Our Values and Ethics At Work

KentuckyOne Health
Corporate Responsibility Program
New Employee Orientation
Learning Objectives

- Understand the importance of our Corporate Responsibility Program.
- Develop a basic understanding of relevant healthcare laws, regulations, and standards.
- Describe the resources available for obtaining guidance on an ethical or compliance concern.
- Understand options for reporting a potential violation of our standards.
- Understand your role in supporting the Corporate Responsibility Program.

"...an organization shall promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law."

### Who Regulates Healthcare?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Indian Health Services</td>
<td>The Department of Justice</td>
<td>Office of Civil Rights</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>Health Resources and Services Administration</td>
<td>Occupational Safety and Health Administration</td>
<td>Drug Enforcement Administration</td>
<td>Agency for Healthcare Policy and Research</td>
</tr>
<tr>
<td>The Joint Commission</td>
<td></td>
<td></td>
<td>Federal Aviation Admin</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td></td>
<td></td>
<td>Centers for Disease Control and Prevention</td>
</tr>
<tr>
<td>American Osteopathic Association</td>
<td></td>
<td></td>
<td>National Institutes of Health</td>
</tr>
<tr>
<td>Department of Labor</td>
<td></td>
<td></td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>National Committee for Quality Assurance</td>
<td></td>
<td></td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>American Medical Association</td>
<td></td>
<td></td>
<td>National Commission on Correctional Healthcare</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>And Many More...</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a Corporate Responsibility Program?

- Helps us understand and comply with complex laws and regulations
- Promotes a culture of honest and ethical behavior
- Provides resources for making decisions based on our entity
- Founded on our core values and standards of conduct

The primary goals of the CRP are threefold:

1. Prevent: Prevent wrongdoings. This includes failure to follow laws, regulations, and policies, including the standards of conduct.
2. Detect: Detect any wrongdoings so they can be corrected immediately.
3. Correct: Correct wrongdoings while taking steps to ensure they do not occur again.
Core Elements of a Corporate Responsibility Program

1. Written standards of conduct
2. Designated corporate responsibility officer
3. Compliance committees
4. Education and training programs
5. Complaint reporting and response process
6. System to respond to allegations of wrongdoing
7. Investigation and corrective action
8. Audit and monitoring systems
9. Measurement of program effectiveness

Corporate Responsibility Officer

Betsy Wade
Vice President, CRP Regional and ACO
Corporate Responsibility Officer
KentuckyOne Health
502-560-8404
Corporate Responsibility is about every employee striving to meet the highest standards of ethical conduct.
• As an organization and as individuals, we are responsible for promptly reporting potential violations of law, regulation, policy or procedure.

• You are protected from retaliation if you make a good-faith report, complaint or inquiry.

• If you are unsure about how to respond to a particular situation, you can use the Catholic Health Initiatives reporting process.

Catholic Health Initiatives Reporting Process:

• Speak with your supervisor or another manager.

• If the supervisor/manager is not available, or you are not comfortable speaking with him/her, or you believe the matter has not been adequately resolved, contact your human resources representative.

• Contact the Corporate Responsibility Officer

• Call the Ethics at Work Line
  - 1-800-261-5607
  - File your report at www.ethicspoint.com
We are subject to a variety of serious consequences if we fail to comply with laws, regulations and organizational policies and procedures.

- Consequences to Catholic Health Initiatives and its organizations may include:
  - Risks to patient safety
  - Refund of payments
  - Civil or criminal liability
  - Exclusion from federal programs
  - Loss of tax-exempt status

- Consequences to individuals may include:
  - Disciplinary action including suspension or termination of employment
  - Termination of contractual relationship
  - Removal from office or board membership
  - Civil or criminal liability
  - Exclusion from federal programs
Gifts

• Do not accept cash or cash equivalents (gift cards).
• Do not accept any gift of more than $100.
• May I receive a free meal from a Business Source? Yes – if a representative is on site, providing education and you have a need for the education.
• Each Business Source may provide lunch/gifts two to three times per year.
Gifts

- What type of gifts may I accept from a Business Source?
- Gifts of minimum value are acceptable, such as T-shirts, promotional pens or office supplies, and flowers, fruit, candy or other small perishable gifts. Gifts that primarily benefit patients may be acceptable if they are not of substantial value, for example, a stethoscope for use in an examination room.
EMTALA

• Emergency Medical Treatment and Labor Act is intended to prevent hospitals from:
  • Turning away or refusing to treat patients based on their ability to pay
  • Transferring patients to “charity hospitals”

• Requires medical screening exam and stabilization before transfer or discharge.
EMTALA Traps for Certain Hospitals

- Babies “We don’t treat or deliver babies!”
- Psych “We don’t treat psych!”
- Diversion “We are on diversion!”
- General comments “You’ll be treated quicker.....”
Our Values and Ethics At Work
HIPAA Privacy and Security
What is HIPAA?

Health Insurance Portability and Accountability Act of 1996

Purpose:

- Portability of insurance coverage (COBRA)
- Protect the confidentiality and security of health information
- Create a framework for standardized transmission of electronic health information

HIPAA applies to covered entities and their business associates:

- Covered Entities are health care providers, health plans/payers, and clearinghouses who send health information electronically in a transaction or code set.
- Business associates are vendors/contracts who create, receive, maintain, or transmit PHI on behalf of a covered entity.
What is PHI?

Any information about a patient written on paper, saved on a computer, or spoken, is *protected health information* (PHI), including:

- Name
- Address
- Social security number
- Phone number
- Email address
- Diagnosis
- Medical history
- Observations of health
- Medications
- Medical record number
- And many more...
HIPAA Privacy Rule

✓ Gives patients federal rights to gain access to their medical records and restricts who can see their health information

✓ Requires organizations to take measures to safeguard patient health information

✓ Requires organizations to train members of the workforce on patients’ rights to privacy and control over their health information

✓ Penalizes individuals and organizations that fail to keep patient health information confidential
Individual Rights

Patients have the following rights under HIPAA:

✓ To know who has access to their health information and how it is used (Notice of Privacy Practices)

✓ To access and request an amendment to their health records in the designated record set (Access and Amendment)

✓ To request a list of people and organizations who have received his/her health information (Accounting of Disclosures)

✓ To request that we communicate with them by alternative means (Confidential Communications)

✓ To request restrictions for the use and disclosure of their health information (Request Restrictions)

✓ To complain to a covered entity, to the Secretary of HHS, or to the Office for Civil Rights (OCR)

✓ To be notified of a breach of their health information (Breach Notification)
Use and Disclosures

- **Required Disclosures**
  - The patient or his/her personal representative
  - Secretary of the Department of Health and Human Services

- **Permitted Uses and Disclosures**
  - Treatment, Payment, and Healthcare Operations
  - Required or permitted by federal, state and local laws

- **Authorized Uses and Disclosures**
  - Patient authorization required for use and disclosures not permitted or required by the privacy rule

- **Minimum Necessary**
  - Use, disclose and request the minimum amount of PHI needed to accomplish the intended purpose

- **Limited Access**
  - Access and use of PHI is restricted to the information needed to do your job
Breach of PHI

- A breach is
  - Unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the privacy or security of the PHI.

- Breach does not include
  - Unintentional acquisition, access, use or disclosure of PHI to an employee or BA if done in good faith, in the normal course of employment or contract so long as it is not further acquired, accessed, used or disclosed by the employee or agent.

Breaches are investigated by the Office of Civil Rights, and may result in fines, penalties, or criminal prosecution.
Avoiding a Breach of PHI

- Recognize where PHI resides within your unit/workspace
- Ensure safeguards are in place to protect PHI as it enters, moves within, and exits your workspace
- Follow CHI policies for encryption of electronic messages and devices containing PHI (or ePHI)

Immediately alert your CRO, Privacy Officer/Privacy Coordinator if you suspect a breach of PHI has occurred.
The Privacy Officer

• Each Entity has an appointed Privacy Officer or Privacy Coordinator. In addition, CHI has appointed a Privacy Officer at the National and Regional level.

• The CHI National Privacy Officer and Entity Privacy Officers:
  - Manage the development of the organization’s privacy standards, policies, and procedures
  - Oversee training and education of the workforce
  - Enforce the rules and investigate violations

Privacy Officer
Marian Hughlett
Regional Privacy Officer
KentuckyOne Health
(502) 560-8347
Security Awareness and the Importance of “You”

You are first line of defense against the loss of data...
...and the devices we use

Everyone is responsible!
Be Accountable

As CHI employees, we all have legal and ethical obligations to protect patient information and to follow security best practices in this effort.

You are responsible:
- For all activities performed using your logon credentials (user names, passwords, etc.)
- To protect your passwords to prevent someone from performing activities using your identity

ACCOUNTABILITY

No Expectation Of Privacy
CHI entities regularly monitor users’ access and use of CHI IT assets

The equipment you use and the information you access on your job belong to CHI
- It is important to understand that everything you do online is monitored and tracked
- Do not expect your email, web usage or other system actions to be private
Password Security

Top Password Tips

- Don’t share them—never give your passwords to anyone else
- Make your passwords long, complex and hard to guess
- Regularly change your passwords, both business and personal
- Create different passwords for business and personal accounts
- Do not write your passwords down and leave them where others can see or find them
- Use CHI Password to change your CHI password* (type https://chipassword.catholichealth.net in your Internet browser)

Good password management and practices are important!

*This is the password you use to log on to your computer, and access Inside CHI, Outlook Webmail, Standard Time & Attendance (Kronos)
Make Security a Priority

Internet Use – The Internet Provides An Entry Point To Your Computer
- Don’t allow browsers or websites to store your passwords, remember your logons, or keep your account signed in
- Do not install plugins or add-ons into your browser

Secure Your Connections
- Always log on to the CHI VPN when accessing confidential data from a public wireless service or hotspot (coffee shop, library, hotel, airport) or your home network

Your Computer Has What You Need
- Do not download, install or otherwise use unauthorized software

Log Off Or Lock Up - Don’t Just Walk Away
- Never leave your computer unattended or unsecured while you are logged on
- Log off your computer yourself – don’t let someone else do it for you

Look Over Your Shoulder
- Use a privacy screen shield or work with your back to a wall so others cannot see your screen
Mobile and Portable Device Security

Treat Mobile And Other Portable Devices Like Cash

- Know where they are—keep laptops, cell phones and smartphones, and tablets close at hand at all times
- Limit access – Secure your devices with a PIN or passcode
- Lock them—Set your devices to automatically lock after a period of inactivity
- Do not store PHI or CHI Confidential Information on your mobile device
- Immediately report lost or stolen devices to the Service Desk
  - Call 866-236-0441
Securing Data

- Never email confidential information to a personal email account
  - Examples: Gmail, Yahoo, Hotmail

- Never save or share confidential information on public Internet or Cloud services
  - Examples include: Dropbox, iCloud, Google Docs

- Save wisely:
  - Never save confidential information to your local hard drive or a personal or non-CHI computer
  - Save confidential information on authorized devices, systems, network drives, etc.
  - Desktops, laptop computers, and USB devices are not meant for permanent data storage
  - Regularly back-up your data to a network drive
Send It Securely

Secure Email Basics

• Do not click on links included in emails (or text messages or instant messages)

• Only open attachments you are expecting and from known and trusted sources

• Don’t reply to emails (or phone calls, text or instant messages) requesting personal, patient or other confidential information

• Do not use CHI email for non-CHI business

• Never send PHI or confidential information to a personal email address

• Don’t forward suspicious emails to others – contact the ITS Service Desk

Encrypt It Before You Send It

• Type #secure# in the email Subject line to send PHI or other confidential information to authorized users outside of the CHI email system
Secure Non-Digital Information

- Secure printouts including confidential information when you leave your desk or office
  - Also applies to handwritten notes and other media—CDs, DVDs, videos, images, external hard drives, etc.

- Don’t leave confidential documents on printers, copy machines or fax machines

- Before faxing confidential data:
  - Check recipient name, fax number and authorization to receive confidential data
  - Ask if the receiving fax machine is in a secure location

- If traveling, keep confidential documents with you at all times

- Secure document disposal
  - Place unneeded documents in provided disposal bins for secure shredding
Who Do You Call?

Report Privacy and Security Incidents or Problems Immediately

It’s better to report a potential problem and discover there isn’t an issue than realize later that you should have

- Contact the ITS Service Desk to report:
  - Loss or damage to any device
  - Compromised passwords
  - Suspected virus of other malicious software activity
  - Suspicious calls or emails

Call 866-236-0441
24 Hours a Day – Every Day of the Year
The Security Officer

• Each Entity has an appointed Security Officer. In addition, CHI has appointed a National Security Officer at the National level.

• The CHI National Security Officer and Entity Security Officers:
  - Manage the development of the organization’s security standards, policies, and procedures
  - Review and mitigate security risks
  - Enforce the rules and investigate violations

Security Official
John Zuziak
Regional Information Security Manager
KentuckyOne Health
(859) 594-3060
Questions/Discussion

“The time is always right to do what is right.”

Rev. Dr. Martin Luther King Jr.
Questions/Discussion

- What’s on your mind?
- Feel free to ask questions about anything that we discussed or anything we may have missed discussing.