Spectrum Health®

# What we Will Cover in This Course

- ✓ Compliance Basics
- ✓ Fraud, Waste and Abuse
- ✓ Deficit Reduction Act
- ✓ False Claims Act
- ✓ Whistleblower Provisions
- ✓ Code of Excellence
- ✓ Privacy/Information Security

# Compliance Training

# What is a Compliance Program?

Simply, a compliance program safeguards the organization’s legal responsibility to abide by applicable laws and regulations.  A compliance program also helps the organization live its values and ethics.

# 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

# What does this mean at Spectrum Health?

| 7 Elements | Example of how SH meets the element |
|---|---|
| 1. Written standards of conduct/policies and procedures | Our Code of Excellence: assists us in living our values and doing the right thing.<br>Policies and procedure can be found in policy tech. |
| 2. Compliance oversight | We have Compliance Officers and Compliance Committees.  A Compliance Officer is able to meet with the President and the Board of Directors if necessary. |
| 3. Effective training and education | We empower our team to do the right thing by offering them training once a year, during onboarding and as needed to help address key risk areas. |

# What does this mean at Spectrum Health?

| 7 Elements | Example of how SH meets the element |
|---|---|
| 4. Monitoring and auditing | Team members involved in operations monitor their own work to make sure it complies with laws and regulations.  The Compliance Department audits operations and monitoring activities to also ensure compliance. |
| 5. Effective lines of communication/reporting process | We provide a third party operated reporting system, the Integrity Help line to encourage team members to report any concerns they have. |

# What does this mean at Spectrum Health?

| 7 Elements | Example of how SH meets the element |
|---|---|
| 6. Enforcement through disciplinary actions | All team members are expected to live our values and follow policies and procedures. If a team member doesn’t follow our policies or procedures, we take appropriate action to address it. |
| 7. Response and corrective action | We respond to all concerns and reports of misconduct by performing an investigation and correcting any issues found.  We continue to monitor corrective actions after the investigation to ensure the issue is properly resolved. |

# Why Have a Compliance Program?

By having a compliance program we aim 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 government health care programs. 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 will 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 implement 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 annually to provide their employees, contractors and agents training regarding the federal and state false claims laws and related qui tam/whistleblowers provisions.

# So What is the False Claims Act?

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.
- 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.

# Liabilities for Violating the False Claims Act

Health care providers who violate the FCA may be subject to civil monetary penalties ranging from $11,665 to $23,331* 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 2020, 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 15-30% 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 who is involved in:

- Reporting potential issues or concerns
- 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 report it to the Compliance Department or the Integrity Help Line at 1-877-319-0266.

# 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
- Compliance Department

You can also contact the Integrity Help Line at: 1-877-319-0266 or access it via the web at: https://spectrumhealth.alertline.com/gcs/welcome

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 team members. All contacts are treated confidentially/anonymously, to the limit the law allows.

# Privacy/Information Security Training

Spectrum Health

# What is HIPAA and the Privacy Rule?

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.

There are two rules for HIPAA:  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 (PHI).

It requires safeguards to protect the privacy of 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
18. Any other unique identifying number, characteristic, or code

It is recommended to use **at least 2 patient identifiers** to identify patients

# Permitted uses for PHI

**HIPAA allows caregivers to use information for:**

**Treatment** – any activity undertaken on behalf of the member related to their health care such as care, referrals, and orders

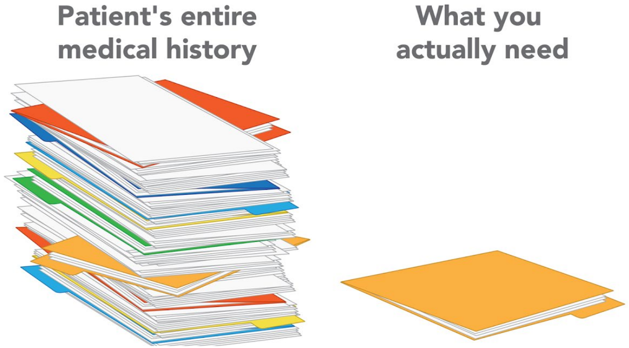
**Payment** – billing, coding, claims management, collection and related health care data processing

**Health Care Operations** – quality assessment or assurance and process improvement activities, recertification, auditing functions, OASIS/HEDIS data collection

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

# Expectations of PHI protection

- Unauthorized accessing of insurance or PHI could result  in disciplinary action, up to and including termination of employment
- **Do Not access your own medical information** if you need to access your own information follow approved release of information protocols such as contacting HIM
- Record access is audited by the Privacy team, returning information on who accessed which charts and when
- Follow Minimum Necessary Standards
- Be present minded to avoid mistakes
- Report and Mitigate all mistakes with PHI



# Auditing and Monitoring

The Privacy team utilizes advanced tools that use algorithms and machine learning to identify and report user patterns highlighting suspicious access to PHI/EMR applications including but not limited to:

**Accessing PHI of a family member, friend, co-worker or oneself**

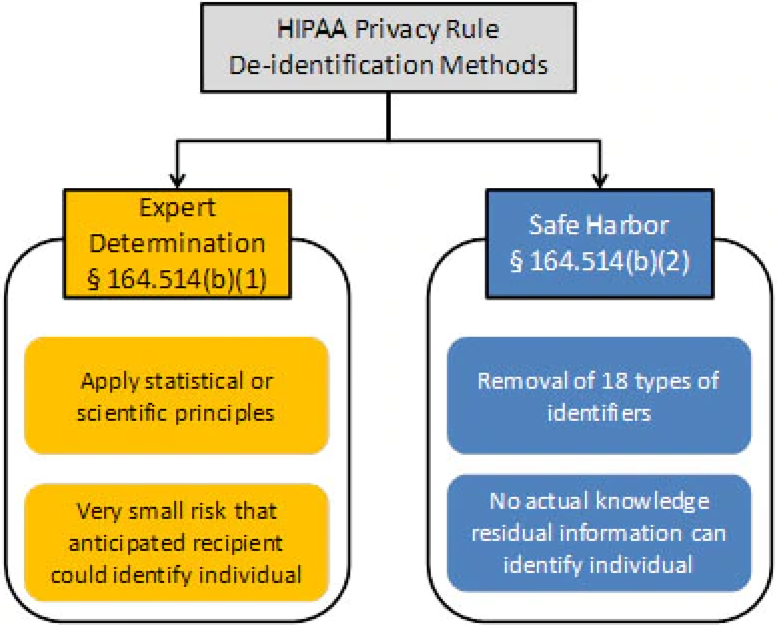
**Accessing PHI that is not customary for the job function**

**Accessing PHI outside of departmental/TPO purposes**

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.

Staff are held accountable for their actions and any access of PHI. Inappropriate access to PHI, regardless of intent, can result in corrective action, <u>up to and including termination of employment</u>.

# De-Identification Methods


HIPAA Privacy Rule
De-identification Methods
Expert Determination § 164.514(b)(1)
Apply statistical or scientific principles
Very small risk that anticipated recipient could identify individual
Safe Harbor § 164.514(b)(2)
Removal of 18 types of identifiers
No actual knowledge residual information can identify individual

You can find more guidance on de-identification methods here: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

# HIPAA Security Rule

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

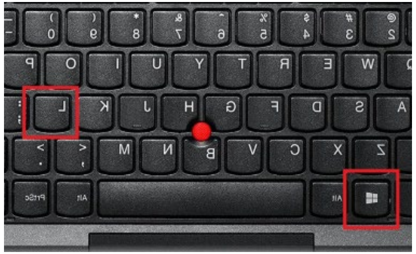
If you are going to use social media, these recommendations may be helpful:

- 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

# Secure your space

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

- Do not leave computers / patient files / sensitive data unlocked (Log out with Windows Key + L OR approved department logout procedures) **<u>even when working from home</u>**
- 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
- Create strong passwords, don't share or reuse them
- It is a violation of policy to share passwords with anyone

# Protecting Sensitive Data

## Check the content of an email

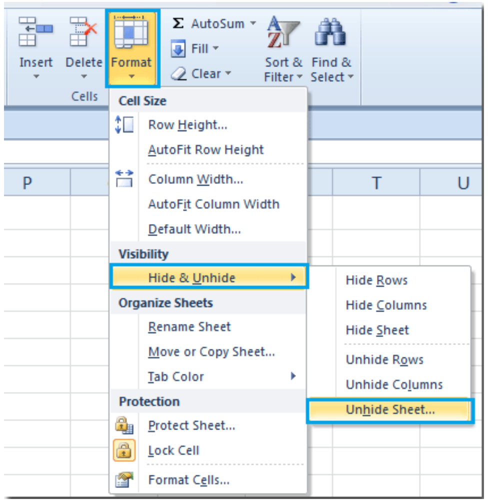
- Does your document/email chain contain PHI?
- Are there hidden excel sheets?
- Is the entire email chain necessary?

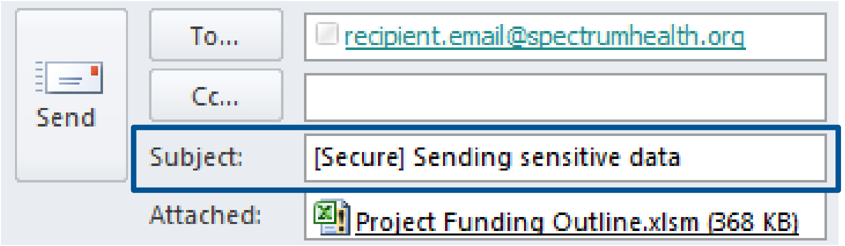
## Where to store sensitive organizational data

- Do not store sensitive data on unapproved cloud services or public network drives

## Sending secure email

- Email containing sensitive information needs to be secured
- To send an email securely, add **[Secure]** to the subject line





To... recipient.email@spectrumhealth.org

Subject: [Secure] Sending sensitive data

Attached: Project Funding Outline.xlsm (368 KB)

# Protecting company data and assets

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 business assets or data off-site unless your role requires it and you have permission
- Do not leave your laptop unattended or unsecured if you are outside the office
- Install appropriate applications to portable devices to decrease the risk of exposure of Protected Health Information (PHI) or Personally Identifiable Information (PII)

**Report all lost or stolen devices** (even personal devices with access to SH resources) to the IS Service Desk at 616.391.4357 or **1-HELP** immediately (24/7) and contact the security services personnel.

Speak with the on-call representative at the IS Service Desk when reporting

# Spectrum Health Acceptable Use Policy

For any other information on use of Spectrum Health assets or access of data please familiarize yourself with the Spectrum Health Acceptable Use Policy and its associated standards.  It can be found in Policy Tech via the InSite homepage.

# Protecting Credit Card Data

The organization handles payment card (credit or debit card) data for patients, members and employees (billing, gift shops, cafes, etc.).

To comply with the Payment Card Industry Data Security Standard (PCI DSS) this data must be protected, **to protect this data you must:**

- Inspect card readers in your area for tampering or unauthorized device substitution
- Do not record or store card numbers (Paper, Word doc, Outlook contacts)
- Do not mail, message, fax, or email card numbers
- Never give out patient/member card information
- Use only approved card entry devices

For more information, visit Information Security on InSite for the PCI Homepage

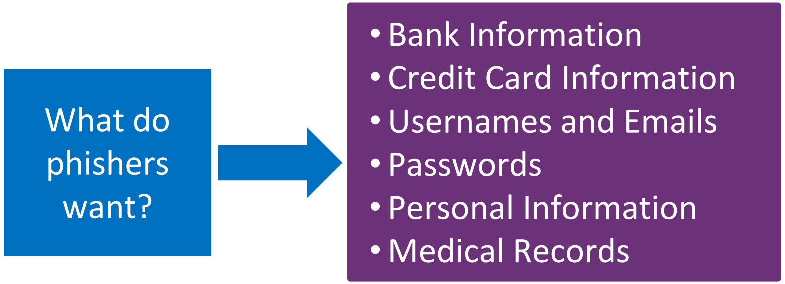
# Phishing

The term ‘phishing’ is taken from the word ‘fishing.’

Much like fishing, ‘phishing’ is when cyber criminals try to lure people into clicking a link or opening an attachment  in an email that will either download malware or steal sensitive data.

## Signs of a Phishing Email

- Impersonal greeting
- Unsolicited link/file
- Punishment/Fear/Urgency
- Poor grammar
- Promoting offers or solutions for current local, national or global issues



What do phishers want?

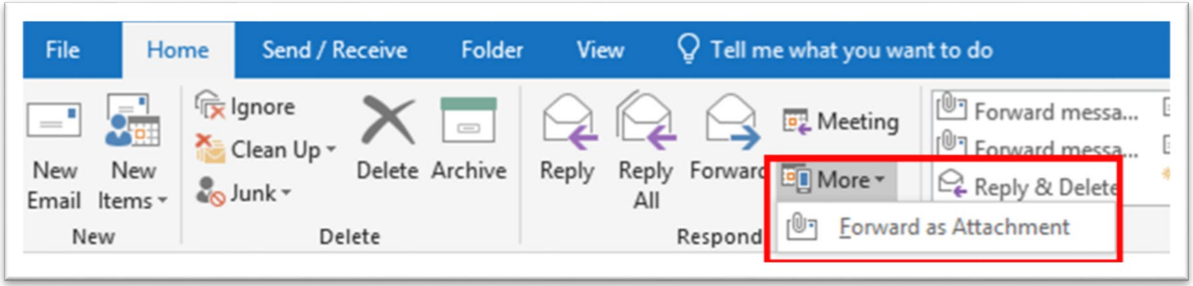
- Bank Information
- Credit Card Information
- Usernames and Emails
- Passwords
- Personal Information
- Medical Records

# 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 an attachment to spam@spectrumhealth.org and delete the message immediately.



**Reminder:** Educational simulated phishing emails are sent randomly to team members to practice identifying and reporting suspicious email. You will be notified if an email reported is educational.

# Privacy and Information Security Contacts

***System Privacy Team:*** privacy@spectrumhealth.org

***Privacy Hotline:*** 616-486-4113

***Spectrum Health IS Service Desk:*** 616.391.4357 (1-HELP)
**Information Security Team:**
securityprivacyawarenesstraining@spectrumhealth.org

®

Spectrum
Health