This self-directed learning module contains information all CHS employees are expected to know in order to protect our patients’ protected health information.

Target Audience: All Non-Management CHS Employees, Students, Volunteers, and Physicians
What is HIPAA?

HIPAA (the Health Insurance Portability and Accountability Act) is a civil rights law passed in 1996 that gives patients important rights with regard to their protected health information.

**THE PRIVACY RULE** provides federal protections for protected health information held by covered entities (CHS) and gives patients an array of rights with respect to that information. At the same time, the privacy rule is **balanced** so that it permits the disclosure of protected health information needed for patient care (treatment) and other purposes such as payment and healthcare operations.

**THE SECURITY RULE** specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of **electronic** protected health information.

For more information, visit [http://www.hhs.gov/ocr/privacy/hipaa/understanding.aspx](http://www.hhs.gov/ocr/privacy/hipaa/understanding.aspx)

**ALL CHS workforce members (employees, students, volunteers, physicians, etc.) are required to ensure the privacy and security of our patients’ protected health information!**
What is Protected Health Information?

PHI (commonly referred to as “patient information”) can be contained in electronic, written, and oral communications. It includes any information that is created or received while a health care worker is providing treatment, processing payment, or performing other healthcare operations.

PHI relates to the past, present or future physical or mental health or condition of a patient.
A patient’s identity can be discovered without knowing his/her name. HIPAA protects information that alone or combined may identify a patient, the patient’s relatives, employer or household members. Health information that includes even ONE patient identifier is PHI and is protected under HIPAA.

**EXAMPLES OF PATIENT IDENTIFIERS**

- Name
- Address
- Birth date
- Telephone numbers
- Fax Numbers
- E-mail addresses
- Social Security Number
- Medical Record Number
- Health plan beneficiary number
- Account number
- Voice recordings
- Photographic images
- Other characteristics which may identify the person

*HIPAA Reference: 45 C.F.R. § 164.514(b)(2)(i)

**Policy Reference: PR.PHI 145.02**
Where Can You Find PHI?

Hint: It’s not just in the paper or electronic medical records.

Here are some examples of other places you might find patient information:

- Patient status boards
- Financial records
- Fax sheets
- Data used for research purposes
- Patient’s identification bracelet
- Prescription bottle labels
- Detailed appointment reminder left on voicemail
- Photograph or video recording of a patient
<table>
<thead>
<tr>
<th><strong>Appropriate Access to PHI</strong></th>
<th>Three HIPAA Recognized Purposes*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Treatment</strong></td>
<td>The provision, coordination, or management of healthcare and related services among healthcare providers or by a healthcare provider with a third party, consultation between healthcare providers regarding a patient, or the referral of a patient from one healthcare provider to another.</td>
</tr>
<tr>
<td><strong>Payment</strong></td>
<td>Various activities of healthcare providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, fulfill coverage responsibilities, and provide benefits under the plan and to obtain or provide reimbursement for the provision of healthcare.</td>
</tr>
<tr>
<td><strong>Healthcare Operations</strong></td>
<td>Certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.</td>
</tr>
</tbody>
</table>

*HIPAA Reference: 45 C.F.R. § 164. 506*
Do You Have a TPO Need to Know?

You should not access PHI unless it is your job to do so. Here are some examples of TPO work-related reasons to access PHI:

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Payment</th>
<th>Healthcare Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending PHI from one department to another within the same facility so that a procedure can be performed</td>
<td>Determining eligibility or coverage under a plan</td>
<td>Conducting quality assessment and improvement activities</td>
</tr>
<tr>
<td>Providers/Physicians sharing information between themselves regarding a patient they both treat</td>
<td>Billing and collection activities</td>
<td>Reviewing the competence or qualifications of healthcare professionals</td>
</tr>
<tr>
<td>Referring a patient to a specialist</td>
<td>Reviewing healthcare services for medical necessity, coverage, justification of charges, etc.</td>
<td>Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs</td>
</tr>
</tbody>
</table>

ASK YOURSELF: Do I need to know this information to do my job?
Inappropriate Uses of PHI: Common Non-compliant Practices

- Viewing medical information belonging to yourself, your family, friends, co-workers, and patients when you are not a member of the health team treating the patient.
- Accidentally handing a patient another patient’s prescription or discharge instructions.
- Informing a friend of a patient’s presence at the hospital.
- Emailing patient information to the wrong address or faxing patient information to the wrong number.
- Sharing or allowing easy access to your passwords.
Discussion of PHI in a public location where others are likely to overhear, such as an elevator or the cafeteria.

More Inappropriate Uses of PHI

- Sign-in sheets that reveal a patient’s diagnosis
- Unattended work stations with PHI
- Improper disposal of PHI

NOTE: PHI in any form should not be left unattended.
COMMUNICATIONS WHEN FAMILY MEMBERS, FRIENDS OR OTHERS ARE PRESENT

**General.** If the patient is present and has the capacity to make health care decisions, providers may generally discuss the patient’s health information with family, friends and others involved in the patient's care if the patient agrees or when given the opportunity, does not object. A provider may also share information if in their professional judgment they decide the patient does not object. See 45 CFR 164.510(b).

**Best Practice.**

We should not assume a patient consents to having visitor/family members present during patient-provider communications. Patients should be given an opportunity to object. Suggested steps to ensure that we protect our patients’ privacy rights include:

1. Ask the visitor(s) to step outside the room or away from the area where the conversation will take place;
2. Ask the patient if he/she wants the visitor(s) or friend(s) to be present during the discussion. Be sure to give a review of the topics to be discussed. If “highly confidential information” such as HIV, mental health, genetic testing, etc. will be discussed, then be sure to notify the patient of the specific topic in private;
3. After the patient has given permission, you may invite the family member(s)/friend(s) back into the room/area; and document in the patient’s medical record that the patient gave permission for others to be present.

**Question**

If a patient has a family member or friend with them while in the exam room, triage area, or other treatment area, can we assume that the patient wants that person there during discussions of their test results or other health information?
Proper Disposal of PHI: What’s In Your Trash?

Dispose of any physical material that contains PHI using the appropriate method: CONFIDENTIAL BIN, SHREDDER, OR REGULATED MEDICAL WASTE RECEPTACLE. Reference Policy PR.PHI 145.15

PAPER
All paper containing patient information must be deposited in a locked confidential shred bin.

LABELS
Removable labels containing patient information should be removed from the container and rendered unreadable before discarding in the regular trash. If the label cannot be removed or destroyed, discard the label or empty container in the regulated medical waste receptacle.

ELECTRONIC PATIENT INFORMATION
Items containing electronic patient information should be disposed of in accordance with IS Policy Reference Policy IS.PHI 600.06

ID BRACELETS
ID Bracelets removed by a workforce member should be disposed of in a locked confidential shred bin

FOR MORE INFORMATION, SEE “DISPOSAL PROCEDURES FOR PATIENT INFORMATION”, CHS POLICY PR.PHI 145.15
Appropriate Uses of PHI: Incidental Disclosures

The following practices are permissible under the Privacy Rule if reasonable precautions are taken to minimize the incidental disclosures to others who may be nearby. In these cases, reasonable precautions would include lowered voices or talking apart from others.

- Healthcare staff may communicate and coordinate services at hospital nursing stations.
- Healthcare professionals may discuss lab test results in a joint treatment area.
- A physician may discuss a patient’s condition QUIETLY in a semi-private room or a waiting room.
- Healthcare professionals may discuss a patient’s condition during training rounds in an academic or training institution.
- A pharmacist may discuss a prescription with a patient over the pharmacy counter or with a physician or patient over the phone.

*HIPAA Reference: 45 CFR § 164.502(a)(1)(iii)
Access to PHI Requiring Patient’s Authorization

Uses and disclosures of PHI that fall outside of TPO purposes typically require the patient’s written AUTHORIZATION. CHS has a standard process and form for authorization.

HIPAA allows for limited exceptions to the TPO and Authorization rules. These exceptions are outlined in the Release/Review of Medical Information Policy (PR.PHI 140.05)

Examples include:
  • Medical Emergencies
  • Threat to the Health or Safety of the Patient
    • Certain Law Enforcement Activities
    • Court Order
Education - HIPAA: Patient Rights

HIPAA grants patient rights with regard to Protected Health Information (PHI):

1. **Inspect and Copy**
   - Barring some specific restrictions (e.g. psychotherapy notes), patients have a right to inspect and obtain a copy of their medical record information.

2. **Amendment**
   - Your obligation is to review the request; no mandate to agree & make change.
   - Make the change only if the record is inaccurate or incomplete.
   - The best documentation is that made at or near the time of the event.

3. **Accounting of Disclosures**
   - Right to know who has seen patient’s information without their authorization.
   - Currently applicable only to uses and disclosures outside of Treatment, Payment, or Healthcare Operations (TPO).

4. **Restrictions**
   - Right to request restriction or limitation on information we use or disclose for TPO.
   - Right to request a limit on information we disclose to a family member or friend.

5. **Confidential Communications**
   - Right to request communication about medical matters in a specific format or location.
   - Request may be denied due to logistical obstacles to implementing them.

---

HIPAA Policies: See Administrative Policy Manual on Synapse.
EVERY patient has the right to receive a copy of the CHS Notice of Privacy Practices, which describes how his or her health information may be obtained, used and disclosed. The Notice also explains to the patient how he/she can get access to that information.

A copy of CHS’ current Notice of Privacy Practices is available on the CHS internet website, each facility’s website, and at every point of patient entry at each of the CHS facilities.

For more information, refer to Policy PR.PHI 145.06 – Receipt & Acknowledgement of Notice of Privacy Practices.
The term “Red Flag” has been adopted by the FTC to mean a pattern, practice, or specific activity that indicates the possible existence of IDENTITY THEFT.

### CLINICAL SETTING
- Patient’s medical condition doesn’t match the medical record.
- Records are inconsistent with the physical state of the patient or his/her medical history.
- Records show substantial discrepancies in age, race, sex, or other physical descriptions.

### NON-CLINICAL SETTING
- Inconsistent information on employment records, medical records, or registration information
- Documents that appear to be forged or altered (including driver’s license, etc.)
- Missing laptops, security codes, equipment with patient or employee information, etc.
- Alerts from consumer reporting or fraud detection agencies

Employees are required to report red flags. If you suspect identity theft or any patient misidentification, talk to your manager, follow your department’s procedure for handling red flags, and contact the Customer Care Line at 704.355.8363

Policy Reference: ADM.PHI 200.16
You should not take patient information, in any form, offsite without proper permission and unless your job specifically requires you to do so. If you must take patient information offsite, be sure to safeguard with these important security measures.

- When using a laptop or PDA offsite that contains patient information, store patient information on the device ONLY if the device is encrypted. To make sure your device is properly encrypted, contact Information Services.

- Papers containing patient information are even more vulnerable than electronic devices storing PHI. Anyone who comes in contact with those papers can see the information. If you have to take paperwork out of your work setting, please take steps to protect it. Do not leave your bag or briefcase unattended. If papers containing PHI are lost or stolen, you should immediately report it to your supervisor.
Using CHS Resources

Individual passwords should NOT be printed, stored online, stored on any electronic device, or given to others.

**REMEMBER:** Anything accessed on a computer using your network information will be traced back to you.

Use caution when sending patient information via email:
- Send only the minimum information needed.
- If sending to an email address that does not end in @carolinas.org or @carolinashealthcare.org, you need to “Send Certified” so that the email will be encrypted.

Acceptable Use Policy: IS.PHI 600.01
In an age where social networking websites, such as Facebook, MySpace, and Twitter, are a popular way to communicate, it is important to remember that the internet is a public domain.

You have an obligation to safeguard PHI regardless of the setting.

Do not post identifying information about patients or their images, etc. A photograph taken in the hospital or office environment may inadvertently have a patient in the background.
Social Networking

Social Media is:
- A great new tool
- Public domain
- Permanent and can have a broadcasting effect

Questions to ask yourself:
- Will my posted comments have a harmful or perceived harmful effect on another human being or organization?
- Is the media I am using public or private
- Who does the information I am about to share belong to?
- Do I have permission to share the information in the media in which I am about to share it?
- Is there a more appropriate media for the communication I wish to make?
- Could this post get me “in trouble” at work? (Is that the desired outcome?)

Guidelines when accessing social networking sites:
- Do not engage in purely personal matters during business hours.
- When identifying yourself as a member of CHS, state that comments are those of your own, not CHS.
- Only use your CHS email address when acting in your official role at CHS.
- All data submitted on the Internet is outside of your control once posted.
- Communicating patient information is strictly prohibited and subject to sanctions.
- See Pages 10 and 11 of the AUP for more details regarding this subject.

Resources:
1) Link to policy:
2) IS Security Bulletin – August:
CHS HIPAA Sanctions

Workforce members using PHI inappropriately will be subject to disciplinary action which may include

WRITTEN COUNSELING
FINAL WRITTEN COUNSELING
TERMINATION

Disciplinary action will be determined based on the severity of the violation.

Refer to Policy PR.PHI 145.13
Reporting Potential Privacy Issues

To report a potential privacy issue or if you have a question or concern about privacy, you should follow the Chain of Command.

I have a privacy question, concern, or potential issue.

Contact your SUPERVISOR

I am uncomfortable talking to my supervisor.

Contact your SUPERVISOR’S SUPERVISOR

I am uncomfortable talking to my supervisor’s supervisor.

Contact your FACILITY PRIVACY DIRECTOR

Contact CHS CORPORATE PRIVACY DEPARTMENT 704.512.5900

Contact the CUSTOMER CARE LINE 704.355.8363
Reporting Potential HIPAA Issues

Questions About HIPAA:
1. Contact your Supervisor.
2. Contact your Facility Privacy Director (FPD)
3. Privacy Questions: 704.512.5900
   Corporate Privacy
4. Security Questions – 704.446.6383
   Robert Pierce, AVP of Information Security
5. HIPAA Privacy and Security SharePoint Site:
   http://sharepoint.carolinas.org/hipaaprivacy

HIPAA POLICIES
HIPAA Policies can be found on the CHS Intranet.
http://synapse.carolinas.org/reference/hipaa/

Who is My FPD?
Each CHS facility has a Facility Privacy Director (FPD) who
serves as the privacy representative for that facility. A
list of FPDs is available on the CHS Intranet.

http://synapse.carolinas.org/documents/ListofFacilityPrivacyDirectors.pdf?#search='FPD'
TEST YOUR HIPAA KNOWLEDGE
The HIPAA privacy and security provisions cover communications which may contain PHI. Which form(s) of communication is/are covered by HIPAA?

a) Oral communications
b) Written communications
c) Electronic communications
d) All of the above
One of your friends recently had a biopsy at the CHS facility where you work. You are worried about her and want to find out the results of the biopsy. What should you do?

a) Use your logon information to access your friend’s medical record even though you have no TPO work-related need to know.

b) Ask a friend who works in the department to access the results for you.

c) Wait for your friend to tell you the results if she chooses to do so.
Question #3

True or False?
Paper containing patient information may be disposed of either in a confidential locked shred bin or you may take it home and throw it in your garbage can.

a) True

b) False
A physician refers a patient to a specialist for consultation. The specialist’s office requests the patient’s medical records and insurance information. The referring physician’s office refuses to disclose this information for fear of violating HIPAA. What is wrong with the referring physician’s understanding of HIPAA?

a) HIPAA does not cover oral communication.

b) The specialist’s office should not receive this information without signed authorization by the patient.

c) The request by the specialist’s office is for treatment purposes, so the referring physician’s office is permitted to release the information without a signed authorization form.

d) Nothing. The referring physician’s office is correct in refusing to disclose the information.
What should you do if you are about to tell a patient his/her test results but his/her family and friends are in the room?

a) Just tell the patient the results with the others in the room because you are in a hurry.
b) Ask the others to leave the room so you can talk with the patient in private.
c) Invite the others back in the room to hear the results if the patient requests they return and knows what is to be discussed
d) All of the above
e) Both b and c
True or False?
Employees who inappropriately use PHI will be subject to disciplinary action up to and including termination.

a) True  
b) False
You are a nurse in a CHS Emergency Department. During one of your shifts, a well-known public figure comes to the Emergency Department for treatment. True or False: It is okay to tell your friends about the public figure’s appearance at the Emergency Department as long as they promise to keep it a secret.

a) True
b) False
Question #8

A new employee at your clinic has not received her logon information. You really need her help scheduling appointments, but without logon information, she cannot access the appointment system. You know that one of your coworkers keeps his password on a post-it note underneath his keyboard. What do you do?

a) Allow the new employee to use your logon information.

b) Tell the new employee where your coworker keeps his information. He won’t mind if she uses it until she has her own.

c) Do not share your password or allow the new employee to use your coworker’s. Notify your supervisor that the new employee needs access to CHS systems to perform his/her job.
Question #9

I attest I have reviewed and am familiar with the CHS Communications Environment Acceptable Use Policy (AUP). I understand that failure to comply with the AUP may lead to disciplinary action, up through termination of employment. The AUP is located on Synapse in the Administrative Policy and Procedure Manual, [IS.PHI 600.01]. Please check the “Yes” box (or sign if taken manually) before submitting the test to receive your score. An affirmative answer is required for the successful completion of the HIPAA Privacy and Security Post Test.

☐ Yes