Information Security Handbook for Employees

Providing our patients with excellence in healthcare includes protecting their information.
This handbook was prepared by Tom Walsh Consulting, LLC for the Kansas Hospital Education and Research Foundation as part of our work with the Kansas Regional Extension Center, under grant #90RC0003/01 from the Office of the National Coordinator, Department of Health & Human Services. (November 2011)
Confidential Information

Confidential information is any information considered to be private and sensitive.

Here are some examples of confidential information:

- Protected Health Information (PHI) *Information about patients*
- Social Security numbers (SSN) *Employees or patients*
- Credit card information
- Financial records
- Passwords, PINs, or other security codes

Confidential information takes on many forms. It can be information printed on paper, or data files stored on a computer, a hand-held device such as a BlackBerry Smartphone, computer media, or voice mail. Regardless of the form it takes, you are responsible to protect it from unauthorized disclosure or modification. Therefore, use only approved procedures when handling confidential information, especially when using the Internet, email, or a fax machine. Your supervisor or our Privacy Officer can provide specific guidance on how to properly handle confidential information.

Access Privileges

To obtain access to an application or computer system, an access request form must be completed and submitted to the Information Technology (IT) department. Contact the IT Service Desk at (extension #) for assistance with the request form.
The computer systems and the kinds of information you are permitted to access are based on your job duties, responsibilities, and a “need to know.” However, access to a certain system does not imply that you are authorized to view or use all the information on that system. Ask your supervisor if you have any questions regarding the kinds of information you are allowed to view or use on a computer system.

Management may limit or deny anyone’s computer access privileges at any time. Reasons for denying access privileges include, but are not limited to, the following:

- Change of job duties or employment termination
- Failure to comply with policies and procedures
- Conduct that interferes with the normal and proper operations of computer systems
- Activity that adversely impacts the ability of others to use computer systems
- Behavior that is harmful, unprofessional, offensive, or harassing to others

**User IDs**

Your user ID uniquely identifies you. You are responsible for all actions associated with your user ID; therefore, it is important to ensure that your user ID is used only by you and no one else.

You will be held responsible for the actions of another individual if you allow them to obtain and use your user ID and password or allow them access to patient information in a clinical application while you are logged on.
Password Protection and Creation

Protecting your password is a critical factor in protecting confidential information; therefore, passwords should be:

- Memorized and never written down in such a way that others can see or use them
- Kept a secret from others

Be aware of scams to trick you into disclosing your password through anonymous phone or email. Under no circumstances should anyone ever ask you for your password or should you voluntarily give it out. You and your supervisor can work directly with IT to set up limited access to files or folders without having to share your user ID and password.

Likewise, you must not attempt to learn another person’s password and/or access another person’s account using their password.

Care should be taken when selecting a password. A poorly chosen password compromises security. Create a “strong” password by following these simple rules:

- It should be at least eight or more characters in length
  (Tip: The longer your password is, the harder it is to break)
- Use at least one upper and one lower case letter
- Use at least one number
- Use at least one special character such as * ? # @ & $
- Avoid using common words that can be easily guessed
- Avoid using personal information such as your child’s name, favorite sports team or pets
Creating a good password can be quick and easy. One method is to use the first letter of each word found in a favorite quote or song lyrics followed by some numbers. For example, for the song, “Oh When the Saints Go Marching In,” the password would be: Owtsgmi.

The strength of the password could be improved by simply changing one of the letters to a special character and adding a number to the end so that the password becomes: Owt$gmi1.

**Computer Workstations**

Position workstation monitors to be facing away from the public view. Log off or lock your computer workstation whenever leaving it unattended. Also, log off when you are leaving your work area, especially at the end of your shift. Leaving a workstation logged on and unattended could lead to an unauthorized access of confidential information.

**Personally Owned Devices**

The IT department must approve any personally owned devices (including, but not limited to, laptops, tablets, iPads, and digital cameras) prior to being connected to workstations or the internal network. [Image] offers a “guest” wireless network for our patients, visitors or contractors. You may use personally owned devices with the guest wireless network on your personal time.
Working from Home

Requests to work from home must be approved by management. While working from home, you are personally responsible for securing information in the same manner that it is protected at work.

Personal Use

Computer systems are intended for business purposes. Limited personal use is permissible as long as it is approved by your supervisor and is on your own personal time.

Email

Organizational email is for conducting work-related communications. Incidental (personal) use is permitted if approved by your supervisor.

You are responsible for all activity on your assigned email account.

Exercise good judgment when reading email. The IT department has employed security controls to prevent most of the unwanted emails from reaching our systems.

However, avoid opening any suspicious emails and attachments from unknown senders. Be aware of hypertext links within an email; it may be a scam.

Secure web mail has been implemented by IT and is used to encrypt outbound email containing confidential information. Contact the IT Service Desk at (extension #) if you need help using this important tool.
Internet Access

Internet access is provided to authorized individuals who have a legitimate business need. The IT department filters and monitors all Internet connectivity. The ability to connect with a specific website does not in itself imply that it is permitted. If you discover that you have inadvertently connected to an inappropriate website please disconnect from that site and notify the IT Service Desk at (extension #).

Additionally, streaming audio or video is prohibited without management approval.

Inappropriate Activity

Under no circumstances should organization-owned (or hospital-owned) systems be used for gambling, personal profit, or to download, distribute materials, comments, pictures, or other forms of communication of a sexual nature or which are otherwise obscene, intimidating, offensive, or create a hostile work environment. Misuse of privileges which exceeds the bounds of our values and generally accepted standards of good taste may result in disciplinary action and in some cases, termination of your relationship with our organization. Additionally, violations of federal, state, and local laws and regulations may result in civil or criminal penalties.

You must not post work-related information to a personal (non-work related) social networking website.
Individual Fines for Willful Intent

Our Sanction Policy is used as guidance for when disciplinary action needs to be taken for a variety of situations ranging from a coaching session for accidental disclosure of PHI to termination for deliberate acts which violate our policies or confidential agreement.

Additionally, you may be personally fined by the Federal government and the State Attorney General under the HITECH Act of 2009, (part of Public Law 111-5) if you act with willful intent and violate our policies regarding the protection of patient privacy.

Under the law, healthcare organizations must report all data breaches whether intentional or unintentional. The name of the individual responsible for an unintentional breach does not get reported to the Department of Health and Human Services.

Auditing and Monitoring

Computer systems are intended for business use. Periodic monitoring and auditing are performed on our applications and systems to ensure appropriate use of files, applications, email, and Internet. For purposes of managing systems, troubleshooting problems, and enforcing security policies, the IT department may periodically monitor your computer activity.

There is no expectation of privacy when using organizational computers or networks.
Please note that some electronic communications, such as email, voice mail, and files stored on the network, still exist on backup media even after you may have deleted them.

**Reporting Security Incidents**

Notify the IT Service Desk at (extension #) and your supervisor if you become aware of or suspect the following:

- Theft of or damage to equipment
- Unauthorized use of user passwords
- Policy violations
- Any other problems or questions with information security or patient privacy

Your supervisor or the IT Service Desk will also notify our Privacy Officer or our Information Security Officer.

We will not take punitive action against any individual making a good faith report regarding behavior that is illegal and/or against policy.

**Backups**

Store files on a network file server (such as the Z: drive) which is backed up daily by IT. Important information should be stored on a network drive and not on an internal hard drive.

**Protecting Media**

Due to the risks and penalties associated with a disclosure, confidential information that is stored on portable media must be encrypted and securely handled. Confidential
information must be placed on a password protected USB drive approved by the IT department. Your supervisor should specify where media containing confidential information will be stored within your department.

*Note:* Media includes: Paper documents, CDs, DVDs, memory devices, USB flash drives, etc.

**Mobile and Portable Devices**

Mobile computing devices include laptops, tablets, iPods, Smartphones, MP3 players, digital cameras and other handheld computing devices. Being mobile, these devices are at greater risk for loss, theft, or other unauthorized access and require additional security and protection.

Consult our Information Security Officer for more details and our policy for using these devices for work.

**Installing Software**

Only licensed and authorized software approved by IT can be installed on organizational computers. No software from home is allowed. Unauthorized software found on your computer will be removed. Obtain permission from the IT department before downloading or installing any software to your computer.

Contact the IT Service Desk at (extension #) for assistance.
Quick Reference Information

Information Security Officer

_[Name and contact information here]_

Privacy Officer / Official

_[Name and contact information here]_

This handbook contains a condensed version of our policies regarding information security and is periodically revised.