



Where big hearts help little patients

Corporate Compliance Program

Mandatory Vendor/Contractor Training Program

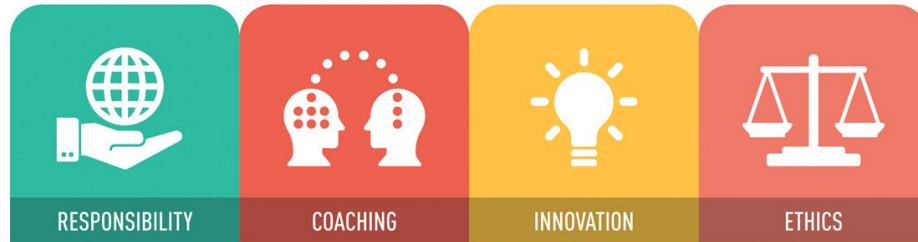
Topics that will be covered

- Introduction
- Code of Conduct
- OMIG Compliance Program Requirements
- Compliance Program Elements
- Compliance Committee
- The System's Compliance Program Overview
- Additional Overview of Compliance Program
- OMIG Program Risk Assessment
- Auditing and Monitoring
- Fraud, Waste and Abuse
- Fraud and Abuse Laws
- Exclusion Screening
- The System's Gift Policy
- Conflict of Interest
- Health Insurance Portability and Accountability Act (HIPAA) and Patient Privacy
- 18 Elements of PHI
- HIPAA Key Terms
- HIPAA and Patient Privacy
- Monitoring Data for Inappropriate Use
- Phishing Schemes
- Cyberattack in the News
- Best Practices
- Doing the Right Thing – Contact Information
- Attestation

Introduction

- Welcome to St. Mary's Healthcare System for Children's (the "System") Mandatory Compliance Training for Vendors/Contractors.
- The System is committed to foster a culture of compliance and integrity to ensure that all vendors/contractors operate at only the highest standard for ethical conduct.
- This training will also cover: Compliance Laws, Rules and Regulations that apply to the System; Stark Law; Anti-Kickback Statute and False Claims Act.
- Once you have completed this training course, please complete the attached attestation. If you are unable to access the attestation, please contact:
chutton@stmaryskids.org
- If you have any questions about this training, please contact the System's Audit and Compliance Manager, Christine Hutton at (718) 281-8587.

Code of Conduct



CODE OF CONDUCT



- Perform your duties in good faith and to the best of your abilities
- Refrain from illegal conduct
- Seek guidance from managers and compliance department when uncertain of statutes and regulations
- Disclose concerns of compliance violations
- Participate in scheduled training regarding St. Mary's compliance program
- Comply with all St. Mary's policies

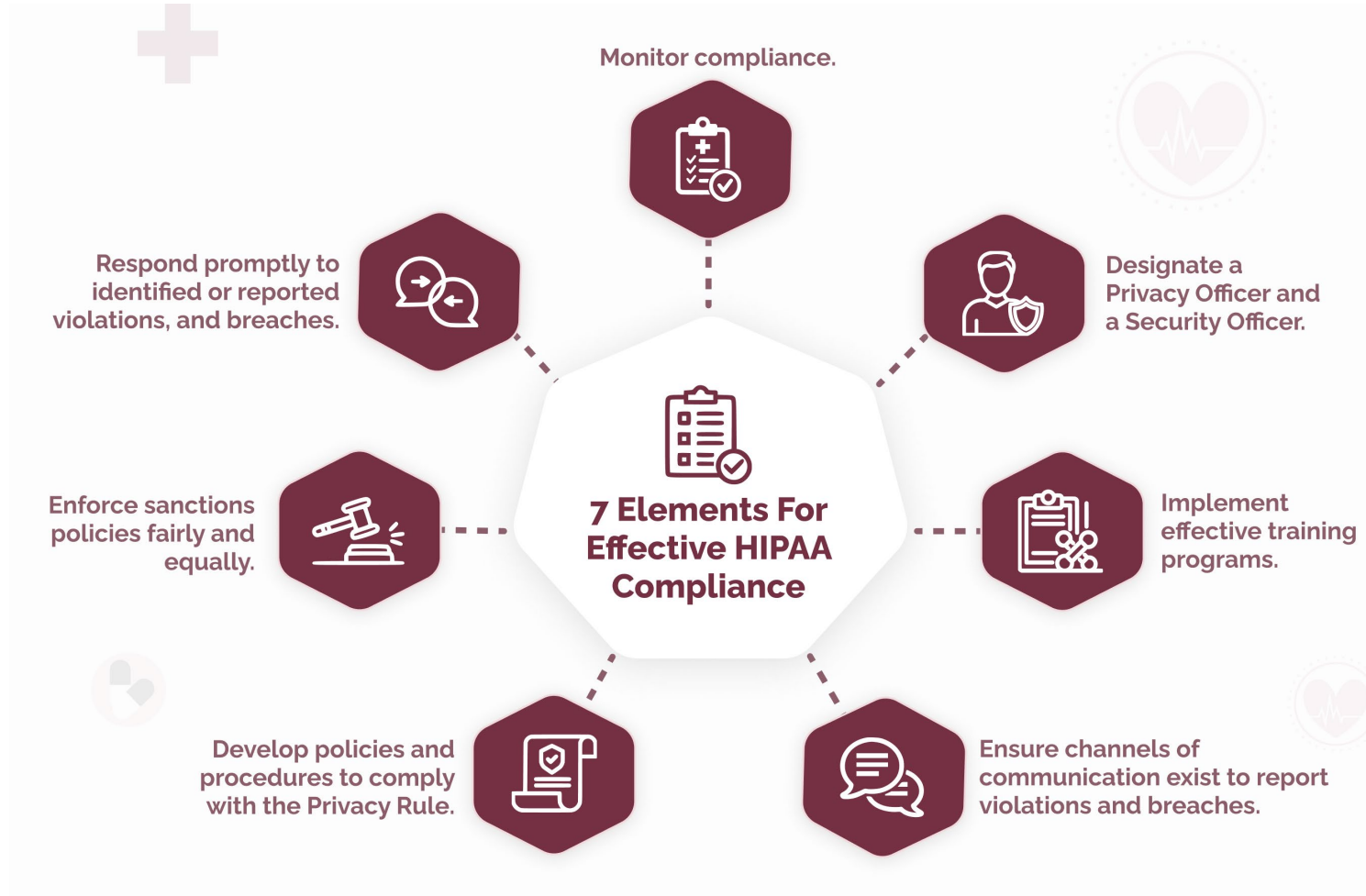
A GUIDE TO REGULATORY COMPLIANCE



OMIG Compliance Program Requirements

The New York State Office of Inspector General (OMIG) oversees the integrity of the NY Medicaid program, include ensuring healthcare providers have an effective compliance program.

Our Chief Compliance Officer (CCO) is vested with responsibility for the day-to-day activities of our compliance program. The requirements for an effective Compliance Program as defined by OMIG are shown below.



The System has designed an individual to serve as its Chief Compliance Officer (CCO), Adam Waxer. The CCO and his team have several responsibilities for the day-to-day activities of our compliance program.

The seven elements required for an effective Compliance Program as defined by OMIG are defined here.

Compliance Program Elements

Compliance Committee



In addition to the Chief Compliance Officer, the System has designated a compliance committee comprised of senior managers, which also plays an important role within the System. This committee meets on a quarterly basis.

The Compliance Committee's responsibilities include:

- Ensuring communication and cooperation by all Affected Individuals (the System's employees, chief executive and other senior administrators, managers, contractors, agents, subcontractors, independent contractors, and governing body and corporate officers) on compliance related issues, internal or external audits, or any other function or activity required by OMIG and other government agencies.
- Ensuring the System has effective systems and processes in place to identify compliance program risks, overpayments, and other issues, and effective policies and procedures for correcting and reporting such issues.
- Report directly to the System's Board of Directors Audit and Compliance Committee and the President and Chief Executive Officer.
- Coordinates with the Chief Compliance Officer to ensure that policies are accurate and complete, trainings is implemented, and audits are completed.
- Reviews the Compliance Committee charter annually

The System's Compliance Program Overview

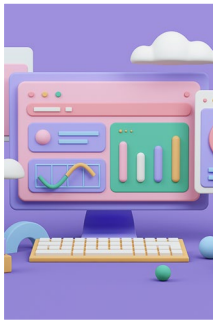
The System's Compliance Program provides an effective communication system to quickly and effectively address concerns, which includes the elements below:



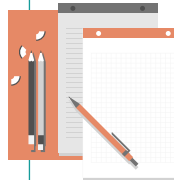
All Affected Individuals can ask questions about compliance and report fraud, waste, abuse and other compliance issues, including reporting anonymously



There is a published lines of communication available to all patients and Affected Individuals



Maintains processes to ensure that reports remain confidential as appropriate unless disclosure is required as part of a government investigation or other legal proceeding



Maintains policies that encourage good faith reporting and prohibit intimidation and retaliation.

Additional Overview of Compliance Program

- ***Disciplinary Standards:***

The System has published a system-wide disciplinary standards:

- All Individuals within the System, regardless of position, are subject to the System's disciplinary standards
- Disciplinary standards with respect to vendors may include measures up to and including reassignment of vendor personnel or suspension or termination of contract

- ***Investigation and Corrective Actions***

The System takes any compliance concerns raised seriously.

- The Compliance Department will follow up on any compliance concerns that may be identified through investigations, reports, auditing, or monitoring
- The Compliance Department, in consultation with applicable stakeholders, will determine whether corrective action is required to address compliance risk and vulnerabilities
- The Compliance Department may perform re-audits, implement new or amended policies and procedures, or implement new or enhanced monitoring process, among other things
- The Compliance Department may call on you to assist with evaluating the need for or implementing corrective actions, where appropriate

OMIG Compliance Program Risk Assessment

According to OMIG requirements, a Provider's Compliance Program shall apply to the required provider's risk areas, which are those areas of operation affect by the compliance program which are listed below:



1. Payments
2. Billing
3. Quality of Care
4. Governance
5. Contractor, Subcontractor, Independent Contractor Oversight
6. Mandatory Reporting
7. Orders Services
8. Medical Necessity
9. Credentialing
10. Other risk identified through Organizational Experience

Definitions to Understand

- **Fraud:** Intentional deception or misrepresentation that an individual **knows, or should know** to be false, which could cause a benefit to the individual or another person or company.
- **Abuse:** Practices that are inconsistent with sound fiscal, business, medical, or professional practices and which result in unnecessary costs to the medical assistance program, payment for services which were not medically necessary, or payments for services which fail to meet recognized standards for health care.
- **False Claims:** Writing untrue information on claims for payments, lying about or hiding facts, or theft of benefits or payments from the person or company who is supposed to receive them. (I.e., punching in, not providing services and then wrote a note)
- **Waste:** Useless or profitless activity; careless use of resources.
- **Risk:** Possible problems with procedures that create or suggest a hazard or possible loss.
- **Duplication of Services:** Billing for services already being provided to the patient (and billed for) when there is no unique circumstance documented in the medical record and the services are not unique and specific from one another.
- **Vendor:** Any seller, supplier, or provider of supplies or services including, but not limited to: (1) Consultant Services; (2) Therapy Services – Physical, Occupational, Speech and Respiratory
- **Whistleblower:** A person who reports possible harmful, unfair, or unjust conduct or practices to the managers of a company with the intent of stopping them

False Claims Act

- The federal and state Federal Claims Act establish liability when any person or entity receives payments from the government. **If the person or entity knowingly submits false claims to the government, then they are liable for penalties and damages for each false claim.** NY State also has a false claim act that is very similar to federal law
- Examples of False Claims:
 - Submitting bills for services not provided
 - Submitting inaccurate/false documentation to receive approval for services
 - Providing incorrect dates of service delivery
 - Billing for services provided by unlicensed providers or other misrepresentation of credentials
 - Billing for services that were not medically necessary
 - Duplicate billing for another service already being provided
 - Submitting inaccurate cost reports
- The System combats fraud, waste and abuse in many ways, including but not limited to, conducting internal audits and responding to external audits.
- If you are made aware of an actual or potential overpayment or fraud, you should immediately notify the Audit and Compliance Manager, Christine Hutton immediately at (718) 281-8587 or (888) 343-2581.

Fraud, Waste and Abuse

In most cases physicians and health care providers are honest and strive to provide high-quality care to their patients/residents.

In 2025, the United States Department of Justice collected more than \$14.6 billion dollars in False Claims against 324 defendants. The Takedown involved federal and state law enforcement agencies across the country and represents an unprecedented effort to combat healthcare fraud schemes that exploit patients and taxpayers.

In case you missed it: Top Fraud, Waste & Abuse Cases in Healthcare

A historic era for healthcare fraud takedowns, by the numbers

\$1.4B:



In June 2020, 10 people were charged in a rural hospital billing scheme targeting southern hospitals. Conspirators included hospital managers, lab owners, billers and recruiters, who billed private payers for expensive lab tests not done in-house, as stated.

\$931M:

In January 2021, five defendants pleaded guilty to a multi-year healthcare telemarketing fraud conspiracy. It involved improper solicitation of patient information, obtaining approvals from telemedicine prescribers, and selling costly prescriptions to pharmacies in exchange for kickbacks.



\$681M:

In July 2020, a years-long fraud scheme in Palm Beach, Florida was busted when the Justice Department found a doctor fraudulently billing tests and treatments for patients seeking drug or alcohol addiction help. Some patients were billed \$10,000 to \$20,000 for tests in a single day.



\$400M:

In March 2019, a Florida woman was charged with setting up hundreds of sham storefronts to sell back and knee braces to senior citizens, then providing unlawful kickbacks and fraudulent DME orders through telemedicine companies for claims reimbursement.



\$325M:

In January 2020, a Texas rheumatologist was found guilty of falsely diagnosing patients with life-long diseases and treating them with medically unnecessary and toxic medications. Some patients were as young as 13 years.



Fraud and Abuse Laws

Two important laws are:

1. Anti-Kickback Statute and
2. Stark Law



They both work to prohibit anyone from paying healthcare providers for referrals as well as prohibit healthcare providers from receiving payments for referrals. Both Anti-Kickback Statute and Stark Law are designed to prevent fraud and abuse that could harm federal healthcare programs and patients/residents.

Both laws have significant penalties for any violation, and the **Anti-Kickback Statute** can even include jail time.

It is therefore vitally important that you follow the System's policies that are designed to ensure compliance with fraud and abuse laws, especially if you work on physician employment, recruitment, or other business relationships with physician or vendor contract.

Fraud and Abuse Laws

ANTI-KICKBACK STATUTE (AKS)

- The AKS prohibits payments or other transfers of value that are intended to induce referrals
 - A relationship will violate the AKS if just one purpose is an intent to improperly induce referrals
- The AKS prohibits the System from “knowingly and willfully” offering, requesting, giving or taking any “remuneration” – basically anything of value, in exchange for healthcare businesses
- Violations of the AKS may result in significant civil and criminal penalties:
 - Forfeiture of federal healthcare program reimbursement
 - Treble damages under the False Claims Act
 - Exclusion from federal healthcare programs
 - Prison

STARK LAW

- Prohibits a physician from referring Medicare and Medicaid patients/residents for certain “designated health services” to a facility with which the physician group, physician (or an immediate family member) has a “financial relationship,” unless a specific exception is met:
 - The Stark Law allows employed physicians to make referrals to their employer so long as certain requirements are met, including that compensation does not take into account the volume or value of referrals.
 - The System is able to employ and contract with physicians if the arrangements fit within exceptions to the Stark Law.
- If a financial relationship violates the Stark Law, every single Medicare and Medicaid referral for designated health services that the physician makes to the System is impermissible.
 - The System must repay any Medicare or Medicaid reimbursement that is received for designated health services referred by the physician.
 - Additional fines and penalties are possible as well

Non-Intimidation and Non-Retaliation

- St. Mary's prohibits anyone from intimidating a workforce member who discloses a compliance concern.
- St. Mary's will immediately investigate and take appropriate action with respect to all suspected acts of retaliation or intimidation
- Any individual found to have engaged in retaliation against a workforce member will be subject to immediate action, in coordination with Departmental Leaders, up to and including termination.

Exclusion Screening

Federal law requires that we screen all Affected Individuals and referring physicians on a regular basis to ensure we do not have any excluded providers on our staff or that we contract with any excluded vendors.

Excluded providers cannot bill federal or state health care programs, either directly or indirectly. If you are excluded from participation in any federal or state health care program, you **must** immediately inform your supervisor or the Compliance Department. Failure to do so will result in severe sanctions.



Gift Policy

Gifts from healthcare industry vendors shall not obtain any improper personal benefit by virtue of their employment/relationship with the System.

All Affected Individuals shall **not**:

- Accept payment by any party other than the System for services provided by the System's entity (St. Mary's Administrative Services, St. Mary's Hospital, Extraordinary Home Care, SMH Case Management, and Extraordinary Pediatrics, PC).
- Split or share fees with a referring agency, facility, individual, or other home care services agency.
- Solicit, receive, or accept from any person or entity, nor offer or give to any person or entity, anything of material value if that person or entity can refer business to the System or if the System is able to refer business to that person or entity except as permitted by law; or
 - Accept any gift, hospitality, or entertainment in any amount from or on behalf of a patient of the System; and shall not accept from any other person any cash or cash equivalents, any gift of more than the nominal value of \$25.00 per gift or an aggregate of \$50.00 per year from any particular person or entity, or any hospitality or entertainment that because of its source or value might influence the employee's independent judgment in transactions involving the System. If any gift is received as allowed under the terms of this provision, the employee shall notify his or her immediate supervisor promptly.
- Provide any gifts or gratuities to any government or public agency representatives except as permitted by law;
- Make payments for a physician's travel to or participation in conferences unless the subject matter of the conference is of direct benefit to the System. Similarly, there shall be no payments of a physician's continuing education fees, no discounted billing services, no interest free loans, and no forgiveness of loans as part of any gift to a physician unless such benefits are specifically allowed as part of a permissible physician agreement; and
- Pay or receive anything of financial benefit in exchange for Medicare or Medicaid referrals, such as receiving non-covered medical products at no charge in exchange for ordering Medicare reimbursed products.
 - The System's staff will not give gifts and entertainment to family members, potential referral sources, and other individuals and entities with which the facility has a business relationship in more than a nominal value of \$25.00 per gift or an aggregate of \$50.00 per year.

Conflict of Interest (COI) Disclosure

As part of the System policy, Conflict of Interest and Recusal:

- Certain System's employees are required to complete a Conflict-of-Interest report in the form of a questionnaire upon beginning their employment and then on an annual basis thereafter
- In addition, the form must be updated before the team members enters into a new financial or other relationship that might create a conflict of interest or affect their ability to carry out their duties and responsibilities objectively.

Even if you are not required to fill out the Annual Conflict of Interest Form, you must disclose to the Chief Compliance Officer any situation that may create an actual or appearance of a Conflict of Interest.

Auditing and Monitoring

An important part of the System's Compliance Program is auditing and monitoring. Compliance conduct audits on risk areas, and corrective action plans are implemented based on the findings to resolve matters.

For example: Conducting annual reviews of the compliance program to determine its effectiveness, and whether any revision or corrective action is required. The Compliance Department partners with many departments across the System to ensure that we are documenting, coding, and billing appropriately and accurately. Any identified overpayments and underpayments are refunded or rebilled to ensure compliance with federal and state program requirements.





Health Insurance Portability and Accountability Act (HIPAA) and Patient Privacy

- What is HIPAA?

A set of rules enacted by the government which, among other purposes, requires the System to protect the privacy and security of patient/resident's health information.

- HIPAA applies to:

1. Covered Entities, including the System and its staff; and
2. Business Associates (vendors, contractors, independent contractors) acting on behalf of the System.

- Other Privacy and Security Regulations:

1. HIPAA/HITECH

18 Elements of Protected Health Information (PHI)

PHI comes in many forms, including oral, written and electronic. Any communication of PHI is covered by HIPAA.

PHI IDENTIFIERS

Names	Photographic Images	Vehicle Identifying Numbers
Addresses	Social Security Numbers	Device Identifying Numbers
Dates	Medical Record Numbers	Web URLs
Phone Numbers	Health Plan Numbers	IP Addresses
Fax Numbers	Account Numbers	Biometric Identifiers
Email Addresses	Certificate/License Numbers	Any Other Unique Characteristic

HIPAA KEY TERMS

- **Minimum Necessary:** As healthcare providers, we must only request, use, disclose, the **minimum necessary** information about patient in order to complete the task at hand.
- The Department of Health and Human Services (HHS) says that the Minimum Necessary Rule relies on the professionalism of medical practices, practitioners and staff to decide which information is reasonable to share.
 1. Treatment
 2. Payment
 3. Health Care Operations

The 3 Allowed Uses of PHI



Treatment

A medical provider will need to share patient information with a nurse so that they can provide proper care.



Payment

Insurance companies require certain medical information in order to provide coverage.



Health Care Operations

PHI may also be used in certain administrative, financial, or legal situations in order to run a business.

HIPAA and Patient Privacy



It is the responsibility of all Affected Individuals within the System to protect the security of our patients/residents' PHI and prevent disclosures to unauthorized individuals



Any vendor that has access to the PHI of the System patients/residents is required to sign a Business Associate Agreement which includes requirements for securely handling and storing PHI



Affected Individuals who becomes aware that PHI may have been improperly disclosed to unauthorized individuals must notify the Compliance Department immediately (718) 281-8587 or (888) 343-2581

Monitoring Data for Inappropriate Use



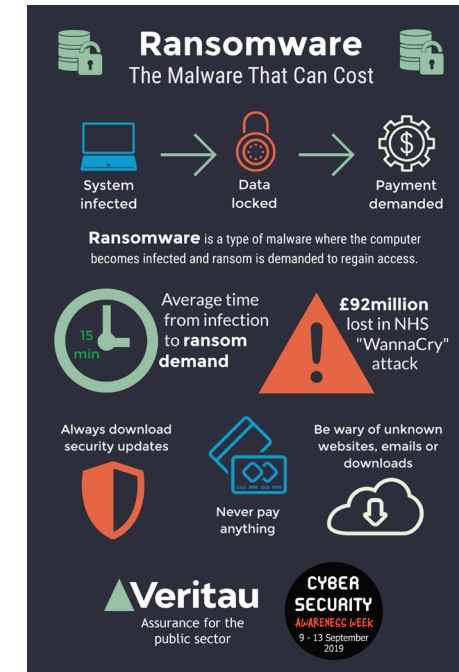
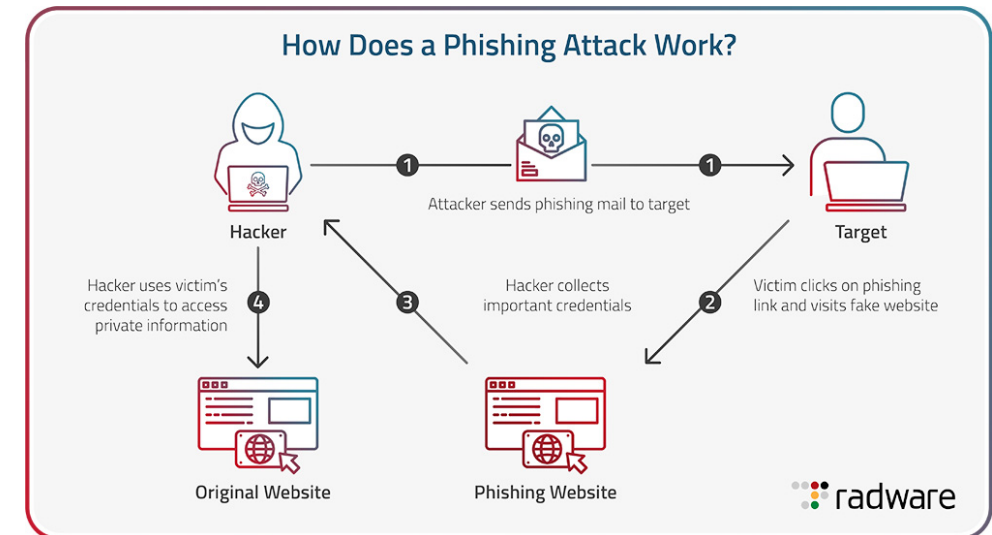
The System conducts an audit that shows all accesses of our medical record systems

The System Will Not Tolerate Mishandling of Our Data!

- Privacy Breach detection and reporting solution that collects and aggregates data 24/7
- Sends alerts to Compliance about occurrences of possible inappropriate access to medical records
- Used to conduct investigations in response to reports/concerns
- Discipline up to and including termination

Phishing Schemes – HIPAA and Patient Privacy

- Cyber attacks often use phishing schemes to gain access to corporate computer systems.
- Remember, never click on unknown links or open attachments received in an email unless you trust the sender and the content.
- Look for signs of a phishing scheme:
 - Misspelled word, grammatical errors
 - Communicate a sense of urgency
 - Covey Pressure to click a link and give out username of password
- **Ransomware:** A type of malicious software that locks files, making them unavailable until the ransom is paid



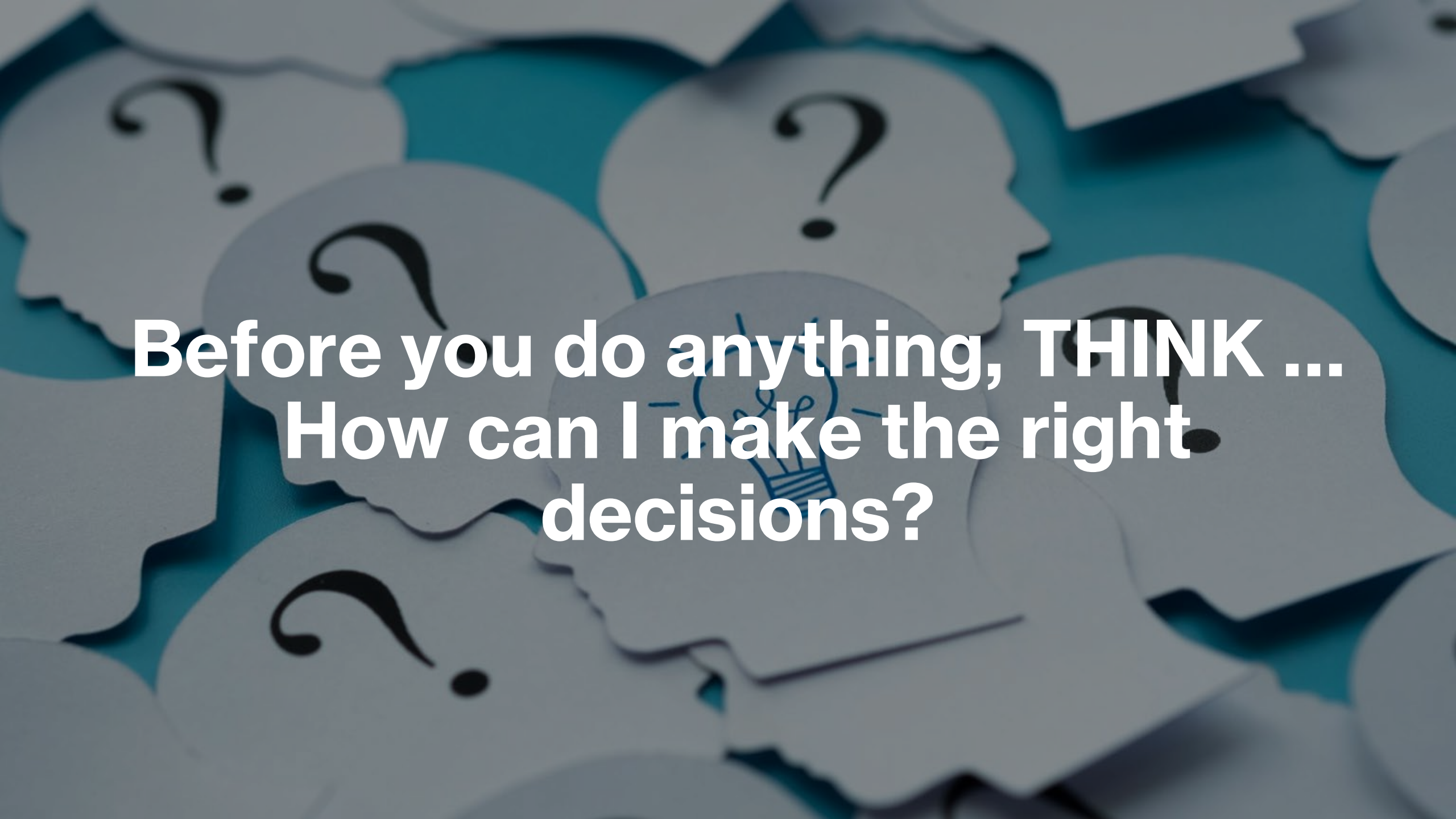


Cyberattacks in the News

- In 2022, FBI revealed that they have successfully thwarted a planned cyberattack against Boston Children's Hospital, which was attributed to the Iranian government before it could damage the hospital's IT network.
- In 2022, 2 million patients affected by Shields Health Care Group Cyberattack. Information removed from its system: Full name, Social Security Number, Date of Birth, Home address, Provider Information, Diagnosis, Billing Information, Insurance Number and information, Medical Record Number, Patient ID, and other medical or treatment information.
 - This cyberattack also affected numerous vendor hospitals
 - A \$15.35 million settlement has been agreed to resolve a consolidated class action lawsuit over the data breach.

Best Practice and Practical Advice

- Other steps you can take to help the System comply with its obligations under applicable laws and policies include:
 - Making sure any coding and billing functions are conducted accurately and in accordance with applicable laws, policies and guidance
 - Maintain accurate, legible and timely records
 - Billing only for those goods and services actually provided and medically necessary
- Safeguarding confidential, patient and other private information
- Protecting the System's business information
- Disclosing any potential or Conflict-of-Interest to the Compliance Department

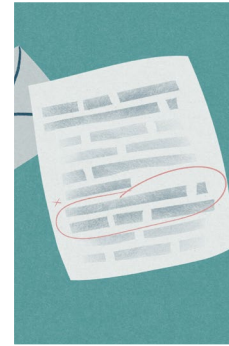
The background features a repeating pattern of light gray silhouettes of human heads in profile, facing right. Each head contains a large black question mark. The silhouettes are layered, creating a sense of depth. A small, faint blue lightbulb icon is visible within one of the central head silhouettes.

**Before you do anything, THINK ...
How can I make the right
decisions?**

Ask yourself these questions



Is it Legal?



Does it comply with the System's Code of Conduct?



Is it in the best interests of our patients/residents and St. Mary's Healthcare System for Children?



Would you be comfortable if the decision put you on the front page of a newspaper?

Does something not feel right?

Who can help me

PROMPTLY REPORT ANY SUSPICIOUS VIOLATION:

YOUR SUPERVISOR



CHRISTINE HUTTON, AUDIT AND COMPLIANCE MANAGER/HIPAA PRIVACY OFFICER

718-281-8587 • chutton@stmaryskids.org

STEVEN POLINSKY, HIPAA SECURITY OFFICER

718-281-8745 • spolinsky@stmaryskids.org

ADAM WAXER, CHIEF LEGAL OFFICER AND CHIEF COMPLIANCE OFFICER

718-281-8585 • awaxer@stmaryskids.org

COMPLIANCE HOTLINE OR SCAN THE QR CODE

(888) 343-2581 • <https://www.integrity-helpline.com/stmaryskids.jsp>

Reporting Obligations:

It is the duty of All Affected Individuals (Employees, Executive/Senior Administration, Managers, Governing Body, Contractors, Agents, Subcontractors and Independent Contractor) affiliated with the System to comply fully with all governing laws, regulations, System's policies and procedures and the Code. Everyone must offer their complete cooperation with any investigation by the System and/or governing authorities.

You are required to report to the Compliance Department or the Compliance Hotline any actual or suspected violation of the Code, the System's policies and procedures. And/or federal or state laws. You **must** report any other compliance related issues, including but not limited to:

- Conflict of Interest,
- Patient/Resident Privacy and Security,
- Fraud or other misconduct of any type relating to the System's operations.

If I report any issues or participate in an investigation as a witness, can I be retaliated or intimidated against?

Answer: No. St. Mary's Healthcare System for Children does **not** permit **intimidation** and/or **retaliation** against anyone for good faith and honest participation in an internal or external investigation.

If you saw it...
please report it.



ST. MARY'S COMPLIANCE PROGRAM

THANK YOU!

- Thank you for taking the time to complete this training course
- Please be sure to complete the return the vendor training attestation to St. Mary's Healthcare System for Children's Compliance Department, by clicking on the link below.

[Vendor Attestation – St. Mary's Healthcare System for Children Compliance Program –
Fill out form](#)

- If you have any questions about anything that was discussed in this training, you may contact the Compliance Department at (718) 281-8587