Privacy & Security of Patient Information Student Training

S&W PRIVACY UPDATE

This module is intended to review the policies and procedures of Scott and White that address the HIPAA Privacy Regulations.

The module is organized to address the following topics;

- **Introductory information on HIPAA**
- **Organizational Responsibilities**
- **Guidance for Staff**
- **Patient's Rights**
- **Reporting Concerns**

What is HIPAA?

HIPAA stands for the

"Health Insurance Portability and Accountability Act".

It covers three areas.

- **Insurance Portability** (Ensures continuity of coverage when changing health plans)
- **Accountability** (Fraud Enforcement)
- **ADMINISTRATIVE SIMPLIFICATION** includes these three provisions
  - **EDI** (Electronic Data Interchange) is standardization of Electronic transactions.
  - **Security** is the protection of electronic health information.
  - **Privacy** addresses protecting the patient's privacy of Protected Health Information (PHI)

HIPAA: Privacy & Security of Patient Information

What is Protected Health Information (PHI)?

- PHI is individually identifiable information that is maintained or transmitted in any form by S&W.
- PHI is any information, verbal or recorded, relating to the health, healthcare or payment for health care provided.
- The information does not have to be created by our organization to be considered PHI.

HIPAA: Privacy & Security of Patient Information

PHI comes in many forms:

- Electronic (computer, mobile device, fax, email)
- Paper
- Verbal
- Photography, filming & recordings

PHI is not limited to a patient's clinical information.
It includes any information that can identify the patient.

Examples: Name, MRN, Address, SS#, Date of Birth,
Billing Information, Photos, Telephone #

HIPAA
Organizational Responsibilities

Treatment, Payment & Health Care Operations (TPO)

S&W is allowed to use and/or disclose PHI in the normal course of providing health care and related business.

Treatment is the coordination of health care or other services.

Payment includes billing, claims management, medical necessity, utilization review activities, determination of coverage.

Health Care Operations includes

quality improvement activities, credentialing, training, underwriting, compliance services, business planning and development, business management and general administration.

HIPAA
Organizational Responsibilities

Notice of Privacy Practices

- A S&W document given to each patient at the first point of service
- Details how S&W uses, discloses and protects PHI for purposes of treatment, payment and health care operations.
- Defines the patient's rights under HIPAA
- Explains how S&W uses PHI for Marketing, Fundraising and Research
- Explains how to file a complaint at S&W or with the Department of Health and Human Services.

HIPAA
Patient Rights

HIPAA gives specific rights to patients. These rights give patients more control over how their health information is used/disclosed.

- **Right to Access PHI-**
  - ✓ A patient can request to review or obtain copies of their PHI.
  - ✓ S&W follows STATE LAW and HIPAA for review and release of PHI.
  - ✓ Patients requesting access to their records should be directed to **Medical Records Release of Information Department (ROI).**
  - ✓ If information is released from other areas the patient should complete the S&W authorization form and this form should be sent to the Health Information Management Department with documentation of what was released and when.
  - ✓ A patient may revoke an authorization, in writing, at anytime.
  - ✓ **Employees should access PHI for personal use through the ROI department or their attending/treating physician.**

- **Right to Request an Amendment to PHI**
  - ✓ A patient has the right to request an amendment to their medical record.
  - ✓ Requests for amendments will be reviewed by the physician responsible for the documentation.
  - ✓ Patients must submit a written request (S&W Request for Amendment of Protected Health Information) to the **Patient Relations Department** or contact them at 724-3035.

HIPAA
Patient Rights

- **Right to Request Restrictions**
  - ✓ A patient has the right to request restrictions on the use and disclosure of their PHI.
  - ✓ Such requests will be reviewed on a case-by-case basis.
  - ✓ HIPAA does not require S&W to accommodate all requests.
  - ✓ Patients should submit a written request (SW Request for Restrictions on Medical Information) to the **Patient Relations Department** or contact them at 724-3035.

- **Right to Request Confidential Communications**
  - ✓ A patient can request that we communicate with them by an alternate means or at an alternate location.
  - ✓ S&W must accommodate reasonable requests for the communications. Examples might be requests that information be sent to a work address/phone # rather than a home address/phone #.
  - ✓ Patients must submit a written request (S&W Request for Confidential Communications) to the **Patient Relations Department** or contact them at 724-3035.

HIPAA
Patient Rights

- **Right to an Accounting of PHI Disclosures**
  - ✓ A patient has a right to an accounting of the disclosures of their PHI that S&W has made without an authorization.
  - ✓ There are exceptions for the accounting. Disclosures that will NOT be listed in the accounting include disclosures for treatment, payment, health care operations or PHI released with a signed authorization.
  - ✓ Patients must submit a written request (S&W Request for Accounting of Disclosures) to the **Patient Relations Department** or contact them at 724-3035.

- **Right to File a Complaint**
  - ✓ A patient has the right to file a complaint if they believe their privacy rights have been violated.
  - ✓ To file a complaint with S&W contact **Patient Relations**, (254) 724-3035
  - ✓ **To file a complaint with the US Dept of Health and Human Services, Office of Civil Rights (OCR), call toll free 1-800-368-1019.**

Penalties

Enforcement of Privacy Regulations by OCR

- Enforcement responsibility of the Office of Civil Rights (OCR) under the US Dept of Health and Human Services.
- There are severe **civil and criminal penalties** for improper disclosure, disclosure under false pretenses, and disclosure made out of malice or commercial purposes.
- **Privacy & Security violations must now be reported to the patient and the OCR**
  - Penalties up to $1.5 million
  - civil and criminal penalties may be imposed including up to 10 years in Prison
  - Physicians and employees can be held **personally liable** of violating a patient's privacy.

Sanctions within S&W

HIPAA requires S&W to

- establish disciplinary sanctions for staff who fail to comply with its privacy policies and procedures, and
- ensure that those sanctions be applied **consistently at all levels** of the organization.\

Violations of privacy or security can result in disciplinary action up to and including termination from S&W Program.

Privacy & Security Breach Notification

Effective September 2009

- "Unsecured" PHI that is breached (intentionally or inadvertently) - Scott & White
  - Must notify patients & Office of Civil Rights (OCR) of unauthorized
    - Access (internal & external)
    - Acquisition
    - Use
    - Disclosure
  - If unable to identify patients or more than 500 patients affected must report in local media and on Scott & White Internet Site
- "Unsecured" PHI is defined as any
  - Electronic PHI that has not been secured by encryption
  - Paper that has not been rendered unusable, unreadable, or indecipherable (i.e. cross-cut shredded or handled in secure manner through confidential waste procedures)
- Includes all forms of PHI
  - Electronic
  - Paper
  - Verbal
  - Photography, filming & recordings

Privacy & Security Breach Notification

- "What S&W Students can do to secure PHI
  - Do not save patient information to laptop, computer, mobile devices, CD, DVD, external drives, USB (flash) drives (unless encrypted)
  - Use only encrypted mobile devices – laptops,USB (flash) drives, etc
  - Do Not use cell phones, smart phones for communication about patients or photos
  - Verify Faxes received appropriately by outside recipients
  - Dispose of paper in the appropriate confidential waste containers
  - Protect visibility of documents and computer screens
  - Avoid carrying paper PHI outside of a S&W facility
  - Log off computer before walking away
  - Notify Corporate Compliance Department immediately of any lost or stolen computers or devices, any inadvertent disclosures, and any potential breaches (i.e. via fax, email, paper, verbal, etc)

Breach Examples that must be reported (not inclusive)

- Lost or stolen Laptop, Desktops
- Lost or stolen mobile devices (blackberry, IPhone, flash (USB) drives, CDs, etc)
- Paper PHI left unsecured (regular trash, left in the cafeteria, in public access areas, taken outside of S&W, etc)
- Paper PHI that has been lost or stolen
- Photos, filming, recordings on cell phones or cameras by staff, residents, etc
- Faxes to wrong numbers
- Mail containing PHI sent to wrong address
- Email containing PHI sent to wrong email address
- Unauthorized access by staff
- Discussion of patient's on social media sites (facebook, twitter, MySpace, etc)
- Verbal communication about patient shared inappropriately with someone other than patient
- PHI accessed appropriately for business purposes but disclosed beyond business purposes

HIPAA
Guidance for Staff

Disclosure Concerns

- Implied Consent – We may make verbal disclosures to family or close friends, if we can infer from the circumstances (i.e. they are in the treatment room) that the patient would not object to the disclosure. The patient should be given the opportunity to object to the disclosure.
- Patients with Dementia - We may disclose health information about the patient to someone who has Medical Power of Attny, cares for the patient or has an established legal right.
- Minors – HIPAA regulations direct us to STATE LAW. There are no changes from current requirements under state law.
- Emergency Situations -If the patient is unconscious or in an emergency situation and is unable to opt-out, use your best judgment about disclosures.

Use Professional Judgment
Make a decision that is in the patient's best interest.

HIPAA
Guidance for Staff

Verifying the Requestor

Before providing patient information, we must take reasonable and appropriate measures to verify that the requestor has a right to that information.

- Suggestions on information that can be used to verify the identity and authority of an individuals requesting information are
  - ✓ Date of Birth
  - ✓ SS#
  - ✓ Address or Phone Number

- Caution – There are some instances when a family member or ex-family member may know the appropriate information and may not have a right to patient information without the patient's authorization. (spouse, parent of adult child)

Use Professional Judgment
Contact your Supervisor

HIPAA
Guidance for Staff

Minimum Necessary

- You should **ONLY** access and use the information you need to perform your job.
- Minimum Necessary also applies to when we are requesting or disclosing information to other health care providers.
- Minimum Necessary does **NOT** apply in the treatment setting.

HIPAA
Guidance for Staff

Opting-Out of the Facility Directory

- HIPAA allows only the following information to be included in the facility's inpatient directory
  - ✓ Patient's Name
  - ✓ Location (Room #)
  - ✓ Condition, in general terms
  - ✓ Religious Affiliation

- A patient may "opt out" and request their stay at S&W remain confidential.

- Patients who have "opted-out" of the facility directory will not receive calls, flower/gift deliveries, and family/friends asking for their room location will not be given any information.

HIPAA
Guidance for Staff

Law Enforcement and Other Officials Requesting PHI

S&W may disclose health information to law enforcement officials without the patient's authorization BUT we must ensure that the disclosures are appropriate and follow HIPAA and STATE LAW.

Therefore,

Refer all law enforcement individuals, calls and/or requests for patient information to

- Legal or Risk Management, 724-4127
- 50 Nurse

HIPAA
Guidance for Staff

HIPAA
Privacy & Security of Patient Information

Photography, Filming, & Recording of Patients

- Permitted Only for Treatment, Identification or Diagnosis
- Photography, Filming, Recording Consent needed for non-patient care purposes (identified or de-identified) for
  - ✓ S&W Education/Training
  - ✓ Quality Improvement Activities
- Marketing Purposes
  - ✓ External Purposes that will be seen or heard by the public
  - ✓ Separate marketing consent required
- S&W Policy SW.051 Guidance for Photography, Recording or Filming
- Must have documented reason for Photography, Recording or Filming that complies with permitted uses

HIPAA
Staff Responsibility

Personal Use of Patient Information

S&W Staff are given access to the minimum amount of patient information necessary to perform the duties associated with their jobs. Staff can ONLY access, review or use/disclose information as it pertains to their specific job responsibilities.

As S&W employees, we should **never** access patient information for personal reasons. This includes paper records and all information systems available to you at Scott & White.
As employees we must remember:

Access to S&W records & information systems are for the business of Scott & White only.

Under **No Circumstances** should patient information be used or reviewed for personal use about you, a family member, an acquaintance, co-worker, employee, friend, etc.

Violations of Privacy are very serious and will result in disciplinary action up to and including termination.

HIPAA
Staff Responsibility

Examples of Personal (Inappropriate) Use

The following is not meant to be inclusive, but to give examples of misuse of Patient Information for personal reasons.

Do not:

- Access your own health information
- Access your family, friends, ex-family member's patient information
- Review patient information out of concern or curiosity
- Look up a staff member's medical or financial information for personal interest
- Do not post information about patients or work issues related to patients on social media sites (Facebook, MySpace, Twitter, YouTube, etc.)
- Look up birth dates, addresses, appointments, test results for family, friends, neighbors
- Review patient information to use in personal relationship
- Discuss patient information with family, friends, other staff when it is not related to the business of Scott & White
- Compile a mailing list from Scott & White records for any reason, except as defined by your job duties

HIPAA
Staff Responsibility

Business Purpose Use in Scott & White

There are times when “accessing patient information for the business of Scott & White would involve accessing our own or families information in these instances it is best to refer this responsibility to someone not involved on a personal basis (supervisor, co-worker, etc). Even friends or ex-family may be uncomfortable with an employee accessing their patient information and referring this patient to a co-worker may help avoid any conflicts.

HIPAA
Staff Responsibility

Handling of Paper PHI & Other Confidential Documents

Paper documents should be handled in a secure manner. The following guidelines should be followed:

- Handle documents securely – do not leave visible to the public or other staff who do not have a business reason to view information
- Do not leave documents unattended in a public area
- Dispose of documents in the appropriate secure confidential waste containers not the regular trash
- Do not take documents containing PHI off the S&W premises
- IV Bags, Med Bags, Prescription Bottles also contain confidential patient information and these should be disposed of in red hazardous waste bags.

HIPAA Security

Security of Electronic Information

- Three Components to HIPAA Security
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards

We all have responsibility to control access to sensitive data and Patient Information.

HIPAA
Guidance for Staff

Physical Security

- Secure rooms, work stations, mailrooms
- Place printers, fax machines, copiers in secure locations away from public
- Secure file cabinets, drawers, mailboxes that hold protected information
- Keep protected information from public view
- Do not play voice messages or hold sensitive conversations on a speaker phone

HIPAA
Guidance for Staff

Controlling Who Has Access

- Assign staff access only to the systems they need to do their job according to policy.
- When staff transfer access should be reevaluated & updated according to policy.
- When staff leave Scott & White access should be terminated according to policy.
- If unsure verify that staff &/or visitors have a right be in the area – don't assume

Role-Based Access

- You are given access to certain systems that are required to do your job – this should be on a "need to know basis" and only access what is necessary to do your job.
- You should not attempt to view information that you have not been given authorization to access.

HIPAA
Guidance for Staff

Computer Security

- Never leave patient information displayed on your computer
- Log out or lock down your computer if you step away
- Protect your Passwords
  - Change your password at regular intervals
  - Never write down your password
  - Do not share your password
- Create a strong password
  - Minimum of 8 characters in length
  - Does not include the User ID.
  - Does not include the same character 3 or more repeated times (e.g. AAA).
  - Composed of at least 1 character from the following classes:
    - Alphabetic: Upper Case (A - Z)
    - Alphabetic: Lower Case (a - z)
    - Numeric: 0 - 9

HIPAA
Guidance for Staff

Faxes

- Use a cover sheet that shows your contact information and a confidentiality disclaimer
- Confirm the recipient's contact information, including fax and telephone
- When sending a fax with sensitive data or patient information call receiver to confirm that fax was received
- Immediately remove confidential information
- Effective September 2009
  - Any faxes inadvertently sent to the wrong # should be reported to Corporate Compliance
  - Faxes sent to wrong phone number (outside of S&W) must be reported to the patient and to the OCR

HIPAA
Staff Responsibility

Laptop & Desktop Computer Use & Security

- Use of Scott & White Laptops and Desktop computers should be limited to Scott & White business purposes only. Most Laptops and some desktops have been encrypted.
- Avoid saving patient or other confidential data to a laptop or desktop computer that is not encrypted
- Use network storage instead of hard drive on computer – this can set up by sending an request for service to Information Systems.
- If you have a S&W computer that you must save PHI or other confidential information to – contact IS Security and request encryption if the device is not already encrypted.
- Report lost or stolen devices immediately
- Contact I.S. for proper “scrubbing” of data, email, etc from mobile devices no longer being used – just deleting files in not sufficient
- Personal Laptops and other devices that contain any PHI, business or other confidential information must meet S&W security standards (encryption, etc)

HIPAA
Staff Responsibility

HIPAA
Privacy & Security of Patient Information

Mobile Devices

Mobile devices include all of the following (not inclusive):

- Cell Phones, IPhones, Blackberries, IPaqs
- Netbooks
- USB (jump, flash) drives
- CD/DVD
- External hard drives
- Pagers with texting capabilities

Avoid using phones, PDA's to share PHI

Protect PHI or other confidential information on mobile devices by:

- Keep the device in your immediate possession or in a secure place.
- Password protect devices. Use encryption software (if available for that device).
- Use only encrypted USB Drives
- Delete confidential information from device immediately
- Protect the data:
  - Data should be encrypted to protect it. Depending on the device holding the data, there are different acceptable ways to encrypt the data. Contact Information Systems (by calling the Helpdesk at 724-2501) for assistance in encrypting data on mobile devices.

HIPAA
Guidance for Staff

Outside Data Storage

- S&W data and documents should only be saved to S&W encrypted computers or servers
- Never copy and paste patient medical record information and save to a computer (S&W or personal)
- Only use S&W encrpyted computers, network or servers to save S&W data or documents - Never use an outside storage source

Strongly encouraged to save to Network Drive (Home drive or other drive can be set up by Information Systems. If computer is lost, stolen or crashes data will be secure on network drive not computer hard drive.

HIPAA
Staff Responsibility

Disposal or "Scrubbing" of Electronic Media

- Simply deleting files from a device does not "clean" the confidential data completely off the device.
- Some electronic media can be cleaned ("scrubbed") by magnetic degaussing. "Erasing" is an insufficient method of cleaning data from electronic media.
- Cell Phones, Blackberries, IPhones, IPaq, PDAs, etc. should have all files deleted and you should perform a manufacturer's hard reset to reset the device back to its factory default settings.
- Physical disposal of electronic media is accomplished by shredding, pulverizing, incinerating or otherwise physically destroying the electronic media so it can not be reconstructed.
- If you have a device that needs to be cleaned ("scrubbed") contact the Information Systems Department Help Desk at 724-2501

Non-Retaliation Policy

Scott & White has a “non-retribution & non-retaliation” policy.

- This means no action of retaliation or reprisal shall be taken against anyone who reports issues to their supervisor, Corporate Compliance, external organizations or for calling the hotline to make a report, complaint or inquiry.
-
- Any concern of retaliation should be reported to Human Resources or Corporate Compliance immediately.

- However, calls to the hotline do not protect callers from appropriate disciplinary action regarding their own performance or conduct.

Examples of Retaliation

Whether an act is retaliatory depends upon the circumstances of each case.

- Examples of retaliatory actions, depending on the specific circumstances, might include (not all-inclusive):
  - Termination, demotion, denial of promotion or transfer
  - A material change in job duties to less desirable duties
  - Threats, unjustified negative evaluations, unjustified negative references, or increased surveillance
  - Temporary suspension (even if later reimbursed) could well dissuade an employee from complaining
  - Schedule changes that might not impact all employees, but may matter to a mother with school age children
  - Instructing employees not to report issues to Corporate Compliance or Human Resources
  - Exclusion from important meetings. Exclusion from lunch would normally be considered trivial; however, exclusion from a weekly training lunch that contributes significantly to the employee's professional advancement might be considered retaliation

Resources

- S&W Privacy & Security Handbook
  - Available on the S&W Intranet (Insite) – HIPAA Page
- S&W has policies and procedures in place that define how to protect the privacy and confidentiality of patient information at Scott and White.
- These procedures are available on the
  - ✓ **S&W intranet, InSite**
  - ✓ **HIPAA Intranet site**
- It is expected that questions will arise about privacy of health information and the policies and procedures for these requirements. Questions/concerns may be addressed to
  - ✓ **The Privacy Officer, Frank Anderson (724-4386) or**
  - ✓ **The Privacy Office, 724-7600**
  - ✓ **Email: HIPAA HIPAA**

HIPAA
Reporting Concerns

If you have questions or concerns regarding any of the privacy policies/procedures, you should contact the

- ✓ **Privacy Office: 254-724-7600**
- ✓ **Email: HIPAA@swmail.sw.org**

Serious concerns about suspected or known instance of potential violations of applicable law or regulations may also be reported through the Scott and White

Compliance Hotline at 1-888-800-1096.