What we will cover in this course

✓ Compliance Basics
✓ Fraud, Waste and Abuse
✓ Deficit Reduction Act
✓ False Claims Act
✓ Whistleblower Provisions
✓ Code of Excellence
✓ HIPAA/HITECH/Security Rule Overview
What is a Compliance Program?

Simply, a compliance program safeguards the organization’s legal responsibility to abide by applicable laws and regulations.
What does a Compliance Program Do?

7 elements of an Effective Compliance Program

1. Written standards of conduct/policies and procedures
2. Compliance Oversight: Compliance Officers and Compliance Committee
3. Effective Training and Education
4. Monitoring and Auditing
5. Effectives Lines of Communication/ Reporting Process
6. Enforcement through Disciplinary Guidelines
7. Response and Corrective Action
The Code of Excellence is Spectrum Health’s Standard of Conduct.

It assists us in:

• Upholding our Core Values
• Doing the right thing, even when no one is looking

All policies and procedures can be found in Policy Tech on InSite
Element 2: Compliance Officers

Entities must designate a Compliance Officer and Committee

- Each Spectrum Health Entity has a Compliance Officer and Committee.
- The Compliance Officer is also able to meet with the President of the entity to keep them up to date on what Compliance and the Committee are working on.
Element 3: Effective Training and Education

Education and training is often the first line of defense for an organization. It can empower employees to do the right thing and prevent compliance issues. Here at Spectrum Health we do this by offering the following:

- Annual Compliance Training
  - Yearly Code of Conduct Attestation
- Onboarding
Monitoring and auditing is an important part of process improvement. It is a process that allows us to ensure that we are providing the best care possible to our patients in every aspect.

At Spectrum Health we:

- Monitor compliance with local, state and federal regulations.
  - Example areas that are monitored or audited are clinical documentation, coding, billing.
- Results including deficiencies should be report to management, compliance committee and the board.
Element 5: Reporting Process

- Talk to your contact in Spectrum Health Medical Staff Services
- Call the Office of Organizational Integrity and Compliance (616-486-2430)
- Call a Compliance Officer (616-486-2430, ask for Compliance Officer)
- Call the Integrity Help Line (1-877-319-0266)

We investigate all reported compliance concerns promptly, reasonably and confidentially to the extent possible.
Element 6: Enforcement through Disciplinary Guidelines

Everyone at Spectrum Health is expected to:

- Complete required compliance education.
- Abide by the Code of Excellence and all applicable policies and procedures.
- Report any misconduct they observe.
- Not retaliate against anyone raising a concern.

If anyone is found to have engaged in retaliatory actions or non-compliant behavior. They can be subject to performance correction, up to termination.
Element 7: Response and Corrective Action

At Spectrum Health we respond to and prevent compliance issues by:

- Completing investigations in a timely manner and correct any issues that are found.
- Providing education.
- Routinely monitoring and auditing to make sure issues have been corrected.
- Reviewing policies and procedures regularly.
- Reporting issues where appropriate to outside agencies.
Why Have a Compliance Program?

By having a compliance program we aim to prevent non-compliance with health care laws and regulations and to prevent the following:

- **Fraud**: *knowingly* making false statements or misrepresentations of facts to obtain unauthorized benefits or payments.

- **Waste**: the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare Program. Waste is generally not considered to be caused by criminally negligent actions but rather by the misuse of resources.

- **Abuse**: actions that are *unknowingly* improper, inappropriate, outside acceptable standards of professional conduct or medically unnecessary.
Laws Governing Fraud, Waste and Abuse

There are many laws that govern fraud, waste and abuse:

- False Claims Act
- Anti-kickback Statute
- Stark Law
- Social Security Act
- The United States Criminal Code
- Deficit Reduction Act

We would like to focus on the Deficit Reduction Act and False Claims Act.
What is the Deficit Reduction Act?

The Deficit Reduction Act of 2005, is multifaceted. The section of the act we will focus on is related to the three provisions that target Medicaid program integrity and fraud and abuse.

- First it provides CMS with funds to fight fraud, waste and abuse.
- Second it created incentives for states to create fraud and abuse laws that mirror the Federal law.
- Third, and most related to us here at SH, it requires that any entity that receives or makes payments to the State Medicaid program of at least $5M annual to provide their employees, contractors and agents training regarding the federal and state false claims laws and related qui tam/whistleblowers provisions.
Now we know that due to the Deficit Reduction Act we must train on the False Claim Act, but what does that mean?

The Federal False Claims Act (FCA), also known as Lincoln's Law, was initially passed during the Civil War to control fraud that was happening with military funds. It is now used to fight fraud in any federally funded contract or program, for us Medicare and Medicaid.
Activities Covered by the False Claims Act

- Knowingly presenting (or causing to be presented) to the federal government a false or fraudulent claim for payment;

- Knowingly using (or causing to be used) a false record or statement to get a claim paid by the federal government;

- Conspiring with others to get a false or fraudulent claim paid by the federal government and;

- Knowingly using (or causing to be used) a false record or statement to conceal, avoid or decrease an obligation to pay money or transmit property to the federal government.
Health care providers who violate the FCA may be subject to civil monetary penalties ranging from $11,181 to $22,363* for each false claim that is submitted.

Penalties of up to three times the amount of damages may also be ordered.

The provider may also be excluded from participating in federal health care programs such as Medicare and Medicaid.

*numbers are for 2018, will be adjusted annually
Blowing the Whistle

Using the “qui tam” (definition/whistleblower) provisions that are a part of law, any person may file a lawsuit on behalf of the government in federal court.

Once filed, the lawsuit is kept confidential or “under seal” while the government investigates the allegations and decides how to proceed.

If the government decides that the lawsuit has merit, it may intervene. In this case, the U.S. Department of Justice will try the case.

The government may decide not to intervene. In this case, the whistleblower would have to continue with the lawsuit on his or her own.
Rewards for Whistleblowers

If the lawsuit is successful, the whistleblower may receive an award ranging from 15 percent to 30 percent of the amount recovered.

The whistleblower may also be entitled to reasonable expenses, such as attorney fees.

If a court finds that the whistleblower planned or initiated the false claims, the award may be decreased. If the whistleblower is convicted of crimes related to the false claims, no award will be given.
Protection for Whistleblowers

The False Claims Act (FCA) contains important protections for whistleblowers who file claims in good faith.

Retaliation against someone who files an FCA lawsuit, or tries to stop or prevent an FCA violation, may entitle the individual to additional relief;

- including reinstatement of employment
- back pay
- compensation for costs and damages
What to do About Retaliation

Spectrum Health prohibits retaliation directed toward a person for reporting concerns in good faith, which may include but is not limited to:

- Reporting potential issues
- Investigating issues
- Conducting self-evaluations
- Audits
- Remedial actions

Any individual who commits or condones any form of retaliation is subject to appropriate discipline up to and including termination.

If you believe that retaliation has occurred it must be promptly reported to your Compliance Officer or the Integrity Help Line.
Reporting Your Concerns

If we are unsure about what to do in a given situation we must get help. Asking a question in good faith is always the right thing to do. So who can you ask for help?

- Talk to your contact in Spectrum Health Medical Staff Services
- Human Resources
- Your Compliance Officer or
- The office of Organizational Integrity & Compliance

You can also contact the Integrity Help Line at: 1-877-319-0266

This resource is available 24 hours a day, seven days a week. Calls are handled by a company outside of Spectrum Health that then refers the report to the appropriate Spectrum Health staff members. All contacts are treated confidentially/anonymously, to the limit the law allows.
HIPAA Privacy/Information Security Rule Overview
What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services to develop regulations protecting the privacy and security of certain health information. To do this they published two rules: the HIPAA Privacy Rule and the HIPAA Security Rule.
The HIPAA Privacy rule establishes national standards to protect medical records and other personal health information. It requires safeguards to protect the privacy of personal health information (PHI) and controls use and disclosures that can be made without patient authorization. Also, it gives patients certain rights to their health information.
Confidentiality

Patients expect that their confidentiality is maintained, and this is enforced by HIPAA.

When accessing patient information, be sure you are only using the **minimum necessary** needed to complete your job functions.

Never access the records of friends or family for reasons outside of TPO purposes. Curiosity and caring are not acceptable reasons to access a patient record. If you are not the care provider for an individual, do not access their information. It is recommended you recuse yourself from patient care involving family members when possible.

Discussing or sharing patient information outside of TPO purposes is a violation of HIPAA and policy. This also includes social media. Never share any information gained through your relationship with the patient on social media. Even in the case of de-identified information, comments from your or your colleagues may lead to inadvertent identification of the individual making the post a breach of privacy.
HIPAA: What is PHI?

Protected Health Information (PHI)

Any information created or received by a covered entity, including demographic data, that relates to:

- The individual’s past, present, or future physical or mental health or condition;
- The provision of health care to the individual; or
- The past present, or future payment for the provision of health care to the individual

AND

That identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.
What are the 18 Patient Identifiers?

1. Names;

2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code.

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death.

4. Phone numbers;

5. Fax numbers;

6. Electronic mail addresses;

7. Social Security numbers;

8. Medical record numbers;

9. Health plan beneficiary numbers;

10. Account numbers;

11. Certificate/license numbers;

12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;

14. Web Universal Resource Locators (URLs);

15. Internet Protocol (IP) address numbers;

16. Biometric identifiers, including finger and voice prints;

17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code.
HIPAA allows caregivers to use information for:

- Treatment activities
- Payment activities
- Operational activities
  (known as TPO)
Self-Access

Accessing your own medical record is strictly prohibited by Spectrum Health policy. Do not, for any reason, access your own information through EpicCare Link.

If you need to access or review your own information that is maintained by Spectrum Health, follow approved release of information protocols such as contacting your provider, logging into your MyHealth account, or contacting the Health Information Management (HIM) team at Spectrum Health.
Audit and Monitoring

The Spectrum Health Privacy department monitors and audits access to the Electronic Medical Records (EMR) across the system. Issues Privacy monitors for include mistaken chart access, inappropriate chart access, and minimum necessary access to patient records. These audits show the amount of time spent in a particular record and the portions of the record that were viewed.

Through the course of your work, you may mistakenly access the wrong patient record. If this happens, back out of the record as quickly as possible and report it to your immediate supervisor or the Privacy department.
Audit and Monitoring

- Correct Chart Access
- Mistaken Chart Access
- Minimum Necessary
- Spectrum Health Policy – prohibits self and family medical record access
De-Identification Methods

Authorization

An authorization must be obtained from a patient for all uses and disclosures other than for Treatment, Payment or Operations (TPO)

* Marketing
* Research
* Uses not otherwise permitted
## HIPAA Civil Penalties

<table>
<thead>
<tr>
<th>Intent</th>
<th>Minimum Per Incident</th>
<th>Annual Cap for All Violations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know or Could Not Have Known</td>
<td>$100 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause and Not Willful Neglect</td>
<td>$1,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect, but Corrected Within 30 Days</td>
<td>$10,000 - $50,000</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Willful Neglect and Not Corrected Within 30 Days</td>
<td>$50,000</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>
Criminal Penalties

Criminal penalties for wrongful disclosure of PHI apply to both covered entities and to employees and other individuals who obtain or disclose PHI maintained by a covered entity without authorization.
The Security Rule requires we maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, we must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI we create, receive, maintain or transmit;

2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;

3. Protect against reasonably anticipated, impermissible uses or disclosures; and

4. Ensure compliance by the workforce.
Guidelines for Use of Social Media

If you are going to use social media, these recommendations may be helpful:

- It is not recommended that you share, post or otherwise publish any information, including images, that you have obtained as a result of your professional relationship with a patient.
- Do not identify patients by name or post information that may lead to identification of posting.
- Never share patient information on social media, even if it is de-identified.
- Do not share photographs/videos of patients without proper authorization.
- It is not recommended to friend or follow patients on social media sites.
- Always be thoughtful about what you post and with whom you connect.
Secure your space

Digital

**Lock up** when you leave
- Windows Key + L OR appropriate logout

Physical

Keep a **clean** desk
- Phones
- CDs & Thumb drives
- Papers

Be aware of “shoulder surfers”
Secure your space

Physical access is the quickest way for someone to get information.

- Do not leave computers / patient files unlocked (Log out with Windows Key + L OR approved department logout procedures)
- Securely store personal devices or carry them on you
- Properly store or dispose of all papers in a secure manner
- Be aware and suspicious of unknown individuals in secure areas
- Choose strong passwords, don’t share or reuse them
What you send

Check the content
- Does your document contain PHI?
- Are there hidden excel sheets?
- Is it necessary?
- Does email chain contain PHI?
- Never send sensitive information from personal emails

Where you store it
- Do not store content on unapproved cloud services
- Do not store on public network drives
Sending Securely

Sending Secure

- Double check recipient email address for spelling and accuracy
- Email sent out to the internet is insecure
- If the information is needed for a business purpose, add [Secure] to the subject line
Phishing

Phishing is...

When someone misrepresents themselves to get something from you (often in email)

• Bank and Credit Card Information
• Usernames and Email addresses
• Passwords
• Personal Information
• Medical Records

What do they want?

All data can be monetized
Phishing cont.

Criminals use:
- Simple conversations
- Malicious links
- Malicious attachments

Criminals use urgency and emotions (punishment, loss of access, etc.) to trick you into acting without thinking.
Preventative measures to avoid phishing

Phishing identifiers

- Unknown sender
- Unsolicited links or attachments
- Directing replies to a different email address
- Sense of urgency or threat

If you suspect phishing

- Do not click suspicious links
- Do not download attachments
- Do not respond or create a conversation
- Do not forward to others in your practice
- Verify sender
Links in email

Signs of a Phishing Email
- Impersonal greeting
- Fear
- Limitations/inconvenience
- Poor grammar
- Urgency
- Unsolicited link/attachment
- Punishment

Irregular Card Activity

Dear Customer,

We detected irregular card activity on your American Express Card on 1st October, 2013.

As the Primary Contact, you must verify your account activity before you can continue using your card and upon verification, we will remove any restrictions placed on your account.

To review your account as soon as possible please:

Please click on the link below to verify your information with us:

https://www.americanexpress.com/

If your account information is not updated within 24 hours then your ability to access your account will be restricted.

We appreciate your prompt attention to this important matter.

© 2013 American Express Company. All rights reserved.
What is a malicious attachment?

Documents that are attachments in phishing emails may be documents that contain macros.

These may:

- Edit system files
- Download viruses
- Install software to steal information

Do not enable macros unless you are 100% sure of who sent it.
Report phishing

If you suspect phishing

- Do not click links
- Do not download attachments
- Do not respond
- Do not forward to others in your department

Forward as attachment to spam@spectrumhealth.org

Delete the message immediately
What is Vishing?

Vishing is using live phone conversations or voice mail messaging to mislead individuals for malicious reasons. Criminals use:

- Simple conversations
- Authority, urgency and fear of loss
- Impersonating reputable individuals

If you are suspicious of the caller, direct them to your leader or gather call-back information, hang up and verify the validity of their requests before calling back.
Why would a criminal use vishing or phishing?

They want to gain access to:

- Computers
- PHI
- Leadership
- Leadership support staff
- Usernames and passwords
- Sensitive systems
- Financial information
- Medical records
- Business information
If you are assigned a portable device, or if you are authorized to use a personal device to check Spectrum Health resources such as email, you need to review the policies for these devices. Portable devices such as laptops, tablets, and smartphones are often stolen for the data they contain, so it is important to safeguard them.

To protect this data you must:

- If you back up confidential information to a USB drive, optical storage device, memory card, flash card, or CD/DVD, it must be encrypted and kept in a secure location when it is not being used.
- Do not take any media storing company electronic data off-site unless your work requires you to do so and you have permission.
- Do not leave your laptop unattended if you are outside the office.
- Install the appropriate applications (such as AirWatch) to smartphones and tablets to decrease the risk of exposure of Protected Health Information (PHI) or Personally Identifiable Information (PII).
- **Report all lost or stolen devices** (even personal ones that access SH resources) to **1-HELP** immediately (24/7) and contact the security services personnel.
  - Speak with the on-call representative at the IS Service Desk when reporting...
For any other information on use of Spectrum Health assets or access of data, see the next page for the Spectrum Health Acceptable Use Policy.
Spectrum Health Privacy Office Contacts

System Privacy Team: privacy@spectrumhealth.org
Privacy Hotline: 616-486-4113
Spectrum Health IS Service Desk:
616.391.4357 (1-HELP)

Privacy/Security Awareness Training requests or questions:
SecurityPrivacyAwarenessTraining@spectrumhealth.org