures will soon be in place that will require all network and NextGen users to change passwords every 90 days. The procedures will not allow the same password to be used twice in a row.

Social Engineering

Social engineering is a con game that tricks a person into revealing his or her password, PHI or other pertinent information. Social engineering can be initiated in person, over the phone, via an authentic looking e-mail, or other means. Under NO CIRCUMSTANCES should you give your password to ANYONE over the phone, in person or in an email *except* IT Support staff who may need that information for troubleshooting purposes.

It is important that when a person calls requesting PHI that we verify that they are who they say they are. We may only release PHI to the patient or the guardian or personal representative of that patient. Should you receive a phone call from a person requesting PHI you must first verify three identifiers.

Examples of Identifiers

- DOB
- Social Security Number
- Name
- Address

Safeguard #4: WORKSTATION AND PORTABLE DEVICE SECURITY

Workstations



The Security Rule requires the implementation of safeguards for all workstations that access ePHI, to restrict access to unauthorized users.

“Workstations” include any electronic computing device, for example, a desktop or laptop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment (PDAs, tablet computers and other portable/wireless devices). The critical variable is not the particulars of the device itself but whether it can access or store PHI.

You can use various disaster and physical access controls to protect the security of your workstation. (see also Safeguard #5).

Disaster Controls protect workstations from natural and environmental hazards, such as heat, liquids, water leaks and flooding, disruption of power, and other conditions exceeding equipment limits.

Physical access controls

Lock or Log-off before leaving a workstation unattended to prevent other individuals from accessing ePHI under your User ID and to limit access by unauthorized users. Before leaving a workstation lock it or log off by pressing the Ctrl, Alt and Delete buttons simultaneously and then selecting the option, “Lock Computer” or “Log Off...”

When leaving for the day, log off of the computer following the instructions above.

The IT Department will be implementing a screensaver which will activate automatically after 7 minutes of inactivity. The user logged into that particular computer will need to enter his or her password to turn the screensaver off.

Lock It Up! Never leave protected information around in paper or electronic form. Please secure all CD's, floppies and USB flash drives that contain PHI. Do not leave sensitive information on remote printers or copiers.

PORTABLE DEVICES & LAPTOPS WITH ePHI



Few computer innovations have introduced more convenience than the development of portable computing devices from laptops and notebooks to PDAs (e.g. Palm Pilots, Blackberry). Unfortunately, the great virtue of these devices- easily carried from place to place- is also their greatest weakness.

According to FBI statistics, one out of every 10 notebook computers will be stolen within the first twelve months of purchase. Given these numbers, the best practice is to keep confidential or sensitive information off such devices entirely. Failing that, safeguards such as pre-theft

physical security and post-theft access controls will protect against unauthorized access to confidential files and information. Examples include:

- Use an internet firewall
- Use up-to-date Anti-virus and Anti-spyware software
- Install computer software updates, e.g. Microsoft patches
- Encrypt, if possible, or at least password protect portable devices
- Lock-it up! Lock office or file cabinet, lock up laptops
- Automatic log-off from programs
- Use a password protected screensaver
- Back-up critical data and software programs.
- Delete ePHI files from all portable devices when no longer needed.

Wireless devices open up more avenues for ePHI to be improperly accessed. To minimize the risk, use the following precautions:

- Do not enable the wireless port that exposes the device, unless it has been secured.
- Use a Virtual Private Network (VPN) if making a wireless connection.
- Adhere to user / device authentication before transmitting ePHI wirelessly.
- Encrypt data during transmission, and maintain an audit trail.
- Refer questions to the IT Department.

Safeguard #5: DATA MANAGEMENT & SECURITY

This refers to the means by which we store, move and dispose of data containing ePHI.

Data Backup and Storage

System back-ups are created to assure the integrity and reliability of data. It is not recommended that you store any original data on local drives or laptops because this data will be lost in the event that the computer crashes.

Any files containing ePHI and stored on a disk, CD or other portable devices should be password protected to restrict access to confidential information. Additionally, get into the habit of scanning floppy disks and CDs for viruses and corruption each time you re-insert them into the computer, particularly when using these devices on multiple computers. Also refer to Safeguard #4: Workstations and Portable Devices Security.

Data Disposal

Policies and procedures will address the appropriately controlled and managed removal and/or destruction of ePHI that is stored or transported on storage devices such as computers, disks and CDs. The following will be addressed:

- Hard-drives, CDs, zip disks or back-up tapes must be "cleaned" before recycling or re-using.
- Contact the IT Department to overwrite, degauss or destroy any digital media before discarding.
- Typical reformatting is not a sufficient way to destroy unneeded ePHI because it does not overwrite the data.

Safeguard #6: SECURE REMOTE ACCESS

The following minimum standards are required for remote network access by portable devices, laptops and home computers connected to the ENT and Allergy network. Minimum network security standards are:

1. Software security patch is up-to-date

2. Anti-virus and Anti-spyware software is running and up-to-date on every device.
3. Turn off unnecessary services and programs.
4. Physical security safeguards and in place to prevent unauthorized access.

Safeguard #7: BE AWARE OF MALICIOUS PROGRAMS AKA “MALWARE”

The term “Malware” refers to **malicious software**. It covers any piece of programming that steals and disrupts or distorts ones ability to access information on their computer.

Viruses and Worms and (Trojan) Horses, Oh My!

These three malicious programs are often used interchangeably. While they are all considered to be malicious programs that can cause damage to your computer, there are differences among the three.

A virus is a program with the unique ability to replicate, or make copies, of itself and spread itself to another recipient. People continue to spread a computer virus, mostly unknowingly, by sharing infected files, visiting an infected webpage or sending emails with viruses as attachments in the email.



A computer worm is similar to a virus and is considered to be a sub-class of one. It is spread to other computers on a network automatically and without the action of humans. A worm doesn't alter or delete files but instead they reside in memory, eat up system resources, and slow down your computer.

A Trojan Horse is a program that is full of as much trickery as the mythological Trojan Horse if is named after. At first glance it appears useful and fools a user into running it. But once activated on your computer the results can vary.

- Some are designed to be more annoying than malicious
 - changing your desktop, adding silly active desktop icons
- Others can cause serious damage
 - Deleting files and destroying information on your system
- Or it could create a "back door" that gives malicious users (a.k.a. “Crackers”) access to your computer.



Spamming, Phishing Scams and Spyware

Spam is unsolicited bulk email, including commercial solicitations, advertisements, chain letters, pyramid schemes, and fraudulent offers. Again, our IT Department does have an anti-spam program in place which catches a majority of these emails and labels the “[SPAM].”. However, not all of these types of messages are captured. If you identify an email as spam:

- Do not reply to the message. Do not spread spam.
- Do not forward chain letters. It is the same as spamming and is against ENT and Allergy Associates policy.
- Do not open or reply to suspicious emails. Delete the message and then delete it again from the recycle bin.
- Never click on the “unsubscribe” link on these emails as this validates that the spam has reached a valid address.



Phishing is a high-tech scam that uses spam and pop-up messages to deceive you into disclosing sensitive information such as bank account numbers, credit card numbers, and passwords). These emails or pop-ups pretend to be from trusted names such as Citibank, Paypal or Amazon. The message usually says that you need to

“update” or “validate” your account information. It might threaten some dire consequences if you don’t respond. The message directs you to a website that looks like the organization’s legitimate website, but isn’t. The purpose? To trick you into divulging the personal information so that operators can steal your identity and run up bills in your name! A reputable company will never ask you to send your password through email.

Spyware is any technology that aids in gathering information about a person or organization without their notice or consent. It is usually installed on a computer as a software virus or as the result of installing a new program from an Internet download. Persons with Spyware on their computer do not even need to be connected to the Internet for information to be gathered. It can be recorded anytime you use your computer and then transmitted when an Internet connection is established.



Computers infected with Spyware will experience:

- Slower than normal page loading speeds
- excessive pop-up ads when surfing the Internet
- pop-up ads or messages that appear even when you are not connected to the Internet
- settings for your browser home page have been changed
- a new toolbar is installed in your browser without your consent.
- Strange or unexpected behavior from your computer even when not on the internet.

These pests can potentially stop an organization in its tracks. Our IT Department currently has a very secure firewall in place, keeps up with security patches and maintains anti-virus software in an effort to protect against these threats. Even though our Network is well protected, an employee’s carelessness could cause a security breach or incident. We can all do our part to help provide better security (remember the 90/10 Rule?).

- Only open an attachment if you are expecting one and if you know the sender.
- Attachments with file extensions such as *.zip, *.exe, *.bat, *.com, *.vbs, *.pif, and *.scr may be malicious and mechanisms are in place to block these files from coming through.
- Do not click on a web link contained in any email from someone you do not know.
- Be cautious of unusual subject lines such as “Your car?”, “Oh!”, “Nice Pic!”, “Family Update!”, “Very Funny!”

If your computer is acting strangely, contact the IT Support Line (914.333.5841) for assistance.

Safeguard #8: E-MAIL SECURITY

E-mail is like a postcard. Email may potentially be viewed in transit by many individuals, since it may pass through several switches enroute to its final destination or never arrive at all!



Although the risks to a single piece of e-mail are small given the volume of email traffic, **emails containing ePHI need a higher level of security and careful addressing!**

At this time, our emails are not encrypted. Encryption is a method of encoding messages to provide privacy for email, discussion group postings, and other communications as they move over intranets or the Internet. Look for more information on encryption in the future as we look ahead to creating an even safer environment for ePHI.

Until then follow these steps before sending an email containing ePHI:

- Verify that the intended recipient's address(es) is typed correctly. Use the automatic name checking function in Outlook.
- Include the confidential footer in all outbound messages with ePHI.
- Password protect any attachments containing ePHI, or do not send the attachment via email!
- Avoid using individual names, medical record numbers or account numbers in unencrypted emails.
- Do not forward emails with ePHI from secure addresses to non-secure accounts (e.g. hotmail, AOL).
 - o Instead check your ENT and Allergy messages remotely via Webmail. Contact IT to find out how to do this.
 - o Obtain reasonable assurances that the recipient is using a secure, rather than hosted, email server which means your email is sent directly to their secure server.
- Only send the minimum amount of patient information needed (minimum necessary rule).

Email Between Patients and Providers

Patients may request email exchange of health information and HIPAA does not ban this. In the absence of an email encryption program, patients must be informed of the risks of using email and that the security of the information cannot be guaranteed. An email consent form is being created to address this requirement. Note that if email is used to exchange substantive health information with a patient, copies of the messages should be kept as a part of the patient's medical record.

Safeguard #9: SAFE SURFING & APPROPRIATE INTERNET USAGE

Internet access is provided to employees of ENT and Allergy Associates, LLP for the purpose of performing work related tasks. While limited personal use is permitted, this is a privilege that can be taken away if abused. Employees should use the Internet responsibly and exercise caution when surfing the Web.



For the most part, our IT department has security measures in place that block us from accessing websites that could be potentially harmful to the network. You can help by only visiting websites that are reputable and that are necessary to the completion of a work related task.

Remember: The Internet is not private! Access to any site on the Internet could be traced to your name and location.

Safeguard #10: REPORT SECURITY INCIDENTS

As with all potential compliance related incidents, it is imperative that all employees take an active role in reporting them so that they can be investigated and, if necessary, mitigated in a timely manner. A security incident is defined in the Security Rule as,

“the attempted or successful or improper instance of unauthorized access to, or use of information, or mis-use of information, disclosure, modification, or destruction of information or interference with system operations in an information system.”

Security incidents can result due to intentional breaches or simply carelessness. Examples of security incidents include, but are not limited to the following:

- Sharing of passwords and/or User IDs
- Failure to log off or lock the workstation when required

- Downloading or installing unauthorized software
- PHI is acquired by an unauthorized person
- Employee resignation not reported promptly to IT so their passwords stay active.
- Using instant messages or chat rooms that are not work related and authorized.

Note: Good faith acquisition of PHI by an ENT and Allergy Associates employee or agent does not constitute a security incident, provided that the PHI is not used or subject to further unauthorized disclosure.

Report Security Incidents:

You can report potential security incidents by calling:

IT Support line at (914) 333-5841

Compliance Hotline at (914) 333-5894

Remember, the Compliance Hotline provides a mechanism for anyone to make an anonymous report. All reports of potential security incidents made via the Hotline will be forwarded to the Security Officer for investigation.