



Information Security for Physician Office Staff

Training year 2007



Objective

This short, informational briefing is designed to update physician office staff who directly access Triad clinical applications on several key topics:

- Outline the Triad commitment to information security
- Review the primary risks to patient data
- Inform you of our expectations for continued access

Triad commitment to information security means

- Understanding security risks helps protect our patient
 - Integrity of patient data and treatment orders is maintained through appropriate access
 - Proactively prevent unauthorized access
- Protection of the Triad reputation and the reputation of its partners and caregivers is a high priority
 - Negative publicity affects our reputation with current and future patients
 - Our reputation allows us to offer new services as community needs change

HIPAA Security Rule

According to the HIPAA Security Rule, each facility must take specific measures to protect the Confidentiality, Integrity and Availability of Electronic Protected Health Information (EPHI).

Confidentiality	Data or information must not be available or disclosed to unauthorized persons.
Integrity	Data or information cannot be altered or destroyed in an unauthorized manner.
Availability	Data or information is accessible and usable upon demand by an authorized person.

Protecting data is a legal requirement

- Compliance is **required** for federal regulations on confidentiality and privacy (HIPAA Privacy and Security Rules)
 - Unique user identifiers (login in accounts)
 - Access control (done through role based access at Triad)
 - Access monitoring
 - Authentication for each access (validating the identity)
- Prosecution of HIPAA complaints has been through Consumer Protection Statutes (e.g. civil suits and class action suits)
 - Both the hospital AND individuals are at risk under these laws
- Compliance is required under state civil codes specifically regarding financial or medical identity theft

State legal requirements

- Several states have enacted consumer friendly identity theft laws (similar to the state of California)
 - They require organizations that collect **SSN, date of birth, or banking information** to notify individuals if their electronic information has been accessed by unauthorized individuals
 - They require partners who collect and manage this information to inform the organizations responsible if they have security breaches (hosting companies, contracted service providers, etc.)
- As of **January 2007**, **Triad facilities in several states must be compliant** with state civil codes to inform residents of breaches of their information
 - Arkansas
 - Arizona
 - Georgia
 - Indiana
 - Louisiana
 - Nevada
 - Tennessee
 - Texas
- Additional statutes directly address protection of Social Security Numbers in additional laws

What is identity theft?

- Fastest growing crime according to the FBI
- Definition
 - Deliberate assumption of another person's identity, usually to gain access to their finances or frame them for a crime, or commit other acts of fraud
 - It may also be a means of blackmail, especially if medical privacy or political privacy has been breached
- Primary targets are financial organizations, retail establishments, and **healthcare organizations**
 - The average patient does not realize that ePHI includes clinical data, and personal identity information. Patient demographics provide everything needed to establish fraudulent identities
 - Small organizations are targeted because security standards and technology are often less stringent than larger facilities. Any facility connected to the Internet is at risk.

What is medical identity theft?

- A subset of Identity theft committed for specific financial reasons
 - To obtain medical services or goods for un-insured or under-insured patients
 - To submit false claims for medical services or goods not delivered to patients (individual or organized criminal activities)
- Presents **High** patient safety risk
 - Patient safety issues with erroneous entries added to existing medical records (erroneous historical treatments, changes in blood type, etc.)
 - Hard to detect unless patient understands the need to review and verify his medical record information
 - Will become harder to correct as widespread use of electronic medical records grows



What can you do to protect patient information (both ePHI and identity)?

- Enforce appropriate access to patient information
- Practice good password management
- Inform us when you have staff changes

Appropriate access levels

- Only access the **minimum** patient information needed for your job
 - Clinical information only
 - Financial information for reimbursement purposes
- If access to information on family members or friends is required by your **job**, ensure your manager is informed and has approved
- Remember, access to patient records is audited and violations can result in removal of electronic access

Preventing wrongful access

- Use your own login account
 - Everyone must have their own login account
 - Accounts that have been inactive for weeks should be deleted
- Don't share your login account under any situation
- Don't login and let someone else use the session
 - You will be held responsible if there is inappropriate access
 - Individuals who have a legitimate need for access should request their own account
- If your account is locked and you don't know how this happened – this could be an intrusion. Call the facility Help Desk as soon as possible.

Password management

- Protect your password
 - Keep them to yourself
 - Don't allow others to give you their passwords
 - Remind anyone who asks you for yours it is not appropriate
 - Avoid writing the password down but if you have to, protect it as you would your own cash or credit card
 - **Never** leave passwords near the workstation
 - Always use different business and personal passwords
- If you suspect someone has learned your password, change it and report the event
- Create a password “strategy” that helps you create passwords you can remember and type easily, but that can't be easily guessed.

Creating strong passwords – what to avoid

- Common words, slang, or jargon
- Passwords that are the same as the account ID
- Names of software programs, applications, or companies
- Names of family members or pets
- Birthdates, anniversaries, current telephone numbers
- Hobbies, favorite movies, or books
- Words that have some “relationship” to you personally

These common approaches are well known by those who attempt to crack passwords – don't help them!

Creating strong passwords - recommendations

- At least 8 or more characters
- Use a combination of upper and lower case and capitalize letters in unusual places (i.e. heAlthier)
- Intentionally misspell a word or phrase (heAlthear)
- Include symbols and special characters as replacements for some of the letters (i.e. h3Althear)
- Use a pass phrase as a memory trigger and replace parts of the phrase with numbers, symbols, or abbreviations

Creating pass phrases

- Start with a random sentence easy to remember but harder to guess
- Collect the first letters from the phrase
- Replace some of the letters with upper case, capitals or symbols
- Practice typing the new password so your fingers “remember”

I saw a duck in a tree

- Take the first letter of each word – isadiat
- Substitute the number 5 for the S
- Add a couple of upper case letters
- Your password becomes **“I5adiaT”**

Good habits pay off

- While it is slightly inconvenient, a good password strategy can stop inappropriate access in many cases
- Inform us immediately of staff changes so we can update access appropriately
 - Generic accounts are not appropriate for access to ePHI
 - We monitor individual access
- Information security isn't hard when it is practiced enough to become a habit
- Put yourself in your patient's place – your financial and personal well being are either protected or at risk by the staff and physicians you work with

Requirements for non-employee access

- Access to Triad applications is provided for our partners' and staff's convenience **provided they practice the same due diligence and protection of ePHI expected of Triad employees**
- Electronic access may be removed if we determine you are not attempting to enforce
 - Password management
 - Individual accounts
 - Appropriate access

What if your bank's employees...

- Shared passwords that could access your bank account?
- Posted passwords in plain sight?
- Chose simple, easy to guess passwords
- Allowed accounts to be active for employees who were no longer employed
- Gave information over the phone to people they had never met that allowed strangers to access your account?

The confidentiality, integrity and availability of protected health information is invaluable to our patients!

Triad Information security framework

- Blue Book policies provide guidelines for information security
 - Information Security policies (IS001 – IS023)
 - HIPAA Privacy policies (HIPAA001 – HIPAA023)
- Annual security awareness training is required by HIPAA (staff end users include technicians, nursing, admissions, business office, etc.). Stay up to date on the requirements for privacy and security
- Confidentiality and Security agreements document user responsibilities
 - Updated as requirements evolve
 - Renewed annually
- Triad facilities appoint Local Security Officers
 - Enforce policies and investigate security incidents
 - Educate and assist everyone on information security requirements
- Triad Compliance Hotline (800 345-8650) is available for anonymous reporting of policy violations
- Facility IS Help Desk can answer questions about possible security incidents and best practices

Final thoughts on information security

- The success of criminals does not depend on their technical abilities, but the lack of technical abilities or awareness on the part of their victims.
- Don't be a victim at home or at work – learn what you need to do to protect yourself and your patients.
- The most effective security defense we have is our workforce:
 - Each person is critical to patient health and the protection of sensitive data
 - Each plays a role in maintaining our company reputation, image, and success
 - People are the most effective security monitors we can have