Compliance & Privacy For Teammates

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

Target Audience: All Carolinas HealthCare System Teammates,
Students, Volunteers, and Physicians

Learning Objectives

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

- **Understand** patient privacy rights and how patient information is kept private and confidential in a work setting
- **Know** how to use and disclose patient information and how to safeguard patient information

- **Know** how to report a privacy or a compliance concern
- **Explain** the importance of a compliance program
- **Identify** key elements of the Carolinas HealthCare System Code of Conduct: *A System of Integrity*
- **Understand** critical compliance 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 privacy or a compliance question or concern
- **Know** how and when to use the Compliance HelpLine

How does CHS Prevent & Identify Non-Compliance?
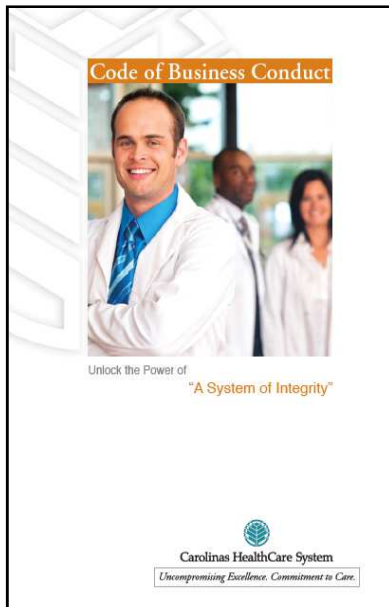
Carolinas Health Care System's Code of Conduct, *A System of Integrity,* is an important resource for all teammates, conveying:

- Carolinas HealthCare System's commitment to Compliance and Privacy
- The Compliance and Privacy Programs' expectations for teammates

Our Compliance & Privacy Programs:

- Provide teammates with policies and guidance related to workplace decisions;
- Help teammates understand potential compliance and privacy violations; and
- Describe the reporting mechanisms available to teammates when they need to discuss a compliance or privacy concern.

This ACE Module will explore Carolinas Health Care System's Privacy and Compliance Programs.

Patient Privacy

Privacy

Patient Privacy is a law!

The Health Insurance Portability & Accountability Act, better known as HIPAA, protects patient information and gives patients important rights.

Patient Information is:

- Any information that is created or received by Carolinas Healthcare System about an individual
- Information that is related to treatment, billing, or healthcare operations
- Can be electronic, written, or oral

NOTE: ALL CAROLINAS HEALTHCARE SYSTEM TEAMMATES, STUDENTS, VOLUNTEERS, PHYSICIANS, ETC. ARE REQUIRED TO PROTECT THE PRIVACY AND SECURITY OF OUR PATIENTS' PROTECTED HEALTH INFORMATION!!

Patient Information is Everywhere!

It's not just in the paper or electronic 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 identification bracelets**
- **Prescription bottle labels**
- **Detailed appointment reminders left on voicemail**
- **Photograph or video recordings of a patient**

PATIENT RIGHTS

- **Notice of Privacy Practices (NPP):** Patients have the right to receive a copy of our NPP.
  - English and Spanish copies are available on carolinashealthcare.org, each facility's website, and at every point of patient entry at each of our facilities/practices.
- **Restrictions & Confidential Communication:** Patients can restrict the use or disclosure of their information and request confidential communications.
- **Inspect & Copy:** Patients can inspect and/or receive a copy of their healthcare records.
- **Amendments:** Patients can request an amendment (correction) to their healthcare records.
- **Accounting of Disclosures:** Patients can request a list showing when and with whom their information has been shared.
- **Complaints:** Patients can file a complaint with a healthcare provider, insurer, and the U.S. Government if the patient believes his or her rights have been violated.
- **Breach Notification:** Patients are notified when their patient information has been compromised.
- **Paid in Full:** Patients can pay for their services in full and request that their healthcare provider not share information with their health plan. We **must** agree to this type of restriction.

Accessing Patient Information

TREATMENT, PAYMENT, OPERATIONS
"TPO"

Patient information should <u>only</u> be accessed for legitimate treatment, payment, or health care operation reasons (quality, education, risk management, etc.).
All other uses or disclosures require an Authorization, an exception, or a law!

DO NOT:

- Access patient information because you are curious regardless of the reason
- Access patient information as a favor to family and friends
- Access your own information through our resources
- Use someone else's login and password

Resist Curiosity – It's Not Worth It

- Every access to the patient record <u>is tracked</u> and can be audited
- Using someone else's login is a violation of policy and will subject you to disciplinary action
- Unauthorized access, including physicians, will be sanctioned

Protect Patient Privacy 24/7

- Sharing information with friends or family outside of work is <u>*never*</u> appropriate and is not allowed.
- All CHS teammates agree to not repeat or reveal any patient information.
- Talking about or sharing patient information will be cause for disciplinary action up to and including termination.

Disposing Patient Information

Dispose of Patient Information Properly!

Dispose of anything that contains patient information in a confidential shred bin, crosscut shredder, or medical waste receptacle.

Paper

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

Labels

Removable labels containing patient information should be discarded in a locked shred bin or regulated medical waste receptacle.

ID Bracelets

ID bracelets removed by a workforce member should be disposed of in a locked 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 on PeopleConnect)

Be on the lookout!

➢ Look for discarded patient information in areas that patients may leave their personal information (such as examination rooms, trash cans in the lobby, etc.)

➢ Post warning signs around trash/recycle cans to properly dispose patient information

Keeping It Down: Incidental Disclosures

Avoid Incidental Disclosures

Incidental Disclosures happen when you are properly using and sharing patient information as part of your job, but it is inadvertently overheard or seen by someone who does not have permission to have access to the information.

Examples: discussions with patients in semi-private rooms or ED bays, calling a patient name in the waiting room (but not discussing their medical condition), whiteboards or computers on wheels in treatment areas.

Avoid releasing too much information!

Reasonable Safeguards

✓ Only use and disclose the <u>minimum</u> patient information requested or required.

✓ Avoid conversations about a patient in front of other patients, visitors, families.

✓ Lower your voice when discussing patient information in person or over the phone.

✓ Avoid conversations about patients in public places (hallways, waiting areas, elevators, cafeteria)

Talking In Front of Family and Friends

Sometimes it's okay to talk to friends and family

They must be involved in the patient's care or payment, and you can only share what they need to know.

- ✓ The patient's friend comes with the patient into the treatment room, and the patient doesn't object to them hearing the conversation
- ✓ The patient's daughter is present and has questions about the charges
- ✓ You need to tell the patient's husband how to take care of her after treatment
- ✓ There's an emergency and you need to talk to the family to make healthcare decisions
- ✓ A friend comes to pick up the prescription for the patient

Sometimes, it's not okay

- ☒ The patient tells us not to talk to their family about their condition
- ☒ A family member wants a copy of the patient's medical record (this requires a written Authorization from the patient)
- ☒ A neighbor is calling in curious to know what's going on (only friends and family indicated by <u>the patient</u> are allowed to get information)

CLEAR THE ROOM

You don't need written consent to share in these situations, but first <u>confirm the patient doesn't object</u>:

- ✓ Give the patient an opportunity to object to who hears the information. If possible, clear the room before you start talking about the patient's personal condition, and make sure the patient is okay with everyone coming back into the room to hear the information.
- ✓ If the patient is unconscious or not available, use your professional judgment to decide if it is in the <u>patient's</u> best interests to share the information.
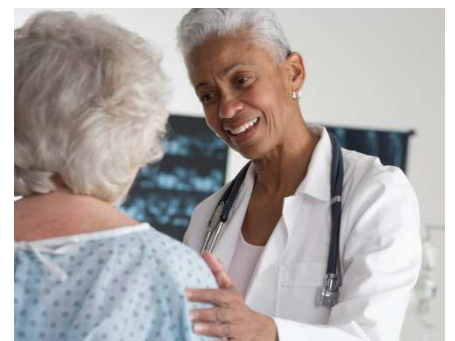
Always Verify Before You Disclose

ALWAYS VERIFY YOU HAVE THE RIGHT PATIENT!

Always check at least *two* (2) patient identifiers (ex: name, DOB, address) to make sure you have the right patient, especially when **handing out patient information.**

Pay particular attention to:
- Medical records
- Receipts
- Depart summaries
- Discharge instructions
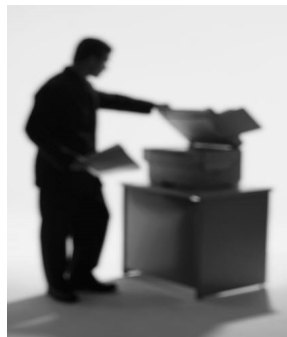- Lab results
- Prescriptions

Best Practices When Mailing Patient Information:
- ✓ Double check mailing address.
- ✓ Make sure documents only contain that patient's information.

Best Practices When Faxing Patient Information:
- ✓ Double check the fax number before faxing every time.
- ✓ Use HIPAA compliant fax cover sheet.
- ✓ Check the confirmation page.

Verify Someone's Identity Before You Disclose Patient Information
- ✓ Remember to make sure people asking for patient information are who they say they are before you disclose.

Information Security: Phishing

Phishing: Sending a false email to gain personal information, such as a request for login or personal information through email or texting.

Did you know that email phishing is the easiest way for criminals to steal information?   When in doubt, do NOT click on the emails! Forward questionable emails to spamreport@carolinashealthcare.org.

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

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!

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."

Avoid Taking Confidential Information Offsite

CAUTION

If you take it, you must protect it – <u>you</u> are responsible for all patient information in your possession!

- ✓ First ask yourself: can I access this information online through secure Carolinas Healthcare System-approved portals, instead of taking it offsite?
- ✓ Only take the *minimum* patient information *necessary* to do the work.
- ✓ Always secure bags or briefcases. Remove any confidential and patient information from your vehicle or lock in your trunk. Never leave information in view or unattended!
- ✓ Inventory what patient information you take to make sure you return <u>all</u> patient information as soon as possible.
- ✓ Never take patient information into a public place, such as a restaurant or coffee shop.
- ✓ Always secure patient information in your house – do not let others (including your family and friends) view or access it.
- ✓ *If patient information or confidential information in any form is lost or stolen, notify your management or Corporate Privacy immediately!*

Workstation on Wheels

🚫 NEVER leave a workstation on wheels unattended in the hallway or in a patient's room with patient information showing!

🚫 NEVER let anyone use your login – it will show up as you in the medical record.

☑ <u>Lock the workstation every time you walk away</u>!

Information Security: Pointers

- NEVER share your user ID and password with anyone. (Our Information Services will _never_ ask you for your password!)
- DO NOT open, forward, or reply to email messages from *unknown* or *suspicious* senders.
- Use different passwords for different accounts.
- Pick *strong* passwords (8 characters: upper case, lower case and numbers).
- Reboot or shut down your computer at the end of your day to ensure security patches are properly applied.

Contact the Support Center at (704) 446-6161 *immediately* IF:
- You click on a suspicious link
- You suspect someone is using your login and password
- You receive unusual error messages or pop-up boxes
- You lose your laptop, smartphone, or other mobile device used to store data or access the network. (Contact the Support Center _before_ you cancel your wireless or phone service if your device is lost or stolen!)
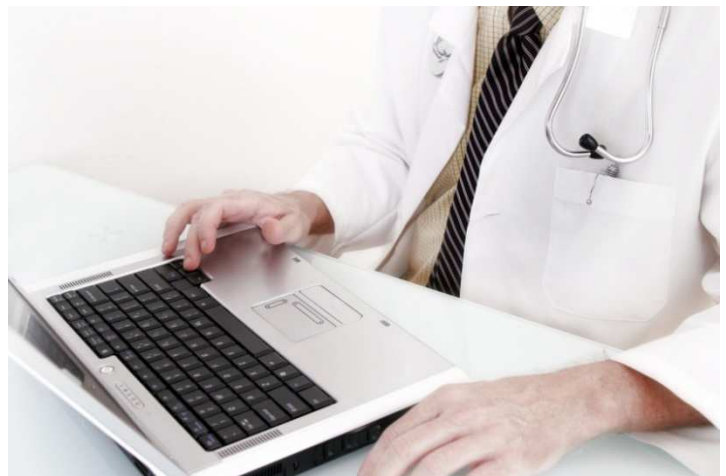
Information Security: Mobile Devices

Security Pointers

➢ Any personally owned laptops, desktops, or mobile devices used to access or store our data must receive prior approval from our Information Services. These devices must be encrypted, have anti-virus software, and appropriate applications from IS for receiving security patches. Call (704) 446-6161 for information.

➢ Do not store patient information on hard drives. Use confidential shared drives behind our firewall.

➢ Use only *encrypted* flash drives approved by our Information Services for patient information or other confidential information.

➢ Do not text *identifiable* patient information.

➢ Do not use personal cloud storage (such as ICloud, DropBox) for patient information – this is not secure!

➢ Be cautious of auto-sync settings on devices to store photos, videos, documents, etc.

CAUTION: AVOID SENDING EMAILS WITH PATIENT INFORMATION
- **Only send the absolute *minimum* patient information needed.**
- **If sending to an email address that does not end in "@carolinas.org" or "@carolinashealthcare.org", you have to send secured using Protected Trust so that the email will be *encrypted*.**
- **Sending without encrypting will be subject to disciplinary action.**

Social Networking

Social media is a great tool that allows people to communicate by networking sites, but should never be used to share patient information.

Remember!

- The internet is a public domain and information posted on social media is not private!

- Communicating patient information is strictly prohibited and will subject you to sanctions, including termination.

- You should never post identifying information about patients OR THEIR IMAGES, etc. (Removing a patient's name is not enough to make the patient anonymous).

- Look at the background! A photograph taken in the hospital or practice environment may inadvertently have a patient, computer screens, or whiteboards in the background with patient or internal information visible.

- Do not "friend" patients on social media – instead, have a professional and personal page, if you want.

What Happens When Things Go Wrong?

Carolinas Healthcare System HIPAA Sanctions

When teammates use, access, or disclose patient information inappropriately, regardless of intent, the privacy of a patient's information may be compromised. Teammates who inappropriately use, access, or disclose patient information are subject to disciplinary action, which may include the following:

- **Verbal Counseling**
- **Written Counseling**
- **Final Written Counseling**
- **Termination**

A breach of patient information can cause harm to the reputation of Carolinas HealthCare System and potentially subject us (and you) to serious penalties!

Civil and Federal Enforcements!

- Individuals can be found criminally liable under HIPAA
- Civil and criminal penalties at the State and Federal level
- Penalties of $100 to $1.5 million dollars
- Institutions can be fined for failure to act

Reporting Privacy Concerns

To report a privacy issue, or if you have a question or concern regarding privacy, you should follow the options below. You will not be penalized for reporting a potential privacy issue.

Contact Your Supervisor

And

Contact Your Facility Privacy Officer*

Or

CHS Corporate Privacy Department
704-512-5900

Chief Privacy Officer: Sara Herron, Senior Vice President
Information Security Official: Robert Pierce, Assistant Vice President

Or

CHS PeopleConnect:
- **Concern & Incident Reporting link**
  http://peopleconnect.carolinas.org/reporting-tools

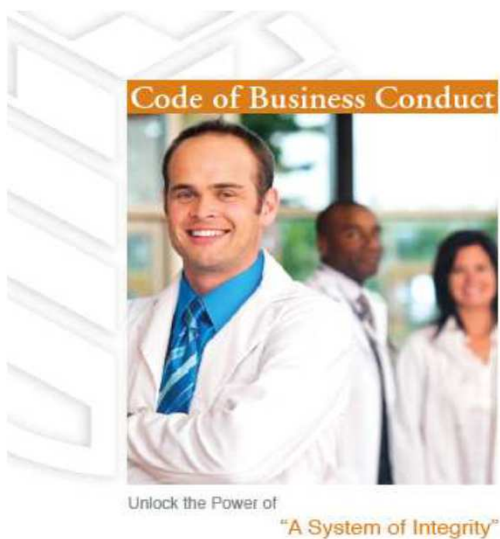- **HIPAA SharePoint–Report a Privacy Concern**

Who is my FPO?
Each facility has a Facility Privacy Officer (FPO) who serves as the privacy representative for that facility.

*A list of FPO's is available on PeopleConnect:
http://peopleconnect.carolinas.org/hipaa

The Carolinas HealthCare System Corporate Compliance Program:

- Educates Teammates on laws and regulations affecting their roles within the System
- Identifies potential fraudulent activity
- 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, no matter who is looking
- Affirms our long-time commitment to fair and ethical business practices

Code of Business Conduct

Unlock the Power of
"A System of Integrity"

Carolinas HealthCare System
Uncompromising Excellence. Commitment to Care.

Our Code of Conduct, **A System of Integrity,** helps Carolinas HealthCare System 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.

Critical Compliance Concept: Patient Care

As a System, we expect that all Teammates will:

- Recognize the patient's right to participate in treatment decisions.
- Provide excellent patient care and customer service.
- Inform the patient of his/her rights and responsibilities.
- Provide prompt and courteous customer service.
- Treat every patient with dignity and respect.
- Keep protected health information confidential.
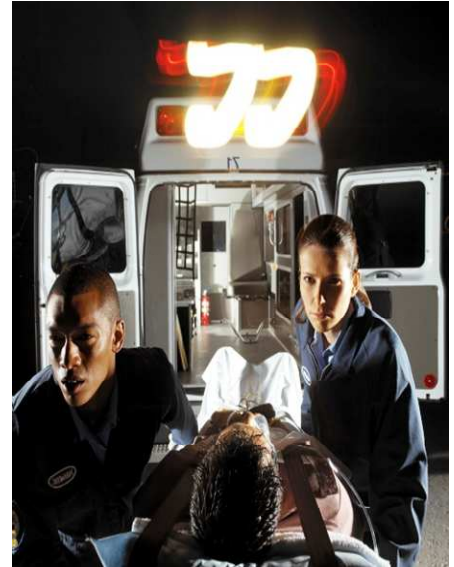
Spotlight: EMTALA
(Emergency Medical Treatment and Active Labor Act)

<u>Any person</u> 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, or nationality
- We are obligated to provide medical screening and to respond to external inquiries for transfer. Hospitals/physicians who fail to fulfill these obligations are subject to fines and penalties.
- It is better to accept a transfer that is borderline than to refuse it.
- Transfers for financial reasons are never appropriate.

Critical Compliance Concept: Conflicts of Interest

A conflict of interest is a relationship, influence, or activity impairing or giving the appearance of impairing one's ability to make objective and fair decisions in the performance of his/her job. Carolinas HealthCare System 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
❖ **Use of organizational supplies for personal business**
❖ **Direct or indirect ownership of a company that is a competitor or a supplier for the System**
❖ **Acceptance of gifts (unless of nominal value) from people doing business or who want to do business with the System**
❖ **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 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 contact my supervisor or Corporate Compliance when I am not sure if I can keep a gift I have been offered?

Critical Compliance Concept: Documentation and Billing

Proper Billing

- We bill only for care and services provided which are properly authorized and documented as medically necessary.
- It is the System's policy to refund any overpayments made as a result of billing errors.

> The Patient Protection and Affordable Care Act (PPACA) requires identified overpayments to be reported, including explanation as to the reason for the error.

Proper Documentation

- Proper documentation is important in all aspects of healthcare delivery.
- System records should comply with regulations regarding legibility, timing and dating of signatures. Back-dating , inappropriate or excessive use of copy/paste in electronic medical records is not permitted.
  Included are the following:

  - Physician Orders
  - Medical Records
  - Billing Records
  - Test Results
  - Dictated Reports

System of Integrity Reference: Page 18

Fraud, Waste & Abuse

Fraud is knowingly and willfully carrying out, or intending to carry out, fraud against any health care benefit program (Medicare or Medicaid). **Waste** involves the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program. **Abuse** includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program.

> ## What's the difference between Fraud, Waste & Abuse?
> Fraud requires the person to have an **intent** to obtain payment and the **knowledge** that their actions are wrong. Waste and abuse may involve obtaining an improper payment, but does not require the same **intent** and **knowledge**.

Potential Consequences of Fraud, Waste & Abuse

Federal and State laws and regulations and System policies and procedures help prevent and detect potential fraud, waste and abuse. In addition to monetary and criminal penalties, fraud or noncompliance has consequences for the organization and its teammates, including loss of provider licensure, exclusion from participation in federal health care programs, reputational damage and possibly jail time.

The False Claims Act

The False Claims Act's purpose is to eliminate fraud, waste and abuse. 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.

System of Integrity Reference: Page 19

Fraud, Waste & Abuse

Our Code of Conduct, **A System of Integrity**, helps Teammates prevent, identify and report fraud, waste and abuse concerns. We are committed to following all laws and regulations and conducting business in a legal and ethical manner. Should errors or noncompliance be identified, Corporate Compliance and appropriate administrators and departments, will take swift action to correct the errors and self-report, as outlined in Carolinas HealthCare System Policy COR 40.13 Self-Reporting and Claims Corrections.

How can I help prevent and detect Fraud, Waste & Abuse?

- As annually required, educate yourself by taking the Compliance ACE Module.
- Ensure data/documentation and billing information are accurate and timely.
- Always verify information that is provided to you.
- Be on the lookout for suspicious activity.
- Report concerns through the Chain of Command.

Teammates reporting suspected False Claims Act violations are protected by law and by CHS Policy; known or suspected false claims may be reported by notifying:

- 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
Policy Reference: COR 40.13
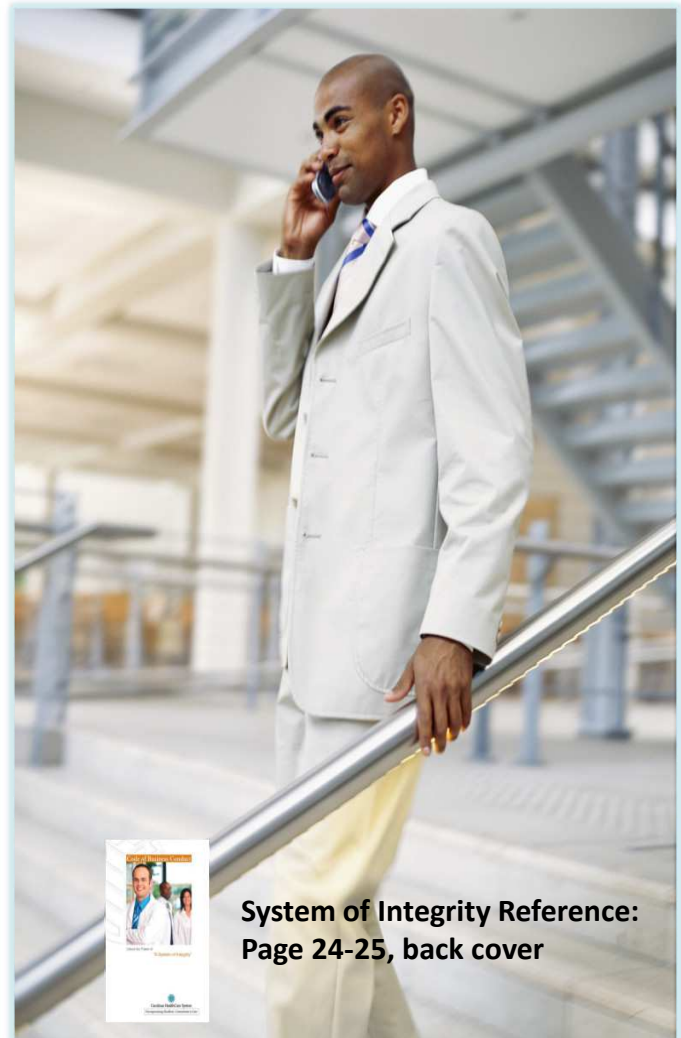
Critical Compliance Concept: Reporting Concerns

The Compliance HelpLine

Carolinas HealthCare System utilizes an external firm to provide an independent, toll-free Compliance HelpLine (888-540-7247). This gives Teammates a way to anonymously report possible violations of the System of Integrity or any laws or regulations.

Key Points regarding the Compliance HelpLine:

- Available 24 hours a day, 7 days a week.
- Operated by an independent contractor.
- Carolinas HealthCare System investigates and responds to all HelpLine inquiries.
- Callers may follow up on the status of an inquiry.

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

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

Critical Compliance Concept: Reporting Concerns

<u>The Chain of Command</u>

The Chain of Command outlines reporting mechanisms available to all teammates. However, questions and concerns can be reported directly to the Corporate Compliance department at any time.

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

Your facility's Human Resources Department

The appropriate regional Human Resources Office

For Compliance Issues

Your Facility Compliance Officer

The Compliance HelpLine or the Corporate Compliance Department

Critical Compliance Concept: HR or Compliance?

HUMAN RESOURCES ISSUES

- Timekeeping/ time abuse
- Pay rates
- Breaks
- Work-related training
- Discrimination
- Termination
- Disagreements among coworkers

COMPLIANCE ISSUES

- Documentation errors
- Inaccurate billing or accounting
- False reimbursement claims
- Conflicts of interest
- Business courtesies/gifts
- Patient Privacy Violations
- 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 Carolinas HealthCare System Code of Conduct.

COR 40.14—Enforcement and Discipline:
Failure to follow the Carolinas HealthCare System Code of Conduct may result in disciplinary action including the possibility of termination.