This course contains annual compliance education necessary to meet compliance and regulatory requirements.

**Instructions:**
To receive credit for completion:
1. Read the content in full.
2. Complete the online exam.
Corporate Compliance & Privacy

Welcome

Purpose:
The purpose of this course is to explore Carolinas HealthCare System’s (CHS) compliance and privacy programs and provide information that all teammates are expected to know to protect our patients, our visitors and ourselves.

Learning Objectives:
When finished with this course, you should be able to:

• Discuss patient privacy rights and how to keep patient information private and confidential
• Describe how and when to use, disclose and protect patient information
• Explain the importance of a compliance program and the key elements of the CHS Code of Conduct: A System of Integrity
• Discuss compliance concepts and policies, laws and regulations that apply to your role
• Identify how to report a privacy or compliance question/concern through the chain of command or the Compliance HelpLine
Corporate Compliance & Privacy

CHS Prevents and Identifies Non-Compliance

*Carolinas HealthCare System’s Code of Conduct, A System of Integrity,* is an important resource for all teammates. It covers:

- CHS’s commitment to compliance and privacy
- Expectations for teammates about compliance and privacy

The CHS Compliance and Privacy Programs help teammates with:

- Workplace decisions about compliance and privacy through policies and guidance
- Ways to identify and avoid potential compliance and privacy violations
- Guidance on how to report or discuss a compliance or privacy concern
Patient Privacy

Patient Privacy is protected by law!

A federal law, called the Health Insurance Portability & Accountability Act (HIPAA), protects patient information and gives patients important rights.

Patient Protected Health Information (PHI) is anything about an individual that is:

- Created or received by CHS
- Related to treatment, billing or healthcare operations
- In electronic, written or oral format

**All** CHS teammates, students, volunteers, providers and others working here are required to protect the privacy and security of our patients’ protected health information.
Patient Information is Everywhere

Patient information is not just in 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
- Appointment reminders left on voicemail
- Photograph or video recordings of a patient
Patient Rights

All patients have the right to:

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive a copy of a Notice of Privacy Practices (NPP). English and Spanish copies are available. You may find these notices on carolinashhealthcare.org, on each facility's website and at patient entrances.</td>
</tr>
<tr>
<td>Request that we limit the use or release of their information. Request that their communications be confidential.</td>
</tr>
<tr>
<td>Review and/or receive a copy of their healthcare records.</td>
</tr>
<tr>
<td>Request an amendment (change) to their healthcare records.</td>
</tr>
<tr>
<td>Request an accounting showing when and with whom their information has been shared.</td>
</tr>
<tr>
<td>File a privacy complaint against a healthcare provider, insurer and the U.S. Government.</td>
</tr>
<tr>
<td>Be informed when the privacy of their patient information has been breached.</td>
</tr>
<tr>
<td>Pay for their services in full and request that their healthcare provider not share information with their health plan. CHS must agree to this type of restriction for qualified situations.</td>
</tr>
</tbody>
</table>
Accessing Patient Information

Remember this acronym: **TPO** = Treatment, Payment, Operations

Patient Protected Health Information (PHI) should only be accessed for legitimate treatment, payment or healthcare 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
- As a favor to family and friends
- Because it is your own information (through CHS tools, such as the Electronic Medical Record (EMR))
- For personal gain, such as for a divorce or child custody matter
Resist Curiosity – It’s Not Worth It

Accessing patient information without permission is a serious offense.

• Every access to the patient record is tracked and can be audited

• Using someone else’s login is a violation of policy and can result in disciplinary action

• Unauthorized access to patient information will be sanctioned, including end of employment
Corporate Compliance & Privacy

Protect Patient Privacy 24 Hours a Day, 7 Days a Week

Patient information is protected. This policy applies even when you are not at work.

• Sharing information with friends or family outside of work is not allowed, even when well-intended

• Teammates are not to repeat or talk about any patient information, even if they don’t mention the patient’s name

• Talking about or sharing patient information will lead to disciplinary action up to and including end of employment
Corporate Compliance & Privacy

Throwing Away Patient Information

Throw away patient information properly!

Throw away anything that contains patient information into a confidential shred bin, crosscut shredder or medical waste container.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Labels</th>
<th>ID Bracelets</th>
<th>Electronic PHI (e-PHI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Throw away all paper containing patient information into a locked shred bin</td>
<td>• Throw away removable labels containing patient information into a locked shred bin or regulated medical waste container</td>
<td>• Throw away ID bracelets into a locked shred bin</td>
<td>• Throw away items containing electronic patient information in accordance with IS Policy IS.PHI 600.06 (available on PeopleConnect)</td>
</tr>
</tbody>
</table>

Be on the lookout for:

Discarded patient information in areas that patients may leave their personal information (such as examination rooms, trash cans in the lobby and bathrooms)

Policy Reference: PR.PHI 145.15 “Disposal Procedures for Patient Information”
Incidental Disclosures

Sometimes, as part of your job, you use or disclose patient information that may be overheard or inadvertently seen by someone else. These situations are called **incidental disclosures**. While you should try to minimize incidental disclosures as much as possible, they are not necessarily privacy violations.

Some examples of how to limit incidental disclosures, while still appropriately using patient information to care for patients, include:

- Keeping your voice down when discussing information with patients in semi-private rooms or Emergency Department (ED) bays
- Only calling out a patient name in the waiting room (but not discussing their medical condition or any other treatment information)
- Only displaying limited information on whiteboards and turning computer screens away from public view in areas where others might see them
Clear the Room

Give the patient a chance to say if it is or is not okay to share medical information with friends and family.

- Give the patient an opportunity to decide who hears the information.
  - If possible, clear the room before you start talking about the patient’s personal condition. At this time, you can ask him/her with whom information can be shared.
  - If you can’t clear the room, let the patient know you are going to talk about his/her health information and give the patient a chance to object.

- Use your professional judgement to decide if it is in the patient’s best interest to share the information when the patient is unconscious or not available, such as in surgery.
## Talking in Front of Family and Friends

Sometimes it’s okay to talk in front of family and friends. Sometimes it’s not okay.

<table>
<thead>
<tr>
<th>It’s okay to:</th>
<th>It’s not okay if:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Share only necessary information when family/friends are involved in the patient’s care or payment</td>
<td>• The patient asks you not to talk to his/her family about his/her condition</td>
</tr>
<tr>
<td>• Examples:</td>
<td>• A family member wants a copy of the patient’s medical record. This requires a written authorization from the patient.</td>
</tr>
<tr>
<td>– The patient’s friend comes into the treatment room and the patient doesn’t object to them hearing the conversation</td>
<td>• A curious neighbor is calling to know what’s going on. Only friends and family indicated by the patient are allowed to get information.</td>
</tr>
<tr>
<td>– The patient’s child is present and has questions about the charges</td>
<td></td>
</tr>
<tr>
<td>– The patient’s spouse needs treatment care information</td>
<td></td>
</tr>
<tr>
<td>– You need family input to make healthcare decisions in an emergency situation</td>
<td></td>
</tr>
<tr>
<td>– A friend comes to pick up the prescription for the patient</td>
<td></td>
</tr>
</tbody>
</table>
Corporate Compliance & Privacy

Show Patients You Care -- Always Make Sure You Have The Right Patient!

Always check at least two patient identifiers (for example, name, date of birth, address) to make sure you have the right patient. This is especially important when handing out, mailing or faxing patient information.

Pay special attention to:

• Medical records
• Receipts
• Depart summaries
• Discharge instructions
• Lab results
• Prescriptions

When mailing or faxing patient information:

- Double check the mailing address
- Double check the fax number before faxing every time
- Make sure documents only contain that patient’s information
- Use a HIPAA compliant fax cover sheet and fill it out completely
- Check the fax confirmation page
Corporate Compliance & Privacy

Information Security: Phishing (Electronic Theft of Information)

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

When phishing, the criminal:

- Makes up fake email addresses to look genuine
- Tricks you with an urgent request
- Adds links that appear to connect to real sites. These links take you to a fake site to steal your information and money.

Phishing is when someone sends a false email to gain personal information, such as a request for login or personal information through email or texting.

Remember: Never give out your password to anyone, including Information Services!
To: you@carolinashealthcare.org

We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below:
www.donotclicklinksfromunknownsenders.com

To: you@carolinashealthcare.org

Our records indicate that your account was overcharged. You must complete the following form within seven days to receive your refund.

Click to complete form.

To: you@carolinashealthcare.org

During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.

When in doubt, do NOT click on the emails! Forward questionable emails to:
spamreport@carolinashealthcare.org
Avoid Taking Confidential Information Offsite

If you take confidential information outside of a Carolinas HealthCare System facility, you must protect it. **You** are responsible for all patient information in your possession!

<table>
<thead>
<tr>
<th>If you must take confidential information offsite:</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Ask yourself first: Can I access this information online through secure Carolinas Healthcare System-approved portals, instead of taking it offsite?</td>
</tr>
<tr>
<td>❑ Take as little patient information needed to do the work</td>
</tr>
<tr>
<td>❑ Always protect your bags or briefcases. Remove confidential and patient information from your vehicle or lock in your trunk. Never leave information in view or unattended!</td>
</tr>
<tr>
<td>❑ Keep a list of what patient information you take. Return all patient information as soon as possible.</td>
</tr>
<tr>
<td>❑ Do not take patient information into a public place, such as a restaurant or coffee shop</td>
</tr>
<tr>
<td>❑ Secure patient information in your house. Do not let others (including family and friends) view or access it.</td>
</tr>
<tr>
<td>❑ Notify your leader or Corporate Privacy immediately if patient information or confidential information is lost or stolen. Notify Information Services immediately if you lose an electronic device.</td>
</tr>
</tbody>
</table>
Corporate Compliance & Privacy

Secure Workstations

When using a workstation, including a computer on wheels:

- **NEVER** leave it unattended in the hallway or in a patient’s room with patient information showing. Unauthorized people might see information or start typing in the medical record.

- **NEVER** let anyone use your login and password. It will show up as you in the medical record. This is a violation of CHS policy.

- Lock the workstation **every time** you walk away so others, including patients and visitors, cannot access or change information. This will also prevent people from accessing information under your login credentials.
Protecting Information – Tips to Know

<table>
<thead>
<tr>
<th>Protect information by following these tips:</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Never share your user ID and password with anyone. CHS Information Services will never ask you for your password!</td>
</tr>
<tr>
<td>❑ Do not open, forward or reply to email messages from unknown senders. When in doubt, do not open it or click on it.</td>
</tr>
<tr>
<td>❑ Use different passwords for different accounts</td>
</tr>
<tr>
<td>❑ Pick strong passwords. Include at least 8 characters with a mix of upper case, lower case, numbers and special characters, if required. Use words and numbers that cannot be easily guessed. For example, do not use Summer 2015 or Password1.</td>
</tr>
<tr>
<td>❑ Reboot your computer at the end of your day to make sure security patches are properly applied</td>
</tr>
</tbody>
</table>

Want more information? Visit PeopleConnect.Carolinas.Org/Protect-Our-Patients and stay connected with #ProtectOurPatients on Yammer.
### Protect mobile devices by following these tips:

- Receive permission from Information Services before using personally owned laptops, desktops or mobile devices to access or store CHS data. Approved devices must be encrypted, have anti-virus software and appropriate applications from Information Services for receiving security patches. Call 704-446-6161 for information.

- Do not store patient information on hard drives. Use confidential shared drives behind the firewall.

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

- Do not text information that could identify the patient in any way.

- Do not use personal cloud storage, such as iCloud or DropBox, for patient information. These are not secure!

- Be careful of auto-sync settings on devices that store photos, videos and documents.

---

**Acceptable Use Policy: IS.PHI 600.01 outlines appropriate use of our Resources. Review this policy before taking the exam.**
Corporate Compliance & Privacy

Contact the Support Center for Help

<table>
<thead>
<tr>
<th>Immediately contact the Support Center at 704-446-6161 if:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✧ You click on a suspicious link</td>
</tr>
<tr>
<td>✧ You suspect someone is using your login and password</td>
</tr>
<tr>
<td>✧ You receive unusual error messages or pop-up boxes</td>
</tr>
<tr>
<td>✧ You lose your laptop, smartphone or other mobile device used to store data or access the network</td>
</tr>
</tbody>
</table>

NOTE: Contact the Support Center before you cancel your wireless or phone service if your device is lost or stolen.
Avoid Sending Emails With Patient Information

If you must email patient information:

- Send as little patient information as needed
- Encrypt messages when emailing patient information and anything with social security numbers to an address that does not end in:
  - @carolinas.org
  - @carolinashealthcare.org
- Send emails using Protected Trust to encrypt the message

NOTE: Sending emails without encrypting them may result in disciplinary action.
Social Networking

Social media should **never** be used to share patient information. The internet is open to the public. Information posted on social media is not private!

- Never communicate patient information through social media. It is not allowed and will result in disciplinary action, including sanctions and end of employment.
- Never post identifying information about patients or their images. **Removing a patient’s name is not enough to make the patient anonymous.**
- Look at the photo backgrounds. Photos taken may accidentally show a patient, computer screens or whiteboards with patient or internal information.
- Do not “friend” patients on social media.

*Policy Reference: HR 5.08 Social Media Policy and IS.PHI 600.01 “Communications Environment Acceptable Use”*
Corporate Compliance & Privacy

Carolinas HealthCare System HIPAA Privacy & Security Sanctions

When teammates use, access or disclose patient information inappropriately, regardless of intent, the privacy of a patient’s information may be compromised.

<table>
<thead>
<tr>
<th>Internal Consequences</th>
<th>Civil and Federal Enforcements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Teammates who inappropriately use, access or disclose patient information are subject to disciplinary action, which may include the following:</td>
<td>A breach of patient information can damage the reputation of CHS and potentially subject CHS (and you) to serious penalties:</td>
</tr>
<tr>
<td>• Verbal counseling</td>
<td>• Individuals can be found criminally liable under HIPAA</td>
</tr>
<tr>
<td>• Written counseling</td>
<td>• Civil and criminal penalties at the State and Federal level</td>
</tr>
<tr>
<td>• Final written counseling</td>
<td>• Penalties up to $1.5 million dollars</td>
</tr>
<tr>
<td>• Termination</td>
<td>• Institutions can be fined for failure to act</td>
</tr>
</tbody>
</table>

## Reporting Privacy Concerns

To report or ask a question about a privacy issue, follow one or more of the options below. You will not be disciplined for reporting a possible privacy issue.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
<th>Option 3</th>
</tr>
</thead>
</table>
| Contact your Leader  
AND  
Contact your Privacy Officer/Representative* | Contact the Corporate Privacy Department at 704-512-5900 | Use PeopleConnect to report a concern |

Facilities, practices and certain corporate services have privacy representatives that can help.

*A list of Privacy Officers/Representatives are available on PeopleConnect: [http://peopleconnect.carolinas.org/hipaa](http://peopleconnect.carolinas.org/hipaa)

For Security issues, call the IS Support Center at 704-446-6161.

Chief Privacy Officer: Sara Herron, RN, SVP
Information Security Official: Robert Pierce, AVP

Concern & Incident Reporting link: [http://peopleconnect.carolinas.org/reporting-tools](http://peopleconnect.carolinas.org/reporting-tools)

HIPAA SharePoint Report a Privacy Concern link: [http://teams.carolinas.org/sites/HIPAA/Privacy/SitePages/Corporate%20Privacy%202015.aspx](http://teams.carolinas.org/sites/HIPAA/Privacy/SitePages/Corporate%20Privacy%202015.aspx)
Corporate Compliance & Privacy

Carolinas HealthCare System Compliance Program

**An effective Compliance Program:**

- Educates teammates on laws and regulations affecting their roles
- Identifies potential fraud
- Provides steps for teammates to follow when 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 CHS’s long-time commitment to fair and ethical business practices

**CHS’s Code of Conduct, A System of Integrity,** helps teammates to uphold CHS’s core values by providing:

- Guidance on ethical matters, including CHS Core Values and Guiding Principles
- A clear understanding of what is expected in the work environment
- What to do when faced with difficult situations
Teammates are expected to:

- 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
Emergency Medical Treatment and Active Labor Act (EMTALA)

EMTALA says that any person requesting an emergency medical evaluation will receive a medical screening examination. This exam is to be provided by a qualified medical professional to determine if the patient has an emergency medical condition. If there is an emergency medical condition, the patient must be stabilized or appropriately transferred to another facility.

Important points about EMTALA:

• EMTALA applies regardless of a patient’s insurance status, race or nationality
• Carolinas HealthCare System must provide medical screenings and respond to external inquiries for transfer. Failing to do either of these things may lead to fines and penalties for hospitals and/or providers.
• It is better to accept a transfer that is borderline than to refuse it
• Transfers for financial reasons are wrong and illegal

Source: Systems of Integrity Reference: p. 8
Conflicts of Interest

A conflict of interest is a relationship or activity that can affect (or appear to affect) someone’s ability to make fair and objective decisions in his/her job.

Carolinas HealthCare System (CHS) does not do business through the improper use of favors, gifts or relationships.

The following would be considered conflicts of interest:

- Using CHS property or supplies for personal use
- Owning (directly or indirectly) a company that is a competitor or a supplier for CHS
- Accepting gifts (unless of minimal value) from people doing business or who want to do business with CHS
- Hiring or contracting with family members to provide goods or services
Corporate Compliance & Privacy

Avoiding Conflicts of Interest

Ask yourself:

- Do I avoid using business equipment or supplies for personal use?

- Do I disclose any business relationship that may be a conflict of interest to my leader or the Corporate Compliance department?

- Do I avoid accepting lavish gifts or entertainment from customers or suppliers?

- Do I contact my leader or Corporate Compliance when I am not sure if I can keep a gift I have been offered?

Source: System of Integrity Reference: p. 11
For more information, refer to CHS Policy COR 40.17 - Conflicts of Interest
Corporate Compliance & Privacy

Fraud, Waste and Abuse

What is fraud, waste and abuse?

<table>
<thead>
<tr>
<th>Fraud</th>
<th>Waste</th>
<th>Abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Knowingly carrying out, or planning to carry out, fraud against any healthcare benefit program (Medicare or Medicaid)</td>
<td>• Overusing services that result in unnecessary costs to the Medicare Program</td>
<td>• Carrying out actions that may cause unnecessary costs to the Medicare Program</td>
</tr>
</tbody>
</table>

What is the difference between fraud and waste/abuse?

<table>
<thead>
<tr>
<th>Fraud</th>
<th>vs.</th>
<th>Waste/Abuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud requires the person to have the goal (intent) to get payment and the knowledge that his/her actions are wrong.</td>
<td>Waste/abuse may involve getting an improper payment, but does not require the same intent and knowledge.</td>
<td></td>
</tr>
</tbody>
</table>
Corporate Compliance & Privacy

Potential Consequences of Fraud, Waste and Abuse

Federal and State laws and regulations and Carolinas HealthCare System (CHS) policies and procedures help prevent and detect potential fraud, waste and abuse.

In addition to fines and criminal penalties, fraud or noncompliance has consequences for CHS and teammates, including:

- Loss of provider licensure
- Exclusion from participation in federal healthcare programs
- Damage to reputation
- Possibly jail time
False Claims Act

The purpose of the False Claims Act is to do away with fraud, waste and abuse.

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.

CHS’s Code of Conduct, A System of Integrity, helps Teammates prevent, identify and report fraud, waste and abuse. CHS is committed to following all laws and regulations and conducting business in a legal and ethical manner. If errors or noncompliance are discovered, CHS will take fast action to correct and self-report the matter.

Policy Reference: COR 40.13 “Self-Reporting and Claims Corrections”
Once fraud, waste or abuse is discovered, it must be corrected fast!

Correction is important. Correction shows that CHS is following the laws and protects our ability to receive healthcare program payment.

CHS Policy COR 40.13 Internal Investigation and Self-Reporting outlines the steps for correction and self-reporting. The Corporate Compliance Department oversees these actions.

Policy Reference: COR 40.13 “Self-Reporting and Claims Corrections”
### Preventing and Detecting Fraud, Waste and Abuse

You can help prevent and detect Fraud, Waste and Abuse:

- Educate yourself every year by taking the *Corporate Compliance & Privacy* ACE Course
- Make sure documentation and billing information are accurate and timely
- Make sure the information that is provided to you and that you provide is correct
- Be on the lookout for suspicious activity
- Report concerns through the Chain of Command (see slide 39)

Teammates who report suspected False Claims Act violations are protected by law and by CHS Policy. Report known or suspected false claims by notifying:

- Your leader or department head
- Facility Compliance Officer (FCO). Find your FCO by visiting the Corporate Compliance Website on PeopleConnect
- Corporate Compliance Department
- Compliance HelpLine

*Policy Reference: COR 40.13 and System of Integrity Reference: p. 19*
## The System of Integrity: Other Important Compliance Considerations

<table>
<thead>
<tr>
<th>The Anti-Kickback Statute</th>
<th>The Stark Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The Anti-kickback Statute forbids anyone from offering kickbacks (bribes, rebates) for referrals for services or purchases of products or items paid under a federal healthcare program</td>
<td></td>
</tr>
<tr>
<td>• CHS and/or its vendors can be fined up to $25,000 and/or involved persons put in prison for up to 5 years for breaking this law</td>
<td></td>
</tr>
<tr>
<td>• The Stark Law regulates financial relationships between hospitals and physicians</td>
<td></td>
</tr>
<tr>
<td>• The Stark Law prohibits physicians from referring certain services to an entity where the physician has an ownership/investment interest or compensation arrangement, unless certain exceptions are met</td>
<td></td>
</tr>
<tr>
<td>• Medicare claims that violate the Stark Law will not be paid. These claims may be subject to fines up to $15,000 for each service. Parties involved in prohibited arrangements are also subject to fines up to $100,000.</td>
<td></td>
</tr>
</tbody>
</table>
## Documentation and Billing

### Correct and Legal Billing

- CHS bills only for care and services provided that 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) requires identified overpayments to be reported, including explanation as to the reason for the error.

### Correct Documentation

- Correct documentation is important in all aspects of healthcare
- System records are to be readable, timely and have properly dated signatures
- Back-dating, incorrect or too much use of copy/paste in electronic medical records is not allowed
- Medical records include:
  - Physician Orders
  - Medical Records
  - Billing Records
  - Test Results
  - Dictated Reports

---

System of Integrity Reference: p. 18
Policy Reference: COR 40.10
## Exclusion From Federal Healthcare Programs

<table>
<thead>
<tr>
<th>Dealing with Persons or Businesses Excluded from Federal Healthcare Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CHS cannot take payment from any person or business that has been disqualified (barred) from federal healthcare programs</td>
</tr>
<tr>
<td>• The Compliance department monitors to identify persons or businesses that have been disqualified (excluded) by federal healthcare programs</td>
</tr>
<tr>
<td>• If a disqualified (excluded) person or business is identified, CHS refunds any money received from federal healthcare programs that was a result of activities ordered or performed by the person or business</td>
</tr>
</tbody>
</table>
Corporate Compliance & Privacy

Chain of Command

The chain of command helps teammates understand how to report concerns. Questions and concerns can be reported directly to the Corporate Compliance department at any time.

If you have a compliance or privacy question or concern:

Talk to your leader

If you don’t think you can talk to your leader:

Talk to your leader’s leader

If you are uncomfortable talking to your leader’s leader:

For Human Resource (HR) Issues, contact your:
- HR department
- Regional HR office

For Compliance or Privacy Issues, contact:
- Your Facility Compliance Officer
- The Compliance HelpLine or Corporate Compliance Department
Corporate Compliance & Privacy

Issues: Compliance and Privacy or Human Resources?

Below are examples of the differences.

<table>
<thead>
<tr>
<th>Compliance and Privacy Issues</th>
<th>vs.</th>
<th>Human Resource Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Documentation errors</td>
<td></td>
<td>• Timekeeping/time abuse</td>
</tr>
<tr>
<td>• Inaccurate billing or accounting</td>
<td></td>
<td>• Pay rates</td>
</tr>
<tr>
<td>• False reimbursement claims</td>
<td></td>
<td>• Breaks</td>
</tr>
<tr>
<td>• Conflicts of interest</td>
<td></td>
<td>• Work-related training</td>
</tr>
<tr>
<td>• Business favors or gifts</td>
<td></td>
<td>• Discrimination</td>
</tr>
<tr>
<td>• Patient privacy violations</td>
<td></td>
<td>• Termination</td>
</tr>
<tr>
<td>• Failure to collect patient co-pays or deductibles</td>
<td></td>
<td>• Disagreements among coworkers</td>
</tr>
</tbody>
</table>
Corporate Compliance & Privacy

The Compliance HelpLine – One of Your Ways to Report

Carolinas HealthCare System (CHS) uses an outside firm for its toll-free Compliance HelpLine: 888-540-7247.

The HelpLine gives teammates a way to anonymously report possible violations of the System of Integrity or any laws or regulations.

The Compliance HelpLine is:

• Available 24 hours a day, 7 days a week
• Operated by an outside contractor
• Alerts CHS to look into and respond to all reported issues
• Available for callers to follow up on the status of a reported concern

NOTE: The HelpLine is not intended to replace current steps for resolving concerns.

System of Integrity Reference: pp. 24-25 and back cover
Corporate Compliance & Privacy

Important PeopleConnect Policies

The following policies are available through PeopleConnect:

**Policy 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.

**Policy 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.
Corporate Compliance & Privacy

Summary

Carolinas HealthCare System privacy and compliance programs affirms CHS's long-time commitment to fair and ethical business practices.

The following are some actions reviewed in this course:

• How to keep patient information private and confidential
• How to use, disclose and protect patient information
• How to report a privacy or a compliance concern
• The importance of a compliance program
• The key elements of the CHS Code of Conduct: A System of Integrity
• Compliance policies and laws that apply to teammates
• How to report a question or concern through the chain of command
• How to use the Compliance HelpLine
Exam Instructions

You have come to the end of the course.

To complete the exam, follow these steps:
1. Exit this course.
2. Click Return to Course Content.
3. Click the exam link.

To receive credit for this course, you must score 80% or higher on the exam.

If you are not able to access PeopleLink Learning, print the exam. Submit the completed paper version of the exam to your leader.
Name: ___________________________  Date: _______

Circle the correct answer(s).

1. One of your family members recently had a medical procedure at the CHS facility where you work. You want to find out the results. What should you do?
   A. Use your access rights as a CHS teammate to access your family member's medical record, even though you are not involved in Treatment, Payments or Operations (TPO) and have no work-related need to know
   B. Ask a teammate who works in the department to access the record for you
   C. Wait for your family member to tell you the results, if he/she chooses to do so

2. You need to throw away papers that contain patient information. What should you do?
   A. Throw the paper away in the trash can
   B. Throw the paper away in a locked shred bin
   C. Throw the paper away in an external dumpster
   D. Leave the paper on the floor or in an unlocked box in your office

3. Which of the following is an example of how to avoid an incidental disclosure of patient information?
   A. Keep your voice down when discussing information with patients in semi-private rooms
   B. Call out patient names in the waiting room, but do not discuss medical conditions or treatment information
   C. Display only limited information on whiteboards and turn away computer screens in areas where others might see them
   D. All of the above
4. You walk into an exam room and the patient’s family and friends are in the room too. Ideally, what should you do first?
   A. Start discussing the patient’s condition in front of everyone, including her HIV status
   B. Ask the patient in front of her family and friends if she’s okay with them staying in the room
   C. Ask family and friends to step outside so you can talk with the patient alone first; then ask the patient who she is comfortable allowing back in to hear the information
   D. Answer C is best practice, but B is okay if it’s not practicable to clear the room

5. At least how many patient identifiers should you use when mailing, faxing or handing out patient information to make sure you have the right patient?
   A. Zero
   B. One
   C. Two

6. You have to take patient information off-site. Which are the correct ways to protect the information?
   A. Carry the records in a file with just a rubber band. Leave them in your car overnight.
   B. Put the records in a locked briefcase or secure envelope. Take them inside your home.
   C. Take all the records with you. Figure out later which ones you need.
   D. Only take as little information as needed. Make sure it is all returned as soon as possible.
   E. Answers B and D only
7. Any personal mobile device used to access or store patient information must be encrypted.
   A. True
   B. False

8. You are a nurse. During one of your shifts, a well-known celebrity comes to your department for treatment. It’s okay to post information or pictures about the celebrity’s appearance at the hospital on your Facebook or Twitter page because your profile is private and only your friends can see it.
   A. True
   B. False

9. Teammates who incorrectly use patient information are subject to disciplinary action, which may include ending the employment relationship.
   A. True
   B. False

10. You can report a privacy issue or incident to which of the following?
    A. Your leader(s)
    B. Privacy Officer/Representative
    C. Corporate Privacy Department
    D. Concern & Incident Reporting link on the HIPAA Privacy & Security SharePoint Site
    E. All of the above
11. The CHS Code of Conduct, A System of Integrity does which of the following?
   A. Gives teammates help with ethical issues, including CHS’s Core Values and Guiding Principles
   B. Educates teammates about their duty to report wrongdoing
   C. Explains what teammates should do when faced with difficult situations
   D. All of the above

12. Suzy comes to the hospital requesting an exam for an emergency medical condition. She does not have insurance. Because Suzy does not have insurance, EMTALA does not require the hospital to provide a medical screening examination.
   A. True
   B. False

13. Which of the following scenarios are a possible conflict of interest?
   i. Mary’s husband is running for mayor. To save money, Mary prints his campaign materials using the printer in her office at a CHS facility.
   ii. Drugs-R-Us, a pharmaceutical company, is giving an educational presentation to a group of clinicians
   iii. Dr. Wilson is an orthopedic surgeon who frequently orders medical devices from a company his brother owns
   A. All of the above
   B. i. only
   C. i. and iii. only
   D. None of the above
14. While being taught new job responsibilities, my leader tells me to take a short cut instead of following the department’s standard process. She says it will help me do my job faster. I discover that the short cut results in errors. What should I do?
   A. Contact my leader’s leader
   B. Call the anonymous Compliance HelpLine
   C. Call Corporate Compliance
   D. Don’t report anything because my leader is always right
   E. Answers A, B and C

15. Teammates who report suspected False Claims Act violations are protected by law and by CHS Policy.
   A. True
   B. False

16. Which of the following examples would be considered acceptable under CHS policy?
   A. Accepting free continuing education certificates from a vendor for classes the teammate never attended
   B. Accepting a very expensive dinner from a vendor or supplier representative
   C. Asking for business from patients on behalf of your brother’s company while on CHS time
   D. Accepting an expensive gift from another provider in return for a patient referral
   E. None of the examples are allowed under CHS policy
17. Fraud can result in consequences to Carolinas HealthCare System and its teammates. Those consequences may include which of the following?
   A. Loss of provider licensure
   B. Exclusion from participation in federal healthcare programs
   C. Damage to reputation
   D. Jail time
   E. All of the above

18. How can Carolinas HealthCare System teammates help prevent and detect Fraud, Waste and Abuse?
   A. Make sure documentation and billing information is correct and timely
   B. Always check that information provided is correct
   C. Be on the lookout for suspicious activity
   D. Report concerns through the Chain of Command
   E. All of the above
19. I attest that I have reviewed the Corporate Compliance & Privacy course and am familiar with the CHS COMMUNICATIONS ENVIRONMENT ACCEPTABLE USE POLICY (AUP) and Privacy Policies. I understand that failure to comply with the AUP and the Privacy Policies may lead to disciplinary action, up through termination of employment. The AUP and Privacy Policies may be accessed via PeopleConnect under the “Policies” tab.

Please select “Yes” or sign if taking the paper exam. A “Yes” answer is required to complete and pass your Corporate Compliance & Privacy exam.

   A. Yes

20. I attest that I have received a copy of the CHS Code of Conduct, “A System of Integrity”, and have been oriented on its contents. I understand that failure to comply with the Compliance Policies and the rules outlined in “A System of Integrity” may lead to disciplinary action, up through termination of employment. The Compliance policies and procedures are located on PeopleConnect, the CHS Intranet website.

Please select “Yes” or sign if taking the paper exam. A “Yes” answer is required to complete and pass your Corporate Compliance & Privacy exam.

   A. Yes