Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Annual HIPAA Security & Information Security Competency

Swedish Medical Center

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

General Information

- FISO- What is a FISO?
  - Facility Information Security Officer
  - Responsible for the physical protection and recovery of all electronic information, ensuring compliance with the HIPAA Security requirements, and enforcement of HCA Information Security Policies
  - Who? Ralph Crow serves as Division FISO. Jeff Schnoor is the Swedish Medical Center FISO
- Helpdesk
  - When in doubt, call the Helpdesk?
    - All Phone, Computer, System issues should be called to the Centralized Service Desk (CSD) or more commonly known as the Helpdesk.
    - Can be reached at ext. 8710

Swedish Medical Center

HIPAA Security

- Federal Law
  - The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
  - The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

HIPAA Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Need to Know

- Information and Privileges are assigned on a “Need-to-Know” basis
  - **Wanting to know is different than needing to know**
- If you are not 100% sure that a person has a true need to know, you should refer the request to your manager
- Information and Privileges should be related to doing job
- If you feel someone is seeing information they have no need to see, please report it to your Manager, FISO, or the IT Helpdesk

Swedish Medical Center

HIPAA Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Sanctions Policy PRI.013

- Governs how we handle violations of HIPAA Security and Information security policies, guidelines, and standards.
- Examples of volitions are as follows.

Inappropriate access, use, disclosure, or disposal of sensitive information	Sending sensitive information via mail, email or fax to a non-authorized individual or the wrong provider
Sending sensitive information via email unencrypted	Improper protection of sensitive information

Health ONE Swedish Medical Center

HIPAA Security

Failure to properly sign-off a workstation	Failure to properly safeguard username and passwords and/or sharing passwords
Accessing one's own record in any system (unless otherwise permitted by HIM.PRI.004)	Intentionally bypassing Company network security controls for unauthorized reasons
Posting sensitive information on the internet or a violation of the Appropriate Use of Communications Resources and Systems policy, EC.026	Photographing a patient within the facility for personal use

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

HIPAA Security

Privacy & Information Security Policies and Procedures

- Applicable Corporate, Information Security policies, Standards and Guidelines are found on Atlas at:
  - **http://atlas2.medcity.net/portal/site/infosec/**
- Applicable Market Policies are Located on the HealthONE Intranet:
  - **Under Policies --> HealthONE P&Ps →HIPAA → Information Security**
  - **Market Sanctions Policy PRI.013**
  - **Under Policies --> HealthONE P&Ps →HIPAA → Healthone Patient Privacy**

HealthONE Swedish Medical Center

HIPAA Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Types of Restricted and Sensitive Information

Restricted

- Information that if disclosed could result in serious or material damage to HCA, the data owner, or other stakeholders
- Information that controls access to other information
- EXAMPLES:
  - Passwords, Secure ID PINs
  - Credit Card #s, Financial Acct #s
  - Merger information, Strategic planning

HIPAA Security

Types of Restricted and Sensitive Information

Confidential

- Information in which an outside party shares ownership or rights
- Information with confidentiality requirements controlled by some regulating body
- ePHI (electronic Protected Health Information)
- Information that, if disclosed, could cause significant damage to HCA, the data owner, or other stakeholders
- EXAMPLES:
  - Social Security #s, Identifiable patient data
  - Employee Human Resources file

Information Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Password Maintenance

- **MOST IMPORTANT:**
- **Whenever the system is capable, passwords must be a minimum of 7 characters, at least one character must be a capital letter, and at least one character must be a number**
- **Don't use something easy to guess such as a spouse's name or pet name, or date of birth, etc.**
- **DO NOT share your password for ANY system with ANYONE for ANY reason….EVER!!!!!**
- **YOU are responsible for anything that happens while that password is being used**
  - **Don't leave yourself logged in when you walk away**
  - **Change password if you think it is compromised**
  - **Create Good Password (see Security Awareness Guide)**

Swedish Medical Center

Information Security

Login Failure or Success

- **Make sure when you login, that you are getting the correct warnings/agreements**
- **Make sure you get the right programs or capabilities**
- **If something looks wrong, let the IT&S Helpdesk know so it can be checked out**
- **Make sure you logout when you leave the workstation**

Information Security

Use of Email

- **Primary use of E-Mail is Business**
  - Can also use for limited personal e-mail from family & friends.
    - Ensure it is minimal and does NOT interfere with doing your job
    - All e-mails are “discoverable” by Company
  - **NEVER pass on a chain-letter/chain e-mail**
    - Anything that says to send on to other people or something bad, or even something good will happen
    - This includes anything that you feel might be humorous or was sent to you from someone outside the organization that doesn’t have a business purpose. What may be funny to one person may be hurtful to another.

Information Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Use of Email

- **NEVER** send a threatening e-mail
- **NEVER** send an insensitive e-mail
  - Sexual, Religious, Racial
  - Anything that makes fun of another group of people
- **NOT** used for personal items
  - Selling
  - Trading, etc
- **NEVER** use email to transmit work related material to a home or personal account.

Swedish Medical Center

Information Security

Use of Email

- **ENCRYPTION**
  - All emails sent to someone outside of the organization that contain confidential or sensitive information must be encrypted.
  - Subject line should be prefaced with the word encrypt enclosed in brackets
  - *e.g. -* ***[encrypt] Patient Information, Doe, John***

Information Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Appropriate Internet Use

- Intended for Business
  - **All Internet use is Discoverable by the Company**
  - **Never visit inappropriate sites**
    - **If you go to one accidentally, leave the site immediately**
    - **NEVER Download anything inappropriate**
    - **NEVER Download Software**
      - **Check with IT&S**
  - **Can use for minimal personal use**
    - **NEVER interfere with Business**
    - **Consult your Manager/Director if in doubt**

Swedish Medical Center

Information Security

Viruses, Worms, etc.

- **We have Antivirus on all servers that scan for known viruses and other malicious agents**
  - **Most viruses are contained in attachments or in internet links, not the e-mail itself**
- **Can only catch KNOWN items**
  - **If something looks suspicious, report it to the IS helpdesk**
  - **If you get an e-mail that has an attachment or internet link and you do not recognize the person it came from, DON'T OPEN THE ATTACHMENT OR CLICK THE LINK**
    - **Report it to the IS Helpdesk**

Information Security

Social Engineering

- This is "Trickery" by someone trying to get you to provide information
- **Surveys either online or by phone**
  - Know who it is and the intent
    - » If suspicious, refer to your Manager

SPAM

- EX: Jokes, sexual drugs, e-cards (from unknown sources)

PHISHING (trying to get information)

- EX: e-mails from banks saying to give info
  - » If you did not request the person or company to do something for you, be very suspicious.

May ask for your password

- Never give out your password

Information Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Workstation Security

- NEVER leave yourself logged in when you are gone
- Position screens so information is not viewable by others who shouldn't see it
- Watch for unauthorized visitors
- When possible keep equipment behind locked doors

Protect Portable Media (anything that stores data and can be easily transported)

- Laptop/Tablet
- PDA/Mobile Phone
- USB / Thumb drive
- CD/DVD

Swedish Medical Center

Information Security

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Portable Media (Continued)

- **Lock up whenever possible**
  - **Includes at home when not in use**
- **When in transit hide from view**
- **Keep on person whenever possible**
  - **Never put in checked baggage when traveling**
  - **Place in space under seat not overhead bin**
  - **Pick up first thing when through Security Check**
  - **Lock up in hotel whenever possible**
- **If disposing, NEVER throw in trash**
  - **Give to IT&S for proper disposal**
    - **Simply breaking a CD/DVD in half is not sufficient**
- **Report Loss to IT&S IMMEDIATELY**

Information Security

Reporting Incidents

- If you notice something that looks suspicious, even a suspicion that someone is seeing information they have no need to know, REPORT IT to the IT&S Helpdesk
    - Helpdesk can be reached at extension 8710 or direct dialing 303-584-2232
- Refer to Security Policy on Incident Reporting on the HealthONE Intranet for specific details.

Ethics & Compliance

EC.026

- **What is EC.026?** It is the HCA policy that covers Appropriate use of Communications Resources and Systems.
- **Where can I find a copy?** Ethics and Compliance Policies on the Intranet or by contacting the ECO or FISO
- **What does it cover?** Appropriate use of Email, Internet, Company resources and systems. It also covers **Social Media** such as Facebook, MySpace, Twitter, Blogs, Wiki's, web diaries and more.

Ethics & Compliance

Social Media

- **NEVER** represent yourself as speaking for the company unless specifically authorized to do so
- **NEVER** post PHI or other sensitive information
- Social Media Activities are discoverable by the company if it is suspected that you have violated social media guidelines.
- Guidelines can be found on Atlas under keyword “Social Media”
- Sanctions for violations of the Social Media guidelines include disciplinary action up to and including termination depending on the severity of the violation.

Ethics & Compliance

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Social Media Violation Examples

Jamie has been working in hospice care for the last six years and one of her patients, Maria, maintained a hospital-sponsored communication page to keep friends and family updated on her battle with cancer. One day, Maria posted about her depression. As her nurse, Jamie wanted to provide support, so she posted, "I know the last week has been difficult. Hopefully the new happy pill will help, along with the increased dose of morphine. I will see you on Wednesday." The site automatically listed the user's name with each comment.

The next day, Jamie was shopping at the local grocery store when a friend stopped her to ask about Maria's condition. "I saw your post yesterday. I didn't know you were taking care of Maria," the friend said. "I hope that new medication helps with her pain."

Swedish Medical Center

Social Media Violation Examples

This is an example of a violation of confidentiality through social media. While Jamie had Maria's best intentions at heart by trying to offer her words of support, she inadvertently disclosed information about a patient on a social media site.

Everyone who read that post now knows about Maria's medication and increase in morphine, violating her right to privacy and confidentiality.

Instances of inappropriate use of electronic media by nurses such as this have been reported to boards of nursing (BONs) and, in some cases, reported to the media.

Ethics & Compliance

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

Social Media Violation Examples

Emily, a 20-year-old junior nursing student, wasn't aware of the potential repercussions that could occur when she took a photo of Tommy, a 3-year-old leukemia patient in a pediatric unit, on her personal cell phone. When Tommy's mom went to the cafeteria, Emily asked him if she could take his picture, which Tommy immediately consented to. Emily took his picture as she wheeled him into his room. She posted Tommy's photo on her Facebook page with this caption: "This is my 3-year-old leukemia patient who is bravely receiving chemotherapy! He is the reason I am so proud to be a nurse!" In the photo, Room 324 of the pediatric unit was visible.

Days later, the dean of the nursing program called Emily into her office. A nurse from the hospital found the photo Emily posted of Tommy on Facebook and reported it to hospital officials who also contacted Emily's nursing program.

Swedish Medical Center

Social Media Violation Examples

While Emily never intended to breach the patient's confidentiality, the hospital faced a HIPAA violation. From Emily's post, people were able to identify Tommy as a cancer patient and the hospital where he was receiving treatment.

School officials expelled Emily from the nursing program for breaching patient confidentiality and HIPAA violations. The nursing program was also barred from using the pediatric unit for their students. Emily's innocent, yet inappropriate action of posting a patient's photo had repercussions for her, the nursing program and the hospital.

Annual HIPAA Security & Information Security Competency

Patient Satisfaction

Constant Courtesy

Teamwork & Respect

Personal Responsibility

Professionalism

- You have completed the module on HIPAA Security & Information Security.
- Please complete the quiz.

Thank you for your time.

Swedish Medical Center