This is the 2017 HIPAA Privacy & Security Refresher Training which focuses on key areas and is required for all workforce members.

The SHC workforce includes members of the Boards of Directors and Trustees and Board of Governors, employees, volunteers, medical staff members, medical and other students, scientific and research staff, interns, residents, fellows, allied health providers, and advanced practice professionals. Workforce members may also include select contractors, subcontractors, and consultants.

New workforce members are required to take the New Hire HIPAA Training in addition to this training.
This year’s Refresher Training will focus on three types Protected Health Information, which is also referred to as PHI, and safeguards to protect the privacy of our patient’s information.

**Remember that protected health information is identifiable information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of healthcare to an individual.**

These areas are:

- Verbal & incidental disclosures
- Paper, including notes, printing and faxing
- Electronic, including reports, applications, and devices

Before we get started, let’s review a few definitions concerning the use and disclosure of PHI.
In our daily activities, we may interact with patient information on an infrequent or regular basis. At times we may need to relay information to co-workers or provide information to others involved in a patient’s treatment. It is important to understand the definitions set by the Department of Health and Human Services in order to understand how to be compliant with the HIPAA privacy and security rules.

Use is defined as—with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Take note that use is between workforce members within an organization. So an example of use would be a nurse providing an update on a patient’s condition to a physician.

Disclosure is defined as—with respect to individually identifiable health information, the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Again, take note that disclosure is between a workforce member and someone outside of the organization. An example would be a provider disclosing health information to a health plan as part of a claim for payment.

Incidental disclosure is defined as a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that
is permitted by the Privacy Rule.

Building off what we discussed about disclosure, an incidental disclosure occurs when someone outside of the organization that is not involved in the treatment of the patient hears or sees PHI.

Examples of incidental disclosure may be a hospital visitor overhearing a provider’s confidential conversation with another provider or patient, or may glimpse a patient’s information on sign-in sheet.

Understanding the difference between use, disclosure, and incidental disclosure are fundamental concepts in understanding SHC privacy and security policies.
Under the HIPAA Privacy Rule, verbal communications require safeguards in order to protect a patient’s privacy.

The Privacy Rule does not prohibit incidental disclosure of patient information so long as reasonable safeguards are taken to minimize the disclosure. What is reasonable depends on the situation and the location. Every effort should be made to ensure the patient’s privacy and if a private room is in proximity it should be utilized, even if that results in minor inconvenience to clinical staff workflow.

Keep in mind, any discussion of highly confidential information, such as mental illness, developmental disability, HIV/AIDS testing or treatment, substance abuse, child abuse, must occur in a private area or room.

For example, in an emergency the need to provide quality care may necessitate loud communications. On the other hand, in a non-emergent situation, discussing a patient's condition in front of other patients, visitors, or family members in a hallway is not appropriate. The key is balancing the objectives of safeguarding confidentiality while engaging in communications for effective and high quality health care.

The use of interpreter services over a speaker phone or device is permissible in clinical areas as long a reasonable effort is made to protect the privacy of the patient. HHS states that discussion of “a patient’s condition or treatment regimen in the patient’s semi-private room” may occur, if proper safeguards are in place, such as, in this case, lowering the
volume of the speaker phone. Other safeguards may include use of a sound masking technology, such as white noise.

Again, from HHS: *The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers’ primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.*
Let’s take a closer look at overhead paging. Remember that an incidental disclosure is a disclosure that cannot be reasonably prevent and is limited in nature.

In the context of overhead paging, it should not be used as a matter of convenience for workforce members and should only be used after reasonable efforts have been made to locate the patient.

Furthermore, patients should be directed to a location that does not specify type of treatment, services, or the condition of the patient.
Paper Notes

Paper reports or notes that contain PHI need to be protected.

Keep papers in a secure area and face down when not being used.

Paper Medical Records require that they be maintained and secured from inappropriate access.

Paper notes or paper reports that contain PHI also require safeguards and need to be protected.

Always keep papers in a secure area, not accessible from the general public. Keep papers face down when not being used.

Be sure to return paper medical records promptly to HIM to ensure that they are properly maintained and secured.

Reports containing PHI need to disposed of properly, by shredding or placing in a locked shred box.
Printing PHI

The only workforce members authorized to print the medical record (or parts) is HIM and the Nursing Manager/Supervisor for patient transfers. This includes printing screen captures.

If you have any questions concerning printing PHI, please see the Privacy or Security Official at your hospital or contact the Corporate Privacy and Information Security Officer at corporate.

For authorized workforce members, when printing reports containing PHI, be sure that you only print the minimum necessary PHI that is needed and that you distribute only to those who have a need to know.
Electronic PHI (ePHI)

ePHI can be found in reports (Excel, Word, PDF), applications, and devices.

Electronic PHI, also called ePHI, can be found in reports, such as Excel, Word, or PDF files, but also in applications and devices.

When you hear of topics like encryption and secure storage, it is because the HIPAA Security rule requires our organization to implement safeguards to protect data.

Let’s look at an example of why these safeguards are so important:

In August of 2016, HHS announced a settlement over $5.5 million for allegations that Advocate Health Care violated federal patient privacy law. The breaches involved information of 4 million people and included medical information, names, credit card numbers, and birthdates. It also involved the theft of four unencrypted laptops.

Protecting ePHI in ANY form is the responsibility of ALL workforce members.

Never store ePHI on an unencrypted device workstation, laptop, or drive (such as a thumb drive or usb stick). Use of cameras or voice recorders require that the data be immediately removed and that the device be stored securely.

Use of technology to store ePHI not owned by SHC is prohibited unless approved in writing by Corporate IS Security, Legal, and Compliance.
Examples of websites could include:
- Websites to track exercise and nutrition
- Websites to store photos
- Websites that store backups
- Websites used for operational or clinical workflows
- Websites used to maintain templates
- Websites used to take notes

Here is the takeaway: If you or someone else is entering PHI into a website, make sure that it is an SHC authorized website. Contact your Security or Privacy Official if you are not sure.
Any software application that collects, transmits, stores, or processes ePHI requires written approval by Corporate IS Security, Legal, and Compliance PRIOR to downloading it, purchasing it, or using it. You can submit a request for review and approval through ServiceNow.

This could be software used in an operational, clinical, or research setting.

There are specific requirements for software that contains PHI. We are required to implement safeguards to protect the data.

Such software is required to meet the HIPAA Security Standards requirements, SHC Security Standards, and we are also required to add it to our documentation.

HIPAA Security Standards require, for example, data to be protected by user name and passwords, access to data be logged, and access to data be restricted.

SHC Security Standards, for example, mandate specific types of encryption and where you can store data.

Additionally, we are required to document all software used in collecting, transmitting, storing, and processing ePHI and how we are protecting the data.
Electronic devices are another form of hardware that runs software.

A current trend in devices and gadgets is their ability to connect to the Internet. This trend is called the Internet of Things – where everyday objects have network connectivity allowing them to send and receive data.

Here are a few examples:
- Thermostats
- Door locks
- Security cameras
- Alarm clocks
- Vending machines
- Appliances

It is important to remember that SHC is required to provide the same levels of protection to these devices as workstations.

If a device is NOT protected adequately, it can become an unauthorized entry point to our network, potentially exposing SHC data to unauthorized users.

Use of cellphones for taking patient photos is prohibited. Patient photos must be taken on SHC owned cameras that do not have wireless network connectivity.
Electronic Reports

Like paper files that contain PHI, electronic files containing PHI need to be securely stored.

Electronic reports must be stored in folders that allow access only to those who have a need to know!

Do not store PHI on a desktop. Reports that contain PHI must be stored in secured folders on SHC servers that only allow access to those who need to have access to the information.

Reports containing PHI should never be stored in public folders.

For example:

Each day you receive a census report and need to store it in a folder so that clinical supervisors and managers can access it, you should not store it a department share where all staff have access to it. It should be stored in a folder that is restricted to only those who have the need to know.
Emailing PHI

Per our policies (Security TECH.005), PHI should only be sent via encrypted email.

PHI should NEVER be placed in the subject line or in calendar invites as it cannot be protected.
6 Points on Security

- Your password and/or PIN is confidential. Do not share it with anyone.
- Make sure that your workstation is set to lock automatically after several minutes of inactivity.
- Logout or lock your computer when you leave it.
- If you don’t expect an email and it presents an offer too good to be true, be cautious, as it may be a phishing attempt.
- Do not use non-SHC owned computers or devices to capture PHI (take pictures, videos, sound, notes).
- Do not text or use instant messaging apps to transmit PHI.
5 Points on Privacy

• Wear your SHC ID badge at all times.
• Do not access health information unless it is necessary to perform your job duties, including that of your friend’s children, family members, and colleague’s children.
• Access only PHI that you “need to know” to perform your job.
• Remove patient information from copy machines, fax machines, printers, or conference rooms and store in a secure area.
• Clinical schedules, surgery schedules, and procedure schedules most likely contain PHI and should not be left out in the view of others. When no longer needed, place in shredding bins, not regular trash cans.
End of Training

If you have any questions, please contact your Privacy or Security Official.

You can also contact the Corporate Privacy and Information Security Officer at amrodriguez@shrinenet.org or call at 813-518-7633.