



Information Security for Physicians

Training year 2007



Objective

This short, informational briefing is designed to update professional staff who directly access clinical applications on several key information security topics

- Outline the Triad commitment to information security
- Review the risks to patient data
- Inform you of our expectations for employee and non-employee workforce



Triad commitment to information security

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

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)
 - Growing number of cases under state identity theft protection
 - As a result of growing publicity on identity theft, case resolution is nearly **always** in favor of the plaintiff (e.g. the physician and hospital administration should have known better)
 - Both the hospital AND individuals are at risk in civil litigations
- 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
 - Less commonly, it enables illegal immigration, terrorism, espionage, or changing identity permanently
 - 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 frequently targeted because security standards and technology are often less stringent than larger facilities. Any facility connected to the Internet is at risk and criminals attempt to access the data undetected so they can “harvest” identities on an ongoing basis.

Identity theft attempts have multiple sources

- Primary risk comes from computer hackers and criminals
- Secondary risks include
 - Inappropriate access by family members or their friends from home computers (i.e. new cases of teenagers setting up false identities to obtain credit cards, curiosity about celebrities and public figures, etc.)
 - Loss or theft of electronic equipment with sensitive information
 - Laptop computers
 - Hand held computers, blackberry devices, and phones that are capable of storing files
 - Removable storage drives (USB drives, iPods, etc.) allow large amounts of data to be copied without detection.

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)
- Physician identity theft risks
 - Theft of a physician name and license number is starting point for criminal activity
 - Electronic access presents opportunity to collect electronic signatures
- 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

To protect patient information, we ask our physicians and professional staff

■ Manage passwords

- Develop a password strategy and change passwords regularly
- Do not share passwords with others (sharing or using another person's account/password is a policy violation)

■ Safeguard remote access

- Don't use the same passwords for patient access as you use for home systems
- Do not access patient information from public computer systems (hotels, conferences, etc.)
- Use Secure remote cards or software tokens when required

■ Protect patient data forwarded to mobile devices

- Safeguard laptop computers left in your office or car and when traveling
- Encrypt data if possible
- Report the loss or theft immediately to the local Security or Privacy Officer



Disciplinary actions for policy violations

- Non-employees and professional staff may have access removed
- Employees may be suspended or terminated
- Individuals may face criminal or civil charges at the federal or state level

Triad Information security framework

The Triad Information Systems Security framework is available to all Triad employees, physicians, and partners as a guideline for ongoing operations

- Blue Book policies provide guidelines and minimum information security requirements
 - Information Security policies (IS001 – IS024)
 - HIPAA Privacy policies (HIPAA001 – HIPAA023)
- Annual security awareness training is required by HIPAA (staff end users include technicians, nursing, admissions, business office, etc.)
- Confidentiality and Security agreements document user responsibilities
 - Updated as requirements evolve
 - Renewed on update or every 2 years
- Local Security Officers or Triad Corporate Information Security Officer
 - Field questions and concerns on data protection and policies
 - Educate and assist everyone on information security requirements
- Local Physician Management Office
- Compliance hotline 800 345-8650

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



Additional Resources

Additional resources are provided in this section if needed:

- Password management guidelines
 - What to avoid
 - Recommendations
- Best practices for working from home computers
- Protecting laptops and PDAs

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

Recommendations for strong passwords

- 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

NOTE: These password examples are NOT good ideas for passwords since they have been shared with most of the workforce.

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**”



Additional password and user IDs protection

If an application doesn't automatically enforce it, you can still

- Change your password every 90 days
- Don't use the same password more than once in 12-month period.
- Never use a generic or “shared” account to access applications that contain sensitive data, such as electronic protected health information (EPHI).

Best practices for working from home

- Install anti-virus software on your home PC
- Set the anti-virus software to automatically update
- Set up an automatic update of the Windows operating system using Windows Update so that every Microsoft update will automatically be applied
- Don't trade files between your work computer and home system without scanning the files individually
- Use spyware scanning or protection software (also free or low cost)
- Clean up files as you go
 - Keep sensitive data within the primary environment
 - Clear browser cache

Protecting laptops and PDAs

- Some states do not require breach notification if the data is encrypted
 - There are low cost and free versions for personally owned equipment to encrypt hard drives and folders
 - Triad provides laptop encryption for all owned devices
- Use lockdown cables to secure your laptop at your workstation.
- Lock up your PDA when it is not in use.
- When traveling with a PDA or laptop
 - Never leave unattended in public areas (airports, restaurants, etc.)
 - Never check it as baggage.
 - If your PDA or laptop is stolen, report it immediately to your help desk or security official