Carolinas HealthCare System

2009 Annual Continuing Education Modules

CMC-NorthEast

HIPAA Privacy & Security Laws

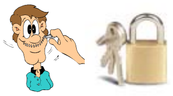
Corporate Privacy, Information Security, and Employee Development

This self-directed learning module contains information you are expected to know to protect our patients, our guests, and yourself.

Target Audience: **CHS Workforce (Employees, Students, Volunteers, and Physicians)**

Contents

"Keep It To Yourself"



What is HIPAA and How Does HIPAA Apply To You?

- HIPAA is a consumer law which gives the patient control over the use of their health information.
- You, as a member of CHS' workforce (All health care employees, students, volunteers, physicians, etc), are required to ensure the privacy and security of our patients' protected health information (PHI) or more commonly referred to as "patient information".
- Electronic, written, and oral communications can contain patient information, and are protected by the Health Insurance Portability & Accountability Act (HIPAA).
- The HIPAA law allows us as workforce members to use patient information for treatment, payment or healthcare operations as defined by HIPAA and required by your job responsibilities.
- We must get a patient's approval before releasing information for all uses with few exceptions outside of treatment, payment, or healthcare operations.
- Workforce members should use only the minimum amount of patient information necessary to perform their jobs.
- **Failure to comply with HIPAA requirements as addressed in CHS policy can lead to disciplinary actions, including possible termination of employment.**
- The CHS Acceptable Use Policy IS.PHI 600.01 and Release/Review of PHI Policy PR.PHI 140.05 along with 25 other CHS policies present specific guidance for protecting all forms of patient information: electronic, written, and oral.

Instructions:

The following module has been written to briefly educate you on the concepts contained in the HIPAA Policies and thus assist you in being compliant. Please:

- Read this module.
- Ask your supervisor if you have any questions about the material.
- Complete the online posttest for this module. (Once you pass the posttest, print it or a copy of your transcript and give it to your supervisor.)
- Record the date you completed the module on your **Employee Annual Continuing Education Record.**
- Contact your supervisor after completing this module to obtain information about department specific policies and procedures.

Learning Objectives:

When you finish this module, you will be able to:

- Understand your role/responsibilities for HIPAA Privacy and Security compliance.
- List ways to protect a patient's privacy/confidentiality/electronic, written, or spoken patient information.
- Locate the CHS HIPAA Privacy and Security Policies and Procedures.
- Know how to report a potential privacy misuse or disclosure.
- Know how to handle inquiries by governmental or regulatory offices.
- Know how to apply the "minimum necessary" rule.
- Know patient rights provided under HIPAA.

HIPAA Contacts

CORPORATE PRIVACY

CHS Chief Privacy Officer	Gene DeLaddy
CHS Assistant Vice President for Privacy	Todd Harrington
CHS Manager, Privacy	Carrie Raines
CHS Manager, Privacy – Technology	Jennifer McGill
CHS Privacy Analyst	Karen Peters
CHS Security Analyst	Jason Shanks

FACILITY DIRECTORS(PRIVACY & SECURITY

	Privacy	Security
CMC & Corporate	Todd Harrington	Robert Pierce
CMC – Lincoln	Lesley Chambless	Morris Cornwell
CMC – Mercy	Collin Lane	Robert Pierce
CMC – Pineville	Jane Firth	Robert Pierce
CMC – Northeast	Katie Thibodeau-Dever	Susan Wilfong
CMC – Randolph	Mary Klock	Robert Pierce
CMC – Union	Royal Link	Lisa Sykes
CMC – University	Tony Kouskolekas	Robert Pierce
Ambulatory Services	Kristin Wade	Robert Pierce
Cannon Research & Medical Education	Joan Connell	Robert Pierce
Carolinas Homecare	Andrea McCall	Jeff Meier
Carolinas Physicians Network	Sara Cole	Robert Pierce
Carolinas Rehabilitation	Janice McNeely	Robert Pierce
CMC Home Infusion	Cathy Maya-Mathews	Jeff Meier
College of Health Sciences	Patricia Campbell	Robert Pierce
Public Health	Connie Mims	Jeff Meier
Anson Community Hospital	Carol Williams	Dale Spencer
Blue Ridge HealthCare System	Tom Eure	Leonard Deal
Cleveland Regional & Kings Mountain	Gail McKillop	Theresa Bridges
Huntersville Oaks	Tereasa Owens	Robert Pierce
Medic	Cristy Althiser	Teresa Womble
Roper St. Francis Healthcare	Stacey Dodd	Mike Taylor
Sardis Oaks	Ty Lewis	Robert Pierce
Wilkes Regional Medical Center	TBD	Steve Kelly
Wallace Thompson Hospital	Susan Foster	Susan Foster
St. Luke's Hospital	Amy Arledge	TBD
Levine's Children's Hospital	Susan Goode	Robert Pierce

How Does HIPAA Apply To You?
- When Releasing Patient Information…

Using Patient Information

Workforce members are allowed to use patient information for treatment, payment, or healthcare operations (TPO) as defined in the HIPAA Law. For any other purpose, CHS must obtain a HIPAA valid authorization signed by the patient or the patient's legal representative (whose relationship is stated), when releasing (using or disclosing) patient information unless a specific exception applies.

Using Patient Information With A Valid Authorization

Carolinas HealthCare System - Authorization for Release of Health Information Form

[illegible]

A **valid authorization** must contain specified elements.

- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
- The CHS approved authorization is recommended. However, if all law required elements are included, a non-CHS authorization can be accepted.
- Only a competent adult (18 years of age or older) or minor emancipated by marriage or court, may sign an authorization to release his / her medical information with the following exceptions:
  - A minor alone can authorize the release of medical information in the case of:
    - Venereal disease and other reportable diseases
    - Pregnancy
    - Abuse of controlled substances or alcohol, and
    - Emotional disturbances

Deceased patients have similar privacy rights to live patients. If the patient is deceased, an estate representative/executor should present letters of administration from a court of law in order to act on behalf of the deceased.

Under the Privacy Law, **psychotherapy notes** have stronger protections. In order to use or disclose psychotherapy notes (even for TPO purposes), the law requires specific individual authorization unless the notes are used inside the treatment program by which they were created.

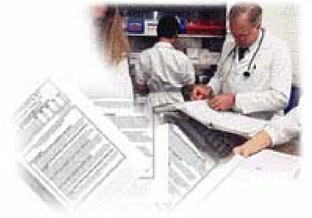
For **non-criminal cases**, CHS facilities may release patient information upon receipt of a valid patient authorization or a court order from a North Carolina Court or a Federal Court. The CHS Legal Department should be consulted for **criminal situations**.

Photographic or other non-typical media:

- All photographic or other non-typical media containing a patient likeness or has affixed, in any manner, patient identifiers are subject to the Authorization requirement.
- Based on the purpose of the photography or capture of patient identifiers or patient likeness in other non-typical media, certain CHS departments are to be contacted for coordination/authorization (e.g., Education, Public Information).

Note: See Policy (PR.PHI 140.05) for scenarios that require authorization to release medical information and scenarios that do not require patient authorization to release patient information.

Using Patient Information With A Valid Authorization: Record Keeping



- Each CHS treatment facility is responsible for documenting the patient information released and the date of release.
- Copies of written requests shall be documented and maintained in original or electronic format in the permanent medical record for six years from the date of creation.

Using Patient Information With A Valid Authorization: Releasing Medical Information

Methods of Releasing Medical Records and Other Patient Information:

- Copies of patient medical records may be released to authorized requestors with patient or legal representative authorization, including via mail.
- Disclosure of health record information via fax will be limited to urgent or non-routine transmittals for continued patient care. In general, sensitive or highly personal health information will not be faxed.
- In rare cases, when a record will not reach a requestor in time for a follow-up appointment, overnight delivery will be utilized.

Reference Policy PR.PHI 140.05 Release/Review of PHI

Providing Information With An Authorization: Limit Interviews, Photographs and Media Releases

News media may <u>not</u> interview or photograph patients, visitors, or employees on CHS premises unless they have received permission from:

- The CHS Public Information Department or Administration
- The patient and Nurse Manager or Charge Nurse
- The employee
- Law enforcement officials, if the patient is in their custody

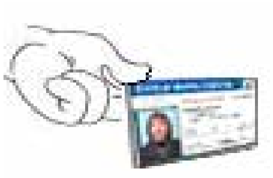
Note: CHS Authorization must be signed by the patient since a patient likeness is considered patient information

Reference Policy ADM 230.01 – Photographs & Interviews of Patient, Visitors, & Employees

Special Note: Always forward any inquiries from the media to the Public Information Department (or the House Supervisor when Public Information is unavailable) <u>without</u> providing any information.

Reference Policy ADM.PHI 230.04 Release of Patient Information to the News Media

Providing Patient Information Without An Authorization: Verify the Identity of a Person Requesting Patient Information



All workforce members are responsible to reasonably verify the <u>identity</u> and <u>authority</u> of an individual requesting patient information before providing the patient information.

- Verification of Identity can be accomplished by:
  - Exchanging unique pieces of information that only the patient or family members would know.
  - Setting passwords up for use with the care team.
  - Asking for the caller's phone number and verifying it using previously collected or publicly accessible information (such as registration information or phone book) before calling back.
- Verification of Authority: "Does this person have the authority to access the requested patient information in their role as a CHS workforce member?"

Special Note: NEVER GIVE INFORMATION ON A PATIENT WHO IS UNDER AN ALIAS.

Reference Policy PR.PHI 145.07 Verifying the Identity of Person Requiesting PHI

Providing Patient Information Without An Authorization: Government Officials and Regulatory Agencies

Any workforce member who is contacted by a government agency (for example, the U.S. Department of Health and Human Services (DHHS) or the Office for Civil Rights (OCR)), should not provide information. Instead, write down the agent's name, the name of the agency for which he/she works, the subject that he/she wants to discuss and any other pertinent information. The employee should then contact his/her immediate supervisor who will immediately contact the AVP for Corporate Privacy or his designee.

Reference Policy - PR.PHI 145.14 Duties of the Chief Privacy Officer (CPO) and Corporate Privacy Depart. Staff and COR 40.11

Providing Patient Information Without An Authorization: As Required by Law

Authorization is not required when releasing patient information as required by law. Such releases are disclosures and must be documented in the medical record or logged in the Reporting Misuses and Disclosures database on Synapse, i.e., CHS' Accounting for Disclosures database.

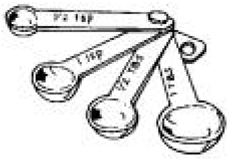
- For example, CHS is permitted to disclose certain elements of patient information in response to a request from a **law enforcement** official in certain circumstances.
- Other examples of exceptions to the authorization requirement may be found in the Release / Review of Medical Information Policy (PR.PHI 140.05) located in the Administrative Policy and Procedure Manual and in the Frequently Asked Questions (FAQs) located on Synapse.

Providing Patient Information Without An Authorization : Motor Vehicle Accident

For patients involved in a motor vehicle accident and upon the request of an investigating law enforcement officer, the CHS employee or medical provider treating the patient (preferably primary members of the treatment team) should provide the following information about the patient:

1. Patient name
2. Patient's current location
3. Whether the patient appears to be impaired by alcohol, drugs, or other substances.

Providing Patient Information Without An Authorization: Use the "Minimum Necessary"



All workforce members must limit the amount of patient information to the minimum necessary to accomplish the "intended" work purpose. Ask yourself the following question before looking at medical records, test results, or any other patient information.

"Do I need to know this information to do my job?"

Requestors should only receive the requested information.

- Do not provide the entire chart/file, if the requestor asks for one particular date of service, unless there are valid reasons for the requestor to receive all dates of service.

Reference Policy PR.PHI 145.05 Minimum Necessary Requirement

Providing Patient Information Without An Authorization: De-identify Patient Information

The Privacy Law requires that patient information only be shared for treatment, payment, and healthcare operations (TPO), or as permitted by law, or as authorized by the patient. Patient information that does not fall into one of these HIPAA defined categories must be de-identified prior to sharing the data in: database reports, data downloads, across interfaces, etc. Methods used for de-identifying data at CHS include: *Safe Harbor*, requiring all PHI elements be removed, and; *Limited Data Set*, allowing some elements of PHI to be shared for research and Public Health purposes provided a Data Sharing Agreement is signed.

Examples of patient identifiers are:

- Name
- Address (including street address, city, county, and last two digits of the zip code)
- Names of relatives and employers
- Birth date
- Telephone numbers
- Fax number
- E-mail address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Serial number of any vehicle or other device
- Electronic mail addresses
- Web Universal Resource Locators-URLs

- Fingerprints
- Voice recordings
- Photographic images
- Any other characteristics which may identify the person

Reference Policy PR.PHI 145.02 De-identification – Removal of Patient Identifiers

Using Patient Information Without An Authorization: Patient Directory Information (General Public and Clergy)

Visitors to a CHS facility may receive information about a patient's location and one word condition description, after first asking for a patient by a combination of at least two of the patient's registered names.

Clergy from the community are required to obtain identification badges, available through the Pastoral Care Department at CMC, in order to have access to their specific list of patients by church or denomination.

A member of ***CHS Pastoral Care*** may have access to patient information in a treatment role (i.e., in the areas to which they are assigned or by physician order).

CHS is not allowed to reveal the presence or absence of patients:

- Requesting to opt out of the facility directory ("Z" code)
- Receiving substance abuse treatment
- Receiving behavioral health services

A sample response when asked about such a patient would be: "We do not have anyone listed in our directory by that name".

Reference Policy PR.PHI 145.01 Disclosure of Patient Directory Information (General Public and Clergy)

Using Patient Information Without An Authorization: Non Employee Workforce Member

Shadowing:

- A shadow placement is an opportunity to "shadow" a healthcare professional.
- Individuals requesting shadow opportunities should follow the non-clinical/volunteer applicant procedures below:

Non-Clinical/Volunteer Applicants:

- Applicants would apply through the Volunteer department and attend appropriate HIPAA training (video and ACE module), complete an application packet, references/criminal background check, interviews, sign a confidentiality agreement/Code of Ethics/Acknowledgement.
- The physician/healthcare professional must obtain the patient's

approval, before allowing the “shadower” into the room.

- The physician must document each patient’s approval.

Students & Faculty that are in a program for academic credit:

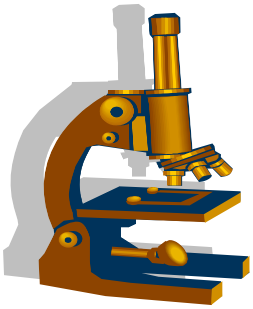
- CHS would have in place an Educational and Affiliated Agreement with the specific school and then follow appropriate procedures (please see ADM 200.13 – Student / Faculty Internships & Field/ Clinical Experiences).

Business Associate Agreements

Patient information may be disclosed to a Business Associate/Vendor (individual or entity) if the patient information is required for the Business Associate to perform services on behalf of CHS and the vendor has signed a Business Associate Agreement as part of their contract with CHS.

ADM.PHI 280.03 Use & Disclosure of PHI for Business Associates

CHS Research Activities



Following approval by CHS’s Institutional Review Board (IRB), which serves as the organization’s Privacy Board, or the IRB’s designee, all requests for patient information for research purposes must:

a. Be documented on the appropriate Research-specific authorization form(s) and signed by the research subject or his/her legal representative and the IRB Chairman or designee.

b. Have the need for patient authorization waived by the CHS IRB.

Reference Policy ADM 240.05 – Authorization for Release/Review of Medical Info for Purposes of Research

Dispose of Patient Information

Dispose of any physical material that contains patient information using the appropriate method: confidential bin, shredder or regulated medical waste receptacle.

Contact Information Services (IS) for disposing of electronic PHI contained in equipment such as laptops, PDAs, CD-ROMS, diskettes, magnetic tapes, etc.

Check with your manager for the proper disposal procedures when deleting, disposing of, erasing, or destroying email messages or other electronic records.

Reference Policy PR.PHI 145.15 Disposal Procedures for Patient Information

Report Violations Using the Following Chain of Command

An workforce member who wants to report any potential Privacy violation should use the following chain of command.

I would like to report a potential Privacy violation

↓

Talk with your supervisor

↓

If the issue concerns your supervisor, or if you are uncomfortable discussing it with your supervisor

↓

Talk with your supervisor's supervisor

↓

If you are uncomfortable discussing it with your supervisor's supervisor, contact:

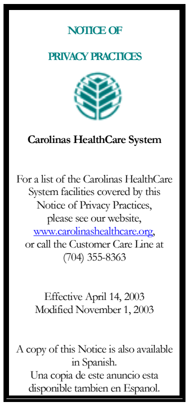
↓ ↓

Corporate Privacy 704-512-5900 or Customer Care Line 704-355-8363

How does HIPAA Apply to You?

– When Respecting Patients' Rights…*A Patient has the right to:*

Receive CHS' Notice of Privacy Practices



NOTICE OF

PRIVACY PRACTICES

Carolinas HealthCare System

For a list of the Carolinas HealthCare System facilities covered by this Notice of Privacy Practices, please see our website, www.carolinashealthcare.org, or call the Customer Care Line at (704) 355-8363

Effective April 14, 2003
Modified November 1, 2003

A copy of this Notice is also available in Spanish.
Una copia de este anuncio esta disponible tambien en Espanol.

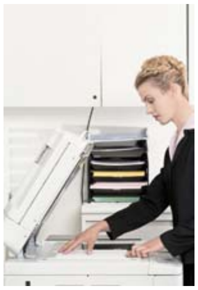
The patient has the right to receive a copy of the CHS's Notice of Privacy Practices which describes how patients' health information may be used and disclosed and how patients can get access to their information.

- An acknowledgement signature must be obtained and on file from each patient indicating they have received a copy of CHS Notice of Privacy Practices. In some settings, acknowledgment signatures will be collected at each registration.
- If a patient refuses to sign or is unable to sign the acknowledgement form, CHS staff must document the reason for not signing on the form.

A copy of CHS's current *Notice of Privacy Practices* is available on the CHS internet website, as well as at every point of entry for each of the CHS facilities. The Notice is available in English and Spanish.

Reference Policy PR.PHI 145.06 Receipt & Acknowledgement of Notice of Privacy Practices

Patient & Relative Access to Health Record Information: Inspect or Obtain a Copy of Medical Record



The patient has the right to access to inspect or obtain a copy of their official medical record. CHS defines a consistent mechanism for all patients to request and obtain access.

Review:

- If a current *inpatient* or his/her authorized representative requests to review the medical record, two conditions must be satisfied:
  - i. Attending physician must be notified (as a courtesy), not give permission
  - ii. An appointment must be set up for a staff member to be present to safeguard against the destruction or alteration of the record.
- CHS does not require an authorization form to be completed by the inpatient in order for the patient to review their medical record; however, documentation of the review and permission for others to review the medical record must be noted in the medical record by CHS staff.

Obtain a Copy:

- All requests for to obtain a copy of medical records by patients after discharge must be referred to the Medical Record Department or CPN Practice Manager provided they present a signed CHS Authorization Form to assure that a valid authorization is obtained.

Reference Policy PR.PHI 140.05 Release/Review of Protected Health Information

Amend or Correct their Health Record Information

Any patient who believes that information in their health record is incomplete or incorrect has the right to request an amendment or correction to the information for as long as the information is kept by or for CHS. Please follow CHS Policy PR.PHI 145.03 regarding the process for accepting or denying a patient's request for amendment.

For example: Patient requests change of address.

Reference Policy PR.PHI 145.03 Request for Amendment or Corrections to Health Record Information

Restrict the Use & Disclosure of their Patient Information

The patient has the right to request a restriction or limitation regarding the use of their health information that a covered entity uses or discloses typically outside of TPO.
For example: A patient desires to opt out of fundraising.

Reference Policies:
PR.PHI 145.09 Use & Disclosure of PHI for Marketing Purposes
PR.PHI 145.10 Use & Disclosure of PHI for Fundraising Purposes
PR.PHI 145.12 Patient's Request for Privacy Protections (Restrictions & Confidential Comm.)

Request Confidential Communications Regarding the Use & Disclosure of Patient Information

The patient has the right to make requests for confidential communications.

For example: A patient can opt out of participation in the Facility Directory, or a patient can request all communications be sent to a special address.

Reference Policy PR.PHI 145.12 Patients' Request for Privacy Protections (Restrictions & Confidential Comm.)

Account for Disclosures of PHI

All non-patient authorized disclosures outside of treatment, payment or healthcare operations (TPO) should be reported to your Supervisor and documented on Synapse in the "Reporting Misuses and Disclosures of PHI" Tracking tool. (Disclosures (not misuses) may be documented in the Medical Record in some circumstances).

Examples:

- Providing PHI for public health purposes or to report diseases is required by law is classified as a non authorized disclosure. Thus, the disclosure should be logged on Synapse or in the Medical Record.
- Inadvertently faxing information to the wrong provider is classified as a "Misuse" and should be logged on Synapse. Misuses must not be documented in the Medical Record.

What to report to your Supervisor:

1) The date of the misuse or disclosure
2) Why the patient information was misused or disclosed
3) The name of the patient(s) whose information was misused or disclosed
4) What patient information was misused or disclosed
5) The name (and address, if known) of who received the patient information appropriately or inappropriately.

Link to Reporting Misuses and Disclosures of PHI Tracking Tool: http://synapse.carolinas.org/reference/HIPAA/

Reference Policy PR.PHI 145.08 Accounting for Disclosures of Patient Information

How Does HIPAA Apply To You?
– As a part of the CHS Privacy and Security Programs…

Use CHS Resources for Acceptable Purposes

Communicating any patient information unless you are involved in the patient's TPO is strictly prohibited by Federal Law. Users of CHS resources are responsible to ensure the safety, security, and confidentiality of all patient information that is downloaded to any communications device, PDA, laptop, etc and to use CHS's Communication Resources responsibly, professionally, ethically, and lawfully. This can include but is not limited to written reports, email, voicemail, faxing, and verbal communication, etc.

Privacy

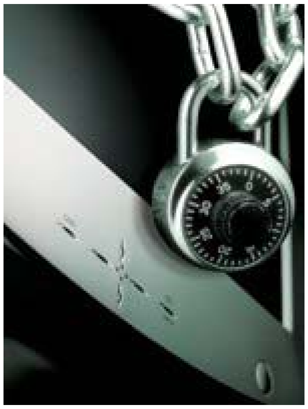
- Any media containing patient information should be maintained in the work environment under confidential and secure conditions.
- Secured Messaging or Secure Mail should be used when emailing patient information for any purpose outside of CHS's firewall. Secured Messaging or Secure Mail can be obtained by completing an OSR.
- When communicating with patients via email, a signed consent form must be obtained from the patient before communication begins. This consent form, along with all e-mail communications between CHS employees and the patient, must be included in the patient's medical chart.
- A CHS Fax cover sheet with Confidentiality Notice statement must be used when a qualified individual faxes any patient information.
- In conversation or discussion (at work or home), information collected for CHS business purposes which includes, but is not limited to the treatment, billing, hospital operations and improvement of patients well-being, shall not be shared inside or outside the business environment with any non-authorized individual(s), group of individuals or organization, etc. As with any communication of patient information, the person communicating the information and the person receiving the information must be authorized to receive and handle the information.
- Schedules, OR Schedules, and any other lists of patients are to be used strictly by CHS staff for TPO.

Security

- Access to communications resources shall be granted as required in each job description.
- A unique, separate login account consisting of an ID and password is required for each User. Users are required to change passwords upon initial login, and as often as required by

CHS.

- New uses of CHS resources must be approved by the CHS IS Security Assistant Vice President or his designee.



Acceptable Use

- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, discriminatory, hostile, suggestive, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail or any other form of electronic communication.
- Users may not deliberately perform acts that waste communication resources.
- Personal use is subject to the same scrutiny as business use and becomes property of CHS.
- CHS software may not be duplicated.
- Unapproved software may not be installed on CHS computing resources.
- **Failure to comply with the Acceptable Use Policy (AUP) may lead to disciplinary actions, including possible termination of employment.**
- Use of resources and any information gained from use of resources ceases when a User's employment or association with CHS terminates.
- Users may not attempt to circumvent CHS's data protection measures or attempt to uncover security loopholes.
- Creations developed using CHS resources become the exclusive property of CHS.

Reference Policy PR.PHI 600.01 Communications Environment Acceptable Use

Sanctions

Failure to comply with the HIPAA Privacy and Security regulations as set forth in CHS policies and procedures will result in disciplinary action. The disciplinary action will be based on the severity and context of the violation in accordance with existing CHS policies and/or appropriate legal actions. Other civil liabilities for employees who violate HIPAA are:

- Department of Health and Human Services (DHHS) may impose fines of **$100/violation up to $25,000/person per year** for negligent violation of a single privacy standard.

- DHHS may make criminal referral to the Department of Justice for "wrongful disclosure" with fines **up to $250,000 and 1-10 years imprisonment.**

If you suspect that someone is in violation of the Privacy Standards, notify your supervisor or contact Corporate Privacy. No disciplinary action will be taken against any employee for reporting a perceived problem or violation of the Privacy Rule.

Reference Policy - PR.PHI 145.13 HIPAA Privacy Sanctions

How Does HIPAA Apply To You?

- When Using Electronic Patient Information…

Securing Patient Information

HIPAA Security is a federal law designed to safeguard a patient's electronic health information. How does this relate to the Privacy Rule? Simply, the Security Rule more specifically addresses information stored in electronic format on hard drives, removable media, etc., or while it is being transmitted over the Internet, e-mail, or by other means. Some examples of these devices are:

- Hard drives
- Floppy disks
- CDROM
- PDA (Personal Digital Assistant)
- Dictaphones
- Magnetic Tapes
- USB "Thumb" Drives
- Flash Memory
- Cellular phone with a built-in camera
- Any future technology that has the ability to store or send data

What is Information Security?

Information security refers to all the precautions and safeguards implemented to ensure that information is: kept confidential, has not been altered or destroyed, and is accessible when needed by those that are authorized to access it. It also involves ensuring that the above examples are disposed of in a proper manner, so that patient information cannot be recovered. CHS maintains information security through the following methods:

- Computer hardware & software (i.e. Firewalls, Anti-virus Software, etc.)
- Policies and procedures
- Physical security
- Disaster recovery preparedness
- Oversight of all of these areas above

All employees should be aware of the CHS Communications Environment Acceptable Use Policy, which specifically defines what is considered acceptable use within our computer environment.

Security Awareness

You will receive additional security reminders and updates over time

via e-mail or newsletters to reinforce the concepts in this module. Such updates will contain current information about the latest security policies and procedures.

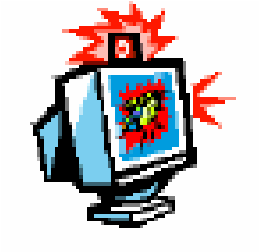
The Assistant Vice President of Information Security should also be notified if information security policies and procedures appear to be violated. If you discover a potential security violation or notice something out of the ordinary that may represent a security risk, you should contact the Assistant Vice President of Information Security, notify your Supervisor, or call the Customer Care Line at 704-355-8363.

Access discipline data on PDAs

Guidelines to ensure the safety of electronic patient information:

Access

- ✓ Choose "*strong*" passwords for all computer accounts. Using a password that is weak can lead to unauthorized access. For instance, never use a pet's name, favorite sports team, or family member's name. A strong password should be a combination of letters and numbers or special characters. (i.e. gr@ysk1e5 – gray skies converted to mixed alpha-numeric)
- ✓ Never write your password on a piece of paper and leave in plain view. If you have difficulty remembering your password and must write it down, place it in a locked drawer that only you have access to.
- ✓ Never share your password with anyone, including other CHS employees or Support Center personnel. Your password should never be required for troubleshooting issues.
- ✓ Ensure laptops and PDAs are properly secured when not in use.
- ✓ Do not disable any security software on your computer without consent. The software on each system is setup in a manner to ensure security. (i.e. Screen savers, Virus Software, etc.)
- ✓ Follow the proper guidelines for disposal of media that contains patient information.



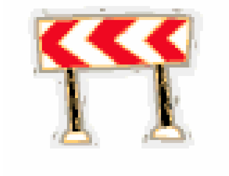
Be aware of the following about viruses and malicious software:

- ✓ Viruses are unwanted software that is installed on your computer without consent in the process of using your computer. Viruses can destroy or distribute information stored on your computer.
- ✓ Do not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source, especially if the subject line is questionable or unexpected.
- ✓ Exercise caution when downloading files from the Internet. Ensure that the source is legitimate and reputable. Verify that an anti-virus program checks the file before it is run.

- ✓ Some of the more recent viruses may cause your computer to perform abnormally slow or behave strangely.

The following precautions should be taken when transmitting patient information over the Internet:

- Send patient information via encrypted e-mail when transmitted over the Internet. (i.e. not addressed to a CHS workforce member) If you require the use of encrypted e-mail, contact Information Security.
- Submit patient information on external web sites only when the site has implemented encryption and you are approved by manager to do so. This would be denoted by a "lock" in the bottom right hand corner of your browser.
- Do not use services such as telnet or ftp (file transfer protocol) to transmit patient information over the Internet.



Access Control

- Generic user names and passwords are no longer allowed in order to access patient information. Each workforce member must have a unique user name in order to gain access to patient information.
- Using another workforce member's user name to access patient information is prohibited.
    - If someone inadvertently ordered the wrong prescription using your account, that record is tied to your user name.
- If a system you routinely use tells you the last time you logged in and it does not match the last time you were in the system, you should contact the IS Support Center for further review (i.e. The system states your last login was on Sunday and you do not work on Sunday; therefore, someone may have used your account inappropriately).

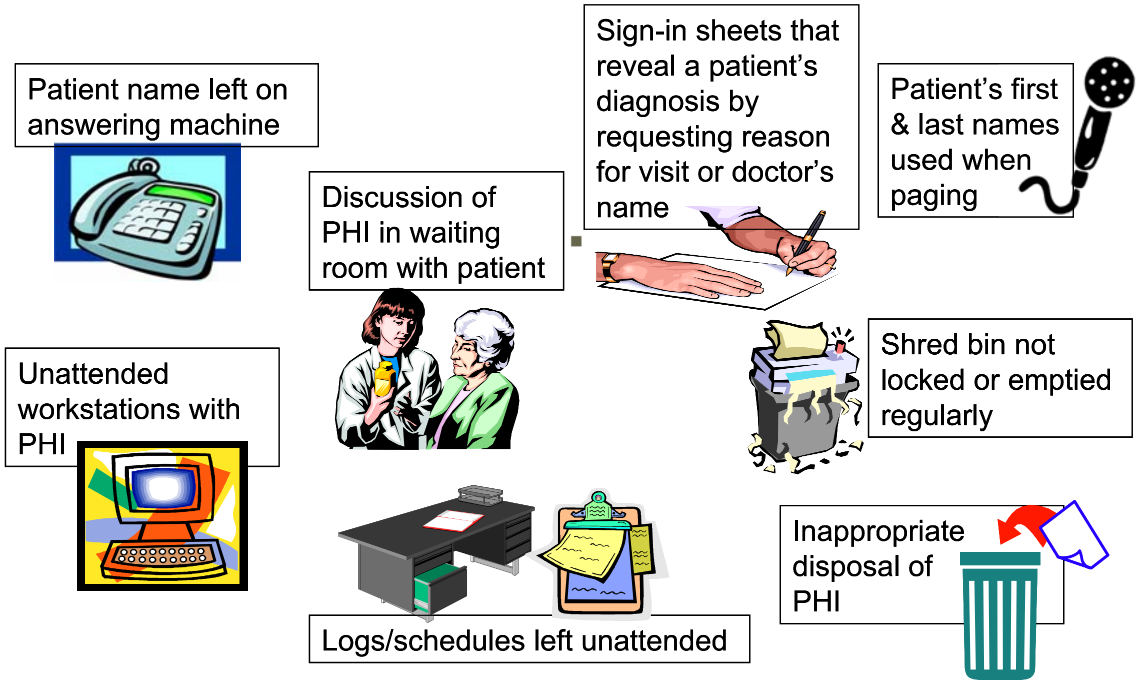
Taking data offsite

You should never 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 appropriate 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.
- Never store your passwords or access codes to patient data on your PDA.
- Consider how the data you store on your device will be backed up in the event of a catastrophic failure. Will patient information be lost?

- Ensure your virus software is up-to-date and working normally.

Common Non-Compliant Practices



Patient name left on answering machine

Discussion of PHI in waiting room with patient

Sign-in sheets that reveal a patient's diagnosis by requesting reason for visit or doctor's name

Patient's first & last names used when paging

Unattended workstations with PHI

Shred bin not locked or emptied regularly

Logs/schedules left unattended

Inappropriate disposal of PHI

HIPAA Privacy Oversight Responsibilities Assigned

	The Chief Privacy Officer, Gene DeLaddy, is responsible for coordinating and verifying that an effective privacy program is in place at each of the CHS facilities to protect the privacy of each patient. A Facility Privacy Director (FPD) leads managers at each facility in continuation of good privacy practices and policy adherence. **PR.PHI 145.14 Duties of the Chief Privacy Officer (CPO) and Corporate Privacy Depart. Staff**

HIPAA Security Oversight Responsibilities Assigned

	The Assistant Vice President of Information Security, Robert Pierce, is responsible for coordinating the implementation of appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI) for all systems managed corporately. **Reference Policy: IS.PHI 600.05 Assigned HIPAA Security Responsibility**

Getting Help

Questions Concerning HIPAA

- Contact your Supervisor
- Submit a question online: http://synapse.carolinas.org/reference/policies_procedures/hipaa/Overview/index.cfm
- Privacy Questions - 704-512-5900
  AVP, Corporate Privacy - Todd Harrington
- Security Questions - is_security@carolinas.org
  AVP, of IS - Robert Pierce

Questions Concerning HIPAA Policies

HIPAA policies can be found:

http://synapse.carolinas.org/reference/policies_procedures/corporate_safety/Administrative_Policy.cfm

Reporting HIPAA Concerns

To report a HIPAA violation call:

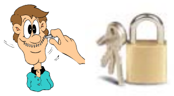
- Customer Care Line - 704-355-8363

To report potential viruses or malicious software call:

- CHS Support Center - 704-446-6161 or 866-446-6161

Customer Care Line

704-355-8363



Posttest

Name: ______________________________________

Date: ______________________________________

Circle the correct answer.

1. **Information governed by the HIPAA Privacy & Security Laws:**

   a) Is restricted to computer databases.

   b) Covers only electronically exchanged data.

   c) Includes electronic, written, and oral communications.

   d) Is limited to electronic and written communication.

2. **The Notice of Privacy Practice describes how a patient's health information may be used or disclosed by CHS to carry out treatment, payment, or health care operations.**

   a) True

   b) False

3. **If a patient's name is the only information removed from a record, the record no longer contains identifiers that can link the record to an individual patient.**

   a) True

   b) False

4. **Patients have a right to request access to their protected health information.**

   a) True

   b) False

5. **If a workforce member is contacted by a government official concerning a privacy issue, the workforce member should not answer any immediate questions, but write down the name, agency, issue/question, and other pertinent information, and tell their supervisor who will contact the AVP for Corporate Privacy immediately.**

   a) True

   b) False

6. **You can give out location and condition for patients with a “Z” beside their name?**

   a) True
   b) False

7. **The release of this type of note requires specific individual authorization even for treatment, payment, and health care operations (TPO) purposes?**

   a) Physical therapy notes
   b) Psychotherapy notes
   c) Nurses notes
   d) Social services notes

8. **When you stop by to visit a hospitalized friend or see a patient as a good will gesture, for whom you have no work assigned responsibility (Treatment, Payment or Healthcare Operations), you are entitled to the same patient information as:**

   a) People who need the information to do their job.
   b) People who are not employed by the hospital, i.e. the general public.

9. **If you, as a workforce member, find yourself in need of information about a patient, friend or seriously ill family member, you, as part of the CHS family, can use your system access to see any information or access any part of the facilities you deem necessary.**

   a) True
   b) False

10. **A workforce member who fails to comply with HIPAA policy may receive disciplinary action including:**

   a) Written Counseling.
   b) Final Written Counseling.
   c) Termination.
   d) All of the Above.

11. **Identify how leaving this message on an answering machine at the patient's home might violate a patient's privacy.**

    "This is Ed Smith from Carolinas HealthCare System calling to remind Jane Brown of her chemotherapy treatment tomorrow at ten o'clock."

    a) Jane's patient information was given out, and this would allow others in the household who might hear this message to find out about Jane's illness.

    b) The type of specialist or clinic Jane is seeing was not given, so the message did not violate Jane's privacy.

    c) Both Jane's name and treatment were stated on the answering machine, disclosing her patient information.

    d) Both a and c are correct.

12. **Doctors should be permitted to see all information about every patient regardless of whether he/she is a physician on record (admitting physician, attending physician, and/or consulting physician).**

    a) True, because the physician should have knowledge about all patients being treated in CHS facilities.

    b) False, because the HIPAA Privacy Law only allows access to patient information when a physician has a work need to know (Minimum Necessary Requirement).

13. **As you enter an elevator, you notice that a physician schedule listing patient names, diagnoses, dates of birth, social security numbers, and physician notes is lying on the floor. What should you do?**

    a) Secure the document.

    b) Tell your supervisor what you have found.

    c) Report the misuse on the Accounting for Disclosures Database.

    d) All of the above.

14. You are required to fax a patient's health information to a familiar physician's office. You place the material in the fax machine located along a busy corridor in the practice, and send it using the pre-programmed number for the physician's office. What are some additional steps you should take to protect the patient's privacy?

a) Fill out and use a CHS fax cover sheet.

b) Call before faxing to validate the fax number and briefly inquire about their ability to receive the fax in a confidential manner (i.e., is the fax machine in a secured location?).

c) Stay close by the fax machine, since your office fax machine is in an unsecured location; eliminating the opportunity for anyone to read the patient's records while it is transmitting.

d) Verify that you selected the correct fax number on the fax machine before transmitting the fax.

e) Obtain the fax confirmation sheet and verify that the fax was sent to the number you intended or call to verify that the fax was received.

f) All of the above.

15. As you enter an unattended work area, you notice a password for the computer system posted on the wall. What should you do?

a) You should notify your supervisor, the Director of Information Security, or call the Customer Care Line.

b) Nothing. You know and trust everyone in your office, and no one would abuse the access of the password.

16. The following is an example of a "strong" password: *panthers*.

a) True

b) False

17. When disposing of a CDROM that contains patient information, I should simply throw it in the trash can?

a) True

b) False

18. According to HIPAA, it is perfectly acceptable to use a generic username and password to gain access to patient information.

a) True

b) False

19. The CHS Communications Environment Acceptable Use Policy defines what is considered acceptable use for computers, phones, etc.

a) True

b) False

20. I received an e-mail from someone I don't know, and it contains an attached file that I was not expecting. What should I do?

a) Open it immediately and see if it deletes my hard drive.

b) Send it to everyone I work with to see if they sent it to me.

c) Do not open it and contact the IS Support Center.

d) All of the above.

21. Anyone can "shadow" a healthcare professional to learn more about Carolinas Healthcare System as long as the individual has approval from the department or practice.

a) True

b) False

22. Workforce members treating patients who are hospitalized as a result of a motor vehicle accident and at the request of the investigating law enforcement officer should provide:

a) No information without an authorization or court order.

b) Patient name.

c) Patient's current location.

d) Whether the patient appears to be impaired by alcohol, drugs, or other substances.

e) B, C & D

23) 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 & Procedure Manual, [IS. PHI 600.01]. Please check the "Yes" box (or sign, if taken manually) before submitting test to receive your score. An affirmative answer is required for the successful completion of the HIPAA Privacy and Security post test.

a) □ Yes

(Complete this section if post test was taken manually)

Workforce member Name: (Print) ______________________________________

Workforce member Name: (Signature) _________________________________

Date: ________________________

Score: __________

Manager's Initials: _________

Back to exams

Glossary

Covered Entity – A health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a transaction.

Disclosure – Providing patient information / protected health information (PHI) to people outside CHS who should have limited PHI for example as required by law.

HIPAA - The Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted by Congress in 1996. It includes:

- Privacy Law — Describes the patients' right to determine how their health information is used or kept private as well as the covered entities' responsibility in maintaining patient information in a private manner.

- Security Law — Describes the means (process and technology) by which an entity protects electronic health information from tampering, destruction, or inappropriate access.

- Other Laws: Identifiers, Transactions and Code Sets, etc.

Misuse – Providing patient information / protected health information (PHI) to people inside or outside CHS who should not have the patient information.

Notice of Privacy Practices (NPP)- The NPP describes how a patient's health information may be used or disclosed by CHS to carry out Treatment, Payment, and Health Care Operations (TPO), as well as describing an individual's rights regarding their health information. A copy of CHS's current NPP is available on the CHS internet web site, as well as at every point of entry for each of the CHS facilities. Each patient will then be asked to sign a written acknowledgment demonstrating that he or she has received a copy or been offered a copy of CHS's NPP.

Patient's Rights - The rights an individual has regarding his or her health information include:

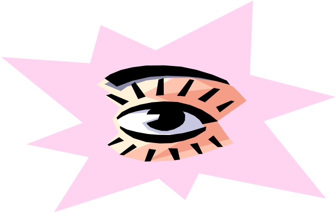
- Right to inspect and obtain a copy of their health information
- Right to request an amendment to their health information
- Right to request restrictions regarding the use and disclosure of their health information
- Right to request confidential communications regarding their health information
- Right to an accounting of disclosures concerning their health information
- Right to a paper copy of the Notice of Privacy Practices

PHI (Protected Health Information) a.k.a. Patient Information - defined as any piece of patient information that individually or collectively can be used to reveal information about a particular patient's health.

Practical Applications – Follow these guidelines to avoid the misuse of patient information in your day-to-day activities

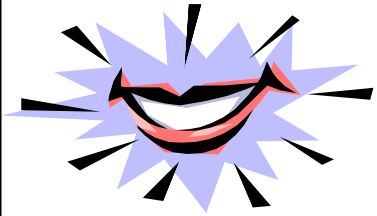
Hearing

- Avoid discussions concerning patient information in public areas such as the cafeteria, elevator, or hallways or on mobile phones or in electronic mail messages.
- Speak in hushed tones, particularly in curtained areas, and clear non-essential people from the area in open treatment areas, registration areas, semi-private rooms, etc.
- Do not discuss patient, family, or employee medical information with anyone who is not involved in the patient's care without specific authorization from the patient to do so.



Seeing

- Avoid faxing patient health information to unsecured locations.
- Immediately remove faxed information from the fax machine.
- Position computer screens to protect against casual viewing by third parties.
- Shred or dispose of patient information using confidential bins provided throughout your facility.
- Appropriately limit the patient information requested on sign-in sheets, etc. Diagnosis or chief complaint should never be included by inference or out right.



Talking

- Do not leave messages which:
  - Contain laboratory and test results.
  - Link a patient's name with clues about his/her diagnosis or medical condition, unless you have authorization to do so.
- Avoid leaving detailed appointment reminders or information that might indicate the diagnosis, type of test, type of clinic or specialist the patient is seeing.
- Exercise caution when leaving a message for a patient, particularly if the condition or treatment involves issues that are often more personal (i.e., those related to psychotherapy, infertility, substance abuse, pregnancy, or HIV).
- When a companion accompanies the patient to the treatment area and sensitive information is to be discussed, ask the patient if you can discuss the information in front of their companion.

Access

- Do not leave patient files, reports, or other information unattended or uncovered where staff or the public, without a need to know, can access the patient information.

- Limit access to the patient's chart and medical record to the medical team involved in the patient's care.

- Obtain or verify written authorization prior to releasing patient information.

- Seek advice from Corporate Privacy before disclosing patient medical records and related patient-identifiable health information to anyone other than the patient or the patient's designee.

- Do not use or share patient information for your own professional or personal use.

- Do not look at your records, records of a friend or other patients' records unless you are involved in treatment, payment or healthcare operations for that patient.

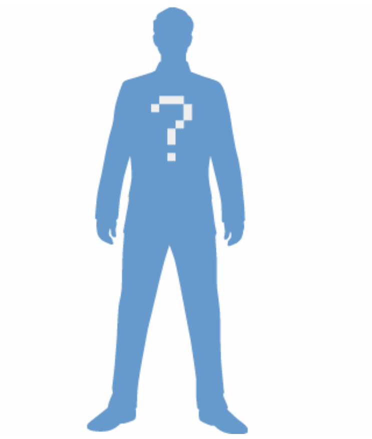
- Keep computer passwords confidential.

- Do not leave computer programs or e-mail programs open in the event another individual may gain unauthorized access.

- When disposing of old computers, remove all patient records, billing information, and patient health information stored in the computer.

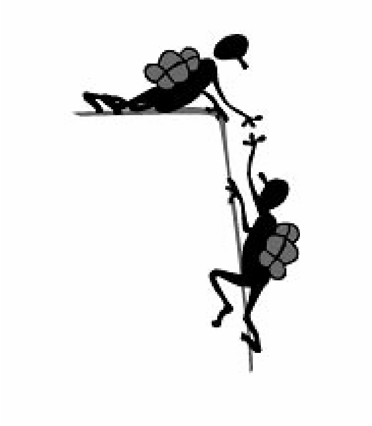
- Ensure computer disks with patient health information are maintained, used and destroyed in such a manner that no one will use the information improperly, such as selling the data to a marketing or pharmaceutical company. Should you have questions regarding the disposal process, please contact IS.

- Secure computer stations to minimize the ability to view and read the computer screen.



Verifying an individual's identity and authority to access patient information

One way you may confirm a caller's intentions is by asking the caller their name and their relationship to the patient; then look at the family names listed in the patient's chart to verify that their name is on the list. Is the patient in the hospital because of domestic violence? Keep it simple: Verification is most times as simple as checking with the patient to determine whether you can reveal information about the patient's situation. Patients may object to you sharing their information even with some well meaning family members. You will need to verify the patient's wishes.



What is my role?

It is important to keep your work environment safe and secure when you are not there. Remember to do the following:

- Secure all patient information to prevent unauthorized access,
- Close computer programs,
- Secure equipment such as printers, faxes, copiers, and
- Lock office doors.

If you step away from your workstation momentarily:

- Ask your co-workers to make certain no one accesses the patient information unless authorized
- Close or turn over patient information
- Turn over clinic schedules or similar documents

In day to day use of PHI:

- Use coversheets with sign-in sheets
- Limit information on white boards or sign-in sheets

Patient Directory Information

Visitors - In the absence of instructions from a patient or a patient's legal representative to the contrary, a CHS employee may disclose the following information about a patient, only if the inquiring individual has asked for the patient by a combination of at least two names the patient is listed by in the CHS registration system.

- ✓ The location and room number in all CHS applicable facilities, except for substance abuse and behavioral health patients (diagnostic descriptors should not be included in room number).

- ✓ The general condition in terms that do not communicate specific medical information about the patient:

  a. **Undetermined** - Patient awaiting physician assessment
  b. **Good** - Vital signs are stable and within normal limits. Patient is alert and comfortable. Indicators are excellent.
  c. **Fair** - Vital signs are stable and within normal limits. Patient is conscious, but may be uncomfortable. Indicators are favorable.
  d. **Serious -** Vital signs may be unstable and not within normal limits. Patient is acutely ill. Indicators are questionable.
  e. **Critical -** Questionable prognosis. Vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable.

Clergy - In the absence of instructions from a patient or a patient's legal representative to the contrary, a CHS employee may disclose the following information about a patient to authorized members of the Clergy for their specific church or in some cases, denomination:

1. Name
2. General condition in terms that do not communicate specific medical information about the patient
3. The location and room number in all CHS applicable facilities can be provided except for substance abuse and behavioral health patients (diagnostic descriptors should not be included in room number)
4. Religious Affiliation