Carolinas HealthCare System

2013 Annual Continuing Education Module

Corporate Compliance and Privacy

For Teammates

This self-directed learning module contains information all CHS Teammates are expected to know in order to protect our patients, our guests, and ourselves.

Target Audience: All Non-Management CHS Teammates, Students, Volunteers, and Physicians

Instructions

- Read this module and complete the post-test. If you have questions about the material, ask your supervisor.
- If you are completing the post-test manually, please include your signature and the date and give it to your supervisor.
- Record the date of completion on your Teammate Annual Continuing Education Record

Learning Objectives

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

- **Explain** the importance of a compliance and privacy program
- **Identify** key elements of the CHS Code of Conduct: A System of Integrity.
- **Understand** critical compliance and privacy concepts and policies, laws, and regulations that apply to your role within the System
- **Know** how to properly use the Chain of Command to get help when you have a compliance or privacy question or concern
- **Know** how and when to use the Compliance HelpLine or Customer Care Line

Compliance

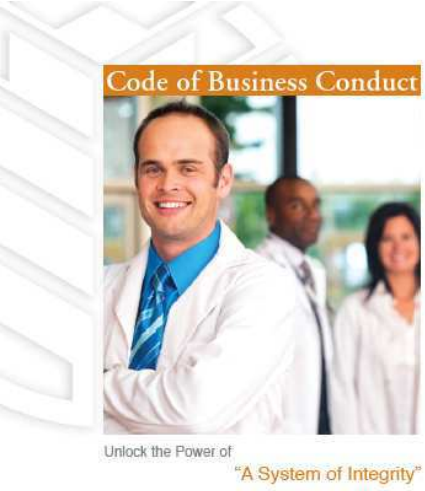
What is a compliance program and *why* do we have one?

Recently, government officials have been cracking down on healthcare fraud and abuse, making compliance programs more important than ever. Healthcare fraud can occur through improper documentation and billing, conflicts of interest, improper patient care, and many other areas.

The CHS Corporate Compliance Program:

- Educates Teammates on laws and regulations affecting their roles within the system
- Identifies potential fraudulent activity (accidental or intentional) on the front end
- Provides guidelines to follow when we are faced with questions of ethics or good business practices
- Encourages Teammates to do the right thing all the time, even when no one is looking
- Affirms our long-time commitment to fair and ethical business practices.

Our Code of Conduct: A System of Integrity



Our Code of Conduct, **A System of Integrity**, helps CHS Teammates uphold the core values of the System by:

- Giving Teammates guidance on ethical matters including our Core Values and Guiding Principles
- Providing a clear understanding of what is expected in the work environment; and
- Explaining what Teammates should do when faced with difficult situations

Carolinas HealthCare System
Uncompromising Excellence. Commitment to Care.

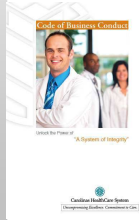
Critical Compliance Concept: Patient Care

As a system, we expect that all Teammates will:

- Provide excellent patient care and customer service.
- Treat every patient with dignity and respect.
- Keep protected health information confidential.
- Inform the patient of his/her rights and responsibilities.
- Recognize the patient's right to participate in treatment decisions.
- Provide prompt and courteous customer service.

Ask Yourself:

- Do I always treat patients with respect and dignity?
- Am I careful not to let my personal feelings or circumstances interfere with patient care?
- Do I respect the privacy rights of our patients?
- Do I respect the confidentiality of patient medical and financial information?

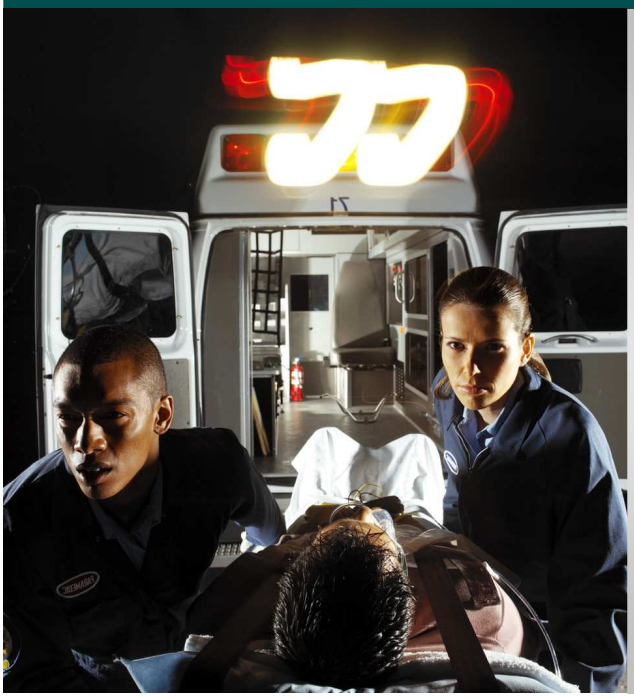


System of Integrity Reference: Page 8

Spotlight: EMTALA

Emergency Medical Treatment and Active Labor Act

Any person who comes to the hospital requesting an evaluation for an emergency medical condition must be provided a medical screening examination by a qualified medical professional to determine if he/she has an emergency medical condition, in which case he/she must be stabilized or appropriately transferred to another facility.



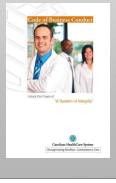
Important Points:

- EMTALA applies regardless of a patient's insurance status, race, nationality, etc.
- We are obligated to provide medical screening and respond to external inquiries for transfer.
- Hospitals or physicians who fail to fulfill these obligations are subject to fines and penalties.
- Transfers for financial reasons are never appropriate
- It is better to accept a transfer that is borderline than to refuse it.

Critical Compliance Concept: Conflicts of Interest

A conflict of interest is a relationship, influence, or activity that impairs or gives the appearance of impairing one's ability to make objective and fair decisions in the performance of his/her job.

CHS does not wish to do business through the improper use of business courtesies, gifts or relationships.



System of Integrity Reference: Page 11

Conflicts of Interest	Acceptable Gifts
• **Use of organizational supplies for personal business**	• **Non-routine business meals of a nominal value for business or educational purposes**
• **Direct or indirect ownership of a company that is a competitor or a supplier for CHS**	• **Promotional items such as pens, notepads, or other items of nominal value**
• **Acceptance of gifts (unless of nominal value) from people doing business or who want to do business with the system**	• **Educational business travel WITH PRIOR APPROVAL**
• **Hiring or contracting with family members to provide goods or services to the organization**	

IMPORTANT NOTE

Gifts of CASH or CASH-EQUIVALENTS are NOT appropriate without prior approval

Ask Yourself:

- Do I ensure that my relationships do not influence how I perform my job duties?
- Do I refrain from using business equipment and supplies for personal use?
- Do I disclose any business relationship that may be a conflict of interest to my supervisor or the Corporate Compliance department?
- Do I avoid accepting lavish gifts or entertainment from customers or suppliers?
- Do I ensure that I request reimbursement only for normal, out-of-pocket expenses incurred when serving as a speaker or member of an advisory board?
- Do I contact my supervisor or corporate compliance when I am not sure if I can keep a gift I have been offered?

For more information on conflicts of interest, refer to CHS Policy COR 40.17—Conflicts of Interest, available via PeopleConnect.

Critical Compliance Concept: Documentation and Billing

Proper Documentation

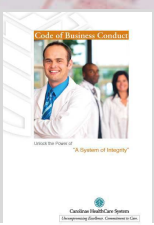
- Proper documentation is important in every aspect of healthcare delivery.
- System records should be prepared accurately, honestly, timely, and in accordance with established financial, accounting, medical and legal procedures.
- Critical areas requiring proper documentation include:
  - Medical Records
  - Physician Orders for services provided, test results and dictated reports
  - Billing records

Proper Billing

- We bill only for care and services provided which are properly authorized and documented as medically necessary.
- It is CHS's policy to refund any overpayments made as a result of billing errors
- The Patient Protection and Affordable Care Act (PPACA), signed into law in March 2010, requires identified overpayments to be reported, including explanation as to the reason for the error.

Ask Yourself:

- Are all bills for services supported by clinical documentation?
- Does the clinical documentation support the necessity for and the level of services provided?
- Do I refrain from altering bills in any way in an attempt to avoid third party edits or denials?
- If I am unsure how to properly process a bill, do I request further information to avoid improper billing?



System of Integrity Reference: Page 18

Policy Reference: COR 40.10

Spotlight: Fraud and Abuse

The False Claims Act

A false claim is a fraudulent request or demand for money; for example, billing Medicare for services a patient never received.

It is a violation of the False Claims Act for a healthcare provider to submit fraudulent or false claims for payment to programs that are funded by Federal or State governments such as Medicare or Medicaid.

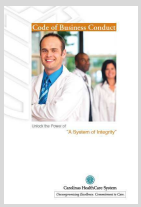
What do I need to know?

- There are serious consequences at both a Federal and State level for false claims, including losing Medicare or Medicaid funding, monetary penalties, and possibly jail time.
- If a teammate knows or reasonably suspects a false or fraudulent claim has been submitted, he or she must report this immediately.
- Teammates who report known or suspected False Claims Act violations in good faith are known as “whistleblowers” and are protected under the law and by CHS (Refer to CHS Policy COR 40.06—Non-Retribution/Non-Retaliation)

How do I report?

Teammates may report known or suspected false claims by notifying any of the following :

- Supervisor or Department Head
- Facility Compliance Officer (FCO) - Find your FCO by visiting the Corporate Compliance Website on PeopleConnect
- Corporate Compliance Department
- Compliance HelpLine



System of Integrity Reference: Page 19

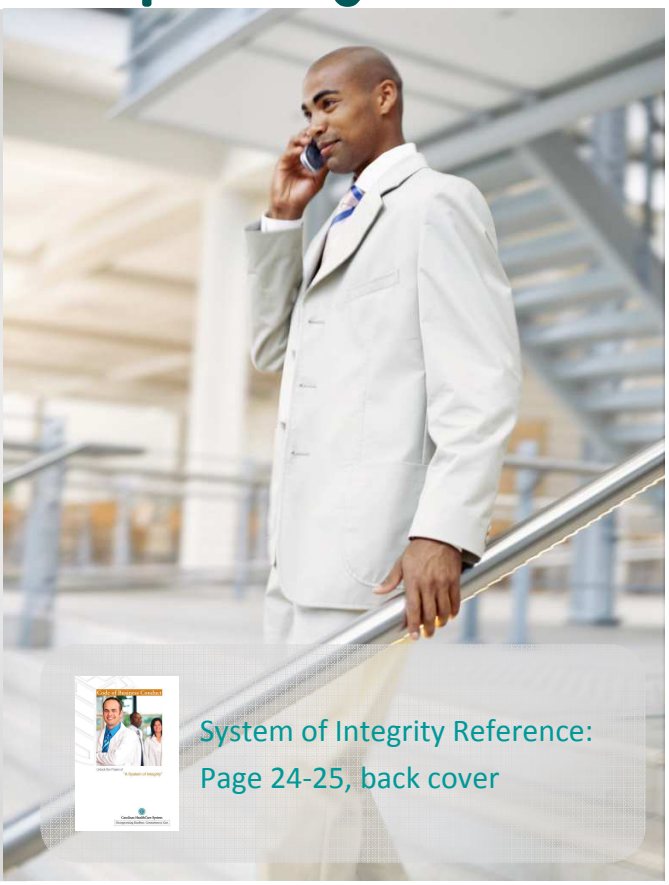
Critical Compliance Concept: Reporting Concerns

The Compliance HelpLine

CHS has contracted with an outside firm for an independent, toll-free Compliance HelpLine available at 888-540-7247. This provides Teammates with a way to anonymously report possible violations of the System of Integrity or any laws or regulations.

Key Points:

- Available 24 hours a day, 7 days a week.
- Operated by an independent contractor.
- Calls are forwarded to CHS within 24 hours; emergencies are forwarded immediately.
- CHS investigates and responds to all HelpLine inquiries.
- Callers may follow up on the status of an inquiry.
- Retaliation against a teammate for providing information to the HelpLine is prohibited.



System of Integrity Reference: Page 24-25, back cover

NOTE: THE HELPLINE IS NOT INTENDED TO REPLACE CURRENT PROCEDURES FOR RESOLVING CONCERNS

The Chain of Command

I have a compliance question or concern

Talk to your supervisor

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

Talk to your supervisor's supervisor

If you are uncomfortable discussing it with your supervisor's supervisor

For Human Resources Issues	For Compliance Issues
Your facility's Human Resources Department	Your Facility Compliance Officer
The appropriate regional Human Resources Office	The Compliance HelpLine or the Corporate Compliance Department

Critical Compliance Concept: Reporting Concerns

HR or Compliance?

HUMAN RESOURCES ISSUES

- Timekeeping/ time abuse
- Pay rates
- Breaks
- Work-related training
- Job descriptions
- Discrimination
- Termination
- Promotions
- Hiring Practices
- Workplace violence
- Disagreements among coworkers

COMPLIANCE ISSUES

- Medical record documentation errors
- Inaccurate billing or accounting
- Falsification of medical or accounting records
- Falsification of reimbursement claims
- Conflicts of interest
- Business courtesies/gifts
- Inaccurate record-keeping
- Failure to collect patient co-pays or deductibles

Important Policies

THE FOLLOWING POLICIES ARE AVAILABE VIA PEOPLECONNECT AND ARE IMPORTANT FOR ALL TEAMMATES TO KNOW:

COR 40.06—Non-Retribution/Non-Retaliation:

No disciplinary action will be taken against any Teammate who reports in good faith a perceived problem or violation of the CHS Code of Conduct

For example—a teammate cannot be disciplined for making an honest report to the HelpLine or to his or her supervisor

COR 40.14—Enforcement and Discipline:

Failure to follow the CHS Code of Conduct may result in disciplinary action including the possibility of termination.

Ask Yourself:

- Am I familiar with the CHS Corporate Compliance Policies?
- Do I contact my supervisor, FCO, or the Corporate Compliance Department immediately when I have compliance questions or concerns?
- Do I understand how to properly utilize the Chain of Command?

HIPAA PRIVACY & SECURITY

What is HIPAA?

HIPAA, the Health Insurance Portability & Accountability Act, is a civil rights law that gives patients important rights with respect to their protected health information (PHI).

What is PHI?

PHI includes any information that is created or received while a healthcare worker is providing treatment, processing payment, or performing other healthcare operations. PHI relates to the past, present or future physical or mental health of a patient and can be contained in electronic, written and oral communications .

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

NOTE: ALL CHS WORKFORCE MEMBERS (TEAMMATES, STUDENTS, VOLUNTEERS, PHYSICIANS. ETC.) ARE REQUIRED TO ENSURE THE PRIVACY AND SECURITY OF OUR PATIENTS' PROTECTED HEALTH INFORMATION!!

PHI: Patient Identifiers*

A patient's identity can be discovered without knowing his or 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
- Email 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: 42 CFR § 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 records!

Here are some examples of other places you might find PHI:

- **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**

ACCESSING PHI

Appropriate Access to PHI: Three HIPAA Recognized Purposes

HIPAA permits the use of PHI for ***treatment, payment,*** and ***healthcare operations.***

Do you have a TPO need to know?

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

Treatment

Sending PHI from one department to another within the same facility so that a procedure can be performed

Providers/physicians sharing information between themselves regarding a patient they both treat

Referring a patient to a specialist

Payment

Determining eligibility or coverage under a plan

Billing and collection activities

Reviewing healthcare services for medical necessity, coverage, justification of charges, etc.

Healthcare Operations

Conducting quality assessment and improvement activities

Reviewing the competence or qualifications of healthcare professionals

Conducting or arranging for medical review, legal and auditing services including fraud and abuse detection and compliance programs

Special Note: Patient Authorization:

Uses and disclosures of PHI that fall outside of TPO Purposes typically require a patient's written authorization. CHS has a standard process and form for that authorization. HIPAA allows for limited exceptions to the TPO and Authorization rules. Examples include medical emergencies, threat to the health or safety of the patient, certain law enforcement activities and court orders.

For more information about the authorization process and exceptions, refer to the Release/Review of Medical Information Policy: PR.PHI 140.05.

Inappropriate Access to PHI: Common Non-Compliant Practices

- Viewing medical information belonging to yourself, your family, friends, coworkers or other patients when you are not a member of the health team treating the patient
- Emailing patient information to the wrong address or faxing patient information to the wrong number
- Discussing PHI in a public location where others are likely to overhear, such as an elevator or the cafeteria
- Informing a friend of a patient's presence at the hospital
- Accidentally handing a patient another patient's discharge instructions
- Sharing or allowing access to your passwords
- Sign-in sheets that reveal a patient's diagnosis
- Leaving a workstation unattended without logging out
- Improperly disposing of PHI

ACCESSING PHI

Appropriate Uses of PHI: Incidental Disclosures*

Certain practices are permissible under the HIPAA 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 or use a whiteboard for scheduling purposes.
- A physician may discuss a patient's condition QUIETLY in a semi-private room or 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 patient over the phone.

NOTE: In emergency situations, loud emergency rooms, or where a patient is hearing impaired, precautions may not be practical. In these cases, healthcare staff are free to engage in communications as required for quick, effective and high quality healthcare.

*HIPAA Reference: 45 CFR § 164.502(a)(1)(iii)

Proper Disposal of PHI: What's in your trash?

You should dispose of any material that contains PHI using the appropriate method: confidential bin, shredder, or medical waste receptacle.

Paper

All paper containing PHI must be deposited in a locked, confidential shred bin.

Labels

Removable labels containing PHI should be removed from the container and rendered unreadable before being discarded in the regular trash. If the label cannot be removed or destroyed, discard the label or empty container in a regulated medical waste receptacle.

ID Bracelets

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

Electronic PHI (e-PHI)

Items containing electronic patient information should be disposed of in accordance with IS Policy IS.PHI 600.06 (available via PeopleConnect)

Policy Reference: PR.PHI 145.15 "Disposal Procedures for Patient Information"

HELP! I found PHI!

If you happen to find PHI that has not been properly disposed of (e.g. an ID bracelet that has been dropped on the floor or a fax cover sheet left in an open recycle bin, bring the PHI to your supervisor immediately.

HIPAA: PATIENTS' RIGHTS

Accept or Deny

We are not obligated to agree, but we *are* obligated to respond in a timely manner with an explanation of denial.

HIPAA grants patients the following rights with respect to their 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**—Patients have a right to request an amendment to their medical record. We are obligated only to review the request and determine whether an amendment is justified and appropriate.
3. **Accounting of Disclosures**—Patients have a right to know who has seen their information without their authorization. This is currently applicable only to uses outside of TPO.
4. **Restrictions**—Patients have a right to request restriction or limitation on information we use or disclose for TPO purposes. They may also request a limit on information we provide to family or friends.
5. **Confidential Communications**— Patients have a right to request communication about medical matters in a specific format or location, but this request may be denied due to logistical obstacles in implementing them.

NOTE: CHS HIPAA Policies and Procedures are available on the HIPAA SharePoint Site, accessible via PeopleConnect.

CHS's Notice of Privacy Practices

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.


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

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

Did You Know?

A copy of the CHS Notice of Privacy Practices is available on the CHS inter-net website, each facility's website, and at every point of patient entry at each of the CHS facilities.

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

Spotlight: Protecting PHI

Taking Data Offsite

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

- When using a laptop or other electronic device containing PHI offsite, do NOT store the PHI on the device unless the device is encrypted. To make sure your device is properly encrypted, contact Information Services.
- Papers containing PHI are even more vulnerable than electronic devices storing PHI. Anyone who comes into 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 notify your supervisor.

Identity Theft Alert: RED FLAGS

The term "Red Flag" refers to any pattern, practice or specific activity that indicates the possibility that IDENTITY THEFT has occurred. The following are examples of red flags you may come across in both clinical and non-clinical settings:

Clinical Setting

- **The patient's medical condition does not match the medical record.**
- **Records are inconsistent with the patient's physical state 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 or equipment with patient or Teammate information.**
- **Alerts from consumer reporting or fraud detection agencies.**

CHS HIPAA Sanctions

When CHS workforce members use PHI inappropriately, regardless of intent, the privacy of patient's PHI may be compromised. Workforce members who inappropriately use PHI are subject to disciplinary action which may include the following:

VERBAL COUNSELING | **WRITTEN COUNSELING** | **FINAL WRITTEN COUNSELING** | **TERMINATION**

Disciplinary action is based upon several factors including severity of the violation. Refer to CHS Policy PR.PHI 145.13

SECURITY 101

The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards to ensure the confidentiality, integrity and availability of *electronic* PHI (e-PHI).
CHS's Acceptable Use Policy: IS.PHI 600.01 outlines appropriate use of CHS Resources. Review this policy before taking the post test.

NEVER share your user ID and password with anyone.

- Do not respond to email, phone or other requests for your user ID and password. No one from Information Services, including the CHS Support Center, will EVER ask for this.
- Do not share your password with co-workers, including new Teammates that may not have access.

DO NOT open, forward, or reply to email messages from unknown or suspicious senders.

- Look for spelling and/or grammatical errors
- Look for requests for personal information: "Our records indicate that your account was overcharged. You must complete the following form within 7 days to receive your refund."
- Be on the lookout for alarming messages: "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, confirm by clicking on the link below."

Use different passwords for different accounts.

- Keep social networking sites (e.g. Facebook, Twitter and Pinterest) separate from online banking.
- Keep personal accounts separate from CHS accounts (e.g. social networking sites and online banking.)

Be a safe internet user.

- Look for "https://" when entering PHI, credit card information, or other sensitive information online.
- Do not click on pop-ups (advertisements, warnings, etc.).
- Do not download unapproved software.
- Be cautious when downloading documents; be sure you are on a site you know and trust

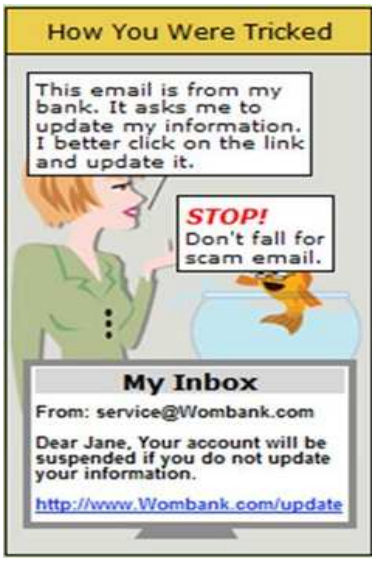
Contact the CHS Support Center Immediately IF:

- You accidentally clicked on a suspicious link or replied to a suspicious email
- You suspect that someone else knows or is using your password
- You receive unusual error messages or pop-up boxes
- You lost your laptop, smartphone, or other mobile device used to store CHS data or access the CHS network.

NOTE: Use caution when sending PHI via email. You should send only the minimum information needed. If you are 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.

SECURITY SPOTLIGHT: SPEAR PHISHING

Did you know that email phishing is the easiest way for criminals to steal information?



The Phisher forges email addresses to look genuine

The Phisher entices you with an urgent request

The Phisher adds links that appear to connect to a real bank but brings you to a counterfeit site to take your information and money!

Never give out your password to anyone; including Information Services!

Requests for login or personal information via email or texting are known as PHISHING.

"Phishing" is the act of sending an email pretending to be from an online store (Amazon, eBay), a financial institution (Chase, SunTrust), or even a Help Desk with the intention of gaining personal information from the recipient. The email usually claims that you need to go to a link provided in the email to update your account information. Phishing uses this technique to obtain personal information such as credit card numbers, bank PINs, and Social Security numbers. Like traditional fishing, it relies on a computer user taking the bait.

Examples of Phishing Messages

- **"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below."**
- **"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."**
- **“Our records indicate that your account was overcharged. You must complete the following form within 7 days to receive your refund.”**

How to protect yourself from Phishing Scams:

Legitimate companies don't solicit personal of sensitive information via email. Delete messages that ask you to confirm or provide personal information (credit card, bank account & Social Security numbers, date of birth, passwords, etc.).

Don’t reply, and don’t click on links or call phone numbers provided in the message. These messages direct you to spoofed sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.

Call the company directly to verify. If you’re concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card, not the number provided in the message.

Spotlight: Social Networking

Social media is a great tool that allows individuals to communicate via networking sites such as LinkedIn, Facebook, Twitter, and Pinterest. It is important to remember that the internet is a public domain and information posted via social media can be permanent and may have a broadcasting effect. You have an obligation to safeguard PHI regardless of the setting. You should never 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.

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 your own, not those of 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 10-11 of the Acceptable Use Policy for more details on this subject.

Ask Yourself:

- Will my posted comments have a harmful or perceived harmful effect on another individual 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?

REPORTING CONCERNS

Chain of Command:

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 OFFICER

Contact the CHS CORPORATE PRIVACY DEPARTMENT 704-512-5900

Contact the CUSTOMER CARE LINE 704-355-8363

Important Contacts:

Questions about HIPAA:

1. Contact your Supervisor
2. Contact your Facility Privacy Officer (FPO) *.
3. Privacy Questions: 704-512-5900—Deanie Auton, AVP Corporate Privacy
4. Security Questions: 704-446-6383—Robert Pierce, AVP Information Security
5. HIPAA Privacy and Security SharePoint Site: http://sharepoint.carolinas.org/hipaaprivacy

HIPAA Policies and Procedures can be found on the CHS Intranet:

HIPAA Policies are located in the "Patient Rights" Section of the Administrative Policy and Procedure Manual.
http://peopleconnect.carolinas.org/policies

Who is my FPO?

Each CHS facility has a Facility Privacy Officer (FPO) who serves as the privacy representative for that facility.
A list of FPO's is available on the CHS Intranet:
http://peopleconnect.carolinas.org/hipaa