



ANNUAL SAFETY AND COMPLIANCE 2026

Regulatory Compliance



REGULATORY COMPLIANCE

Upon completion of the business compliance training, you will understand:

- Identity Theft Prevention Program
- The Emergency Medical Treatment & Labor Act (EMTALA)
- Accurate Documentation
- Physician Referrals and The Law
- Exclusion Checking
- Government Inquiries and Whistleblower Protection
- Fraud, Waste, and Abuse



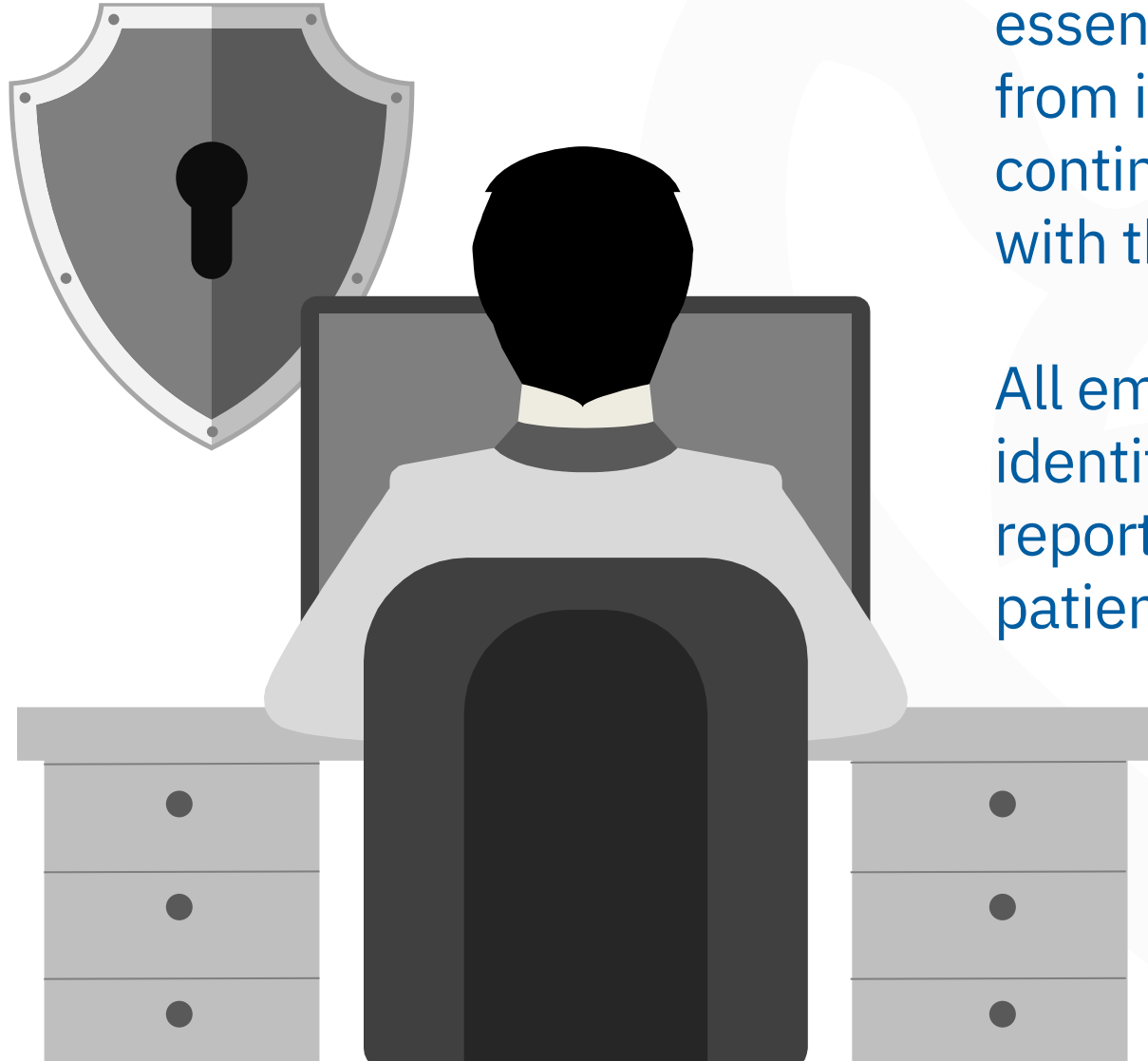
IDENTITY THEFT PREVENTION PROGRAM

Why Identity Theft Prevention Matters: protecting MHS, our patients and our reputation.

- Identity theft can destroy trust and cost millions
- Healthcare data is a 'prime target' for criminals
- A proactive Identity Theft Prevention Program means we have compliance, credibility and control
- No protection means risk to our organization



IDENTITY THEFT PREVENTION PROGRAM



Appropriate identification of patients is essential, not only for the protection of patients from identity theft, but also to support the continuum of care for subsequent encounters with the same patient.

All employees play a part in preventing patient identity theft by identifying, recording, and reporting any red flags that would suggest a patient's identity is being stolen.



IDENTITY THEFT PREVENTION PROGRAM

Red flags are patterns, practices, or specific activities that indicate the possible existence of Identity Theft. **Early Detection = Prevention**



Identification documents that appear to have been altered or forged or that are not consistent with the appearance of the person presenting the ID



The name or SSN provided by the person is known by MHS to be the same as another person



Personally identifiable information is provided which is known to be fictitious



A complaint or question is received from a patient that they received a bill for another person for a service that they deny receiving



A patient or insurance company reports that coverage for legitimate MHS stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached



A practitioner's review of medical history with the patient reveals that information in the record is inconsistent with the patient's stated history and may reflect that someone other than the patient has been treated under their identity



IDENTITY THEFT PREVENTION PROGRAM

If you identify a red flag while interacting with a patient, during treatment, or while working with a patient's medical records, you should make a note of the red flag and report it to your supervisor or the Compliance Department for further investigation and record keeping.

The Compliance department will investigate any red flags and take steps to prevent or mitigate the identity theft. You may face civil or criminal penalties for failure to report red flags that you identify.





Emergency Medical Treatment and Labor Act (EMTALA)

MHS complies with the EMTALA in providing emergency medical treatment to all MHS hospital patients, regardless of ability to pay or type of payment.

Medical Screening Exam

MHS hospitals provide a medical screening exam by qualified medical personnel within their capacity to all individuals who come to our hospitals for emergency treatment. MHS does not delay treatment to ask about insurance benefits or financial information.

Transfers

Patients are only transferred to another facility if MHS cannot meet their medical needs and appropriate care is available elsewhere. Patients may only be transferred after they have been stabilized and are formally accepted by another facility. Such patients are transferred by an appropriate mode of transportation after an explanation of risks and benefits of transfer.



ACCURATE DOCUMENTATION

Medical Records: Do It Right

Accurate Medical Record Documentation: Strong Records = Strong Defense

- Accurate, timely, and complete documentation
- Retention policies that meet legal and payer requirements
- Protect against identity theft, audits, and liability

Medical records must be maintained for every person evaluated or treated at any clinic or facility. All medical records must be legible, accurate and written timely, and should contain sufficient documentation to support the medical necessity of the services provided.



ACCURATE DOCUMENTATION

MHS takes great care to ensure that all coding and billing is accurate and in compliance with all federal and state laws and regulations.

MHS prohibits any employee or agent of MHS from submitting any claim for payment that they know is false or fraudulent. Deliberate misstatements to government agencies or other third-party payers will expose the employee to potential criminal penalties and disciplinary action.

Code What You Do—Bill What's Right

Follow ICD, CPT, and HCPCS coding and billing standards

- No guesswork. No “close enough.”
- Avoid intentional miscodes to inflate payments

If you have any questions or wish to report any improper billing or coding, you should contact your supervisor, the Chief Compliance Officer, or the Compliance Hotline.



PHYSICIAN REFERRALS AND THE LAW

Physician Referral Law

Referrals Should Be Based on Care—Not Cash

- Stark Law: No self-referrals for designated health services
- Anti-Kickback Statute: No rewards for patient referrals
- Violations = fines, jail time, exclusion from federal programs
- Transparency is not optional—it's required

All employees, affiliated physicians, and agents of MHS who know of or suspect issues of **non-compliance** with the Anti-Kickback Statute and Stark Law (Physician Referrals) policy and procedure have an affirmative obligation to report such issues.



EXCLUSION CHECKING

Exclusion Checking: Protecting the System. Exclusion checking ensures we don't employ or contract with individuals or entities barred from participating in federally funded healthcare programs (like Medicare or Medicaid).

What you need to know:

- Everyone working in the healthcare space is subject to exclusion screening
- Regular checks must be done using databases like the Office of Inspector General (OIG) or System for Award Management (SAM) lists
- If someone is found on these lists, they cannot work in positions involving federal healthcare funds

This protects our organization from penalties and protects patients from potential harm.



EXCLUSION CHECKING

Why Someone Might Be Excluded: Protecting the System

Exclusion checking protects patients and the healthcare system from individuals who have demonstrated unethical, dangerous, or fraudulent behavior. That's why regular OIG checks are critical.

Example:

Medicaid Fraud

Imagine a doctor who repeatedly bills Medicaid for services that were never provided, such as:

- Charging for patient visits that never happened
- Submitting claims for expensive procedure that were never performed
- Falsifying records to get higher reimbursements



EXCLUSION CHECKING

If caught, the OIG may:

- Investigate and confirm the fraud
- Impose civil monetary penalties or criminal charges
- Exclude the doctor from participating in any federal healthcare program

Hiring or contracting with someone on the OIG list, even unknowingly, can result in:

- Heavy fines for our organization
- Loss of Program funding
- Risk to patient safety and trust



Government is Watching!

Government Inquiries and Investigations: **Investigations Are Real.**

- Department of Justice (DOJ), Office of Inspector General (OIG), and Centers for Medicare & Medicaid Services (CMS) are actively investigating fraud
- Whistleblower lawsuits and audits are on the rise
- Ignorance is not a defense—compliance is your armor



GOVERNMENT INQUIRIES & WHISTLEBLOWER PROTECT

We cooperate with government inquiries as well as internal and external audits and investigations. When receiving non-routine requests, you should consult with the Legal and Compliance Department to ensure that requests are handled properly.

We are truthful in what we say. We never alter or destroy records in violation of the law.



Whistleblower Protection

Whistleblower is a person who exposes information or activity that's deemed illegal, is dishonest, or violates professional or clinical standards.

- False Claims Act protect whistleblowers from retaliation
- Compliance culture means report, protect, and resolve
- Your voice matters and the law backs you up



False Claims Act protects Whistleblowers from retaliation.

Protected: A person who reports false claims or brings legal action to recover money paid for false claims is protected from retaliation.

Rewarded: A person who brings a successful whistleblower lawsuit gets at least 15% but not more than 30% of the money the government collects.





Fraud, Waste & Abuse (FWA)

Fraud, Waste, and Abuse



Fraud

Knowingly and willfully executing, or attempting to execute, a scheme to defraud any health care benefit program, or to obtain any of the money or property owned by any health care benefit program.



Waste

Practices that, directly or indirectly, result in unnecessary costs to the Medicare Program, such as overusing services.



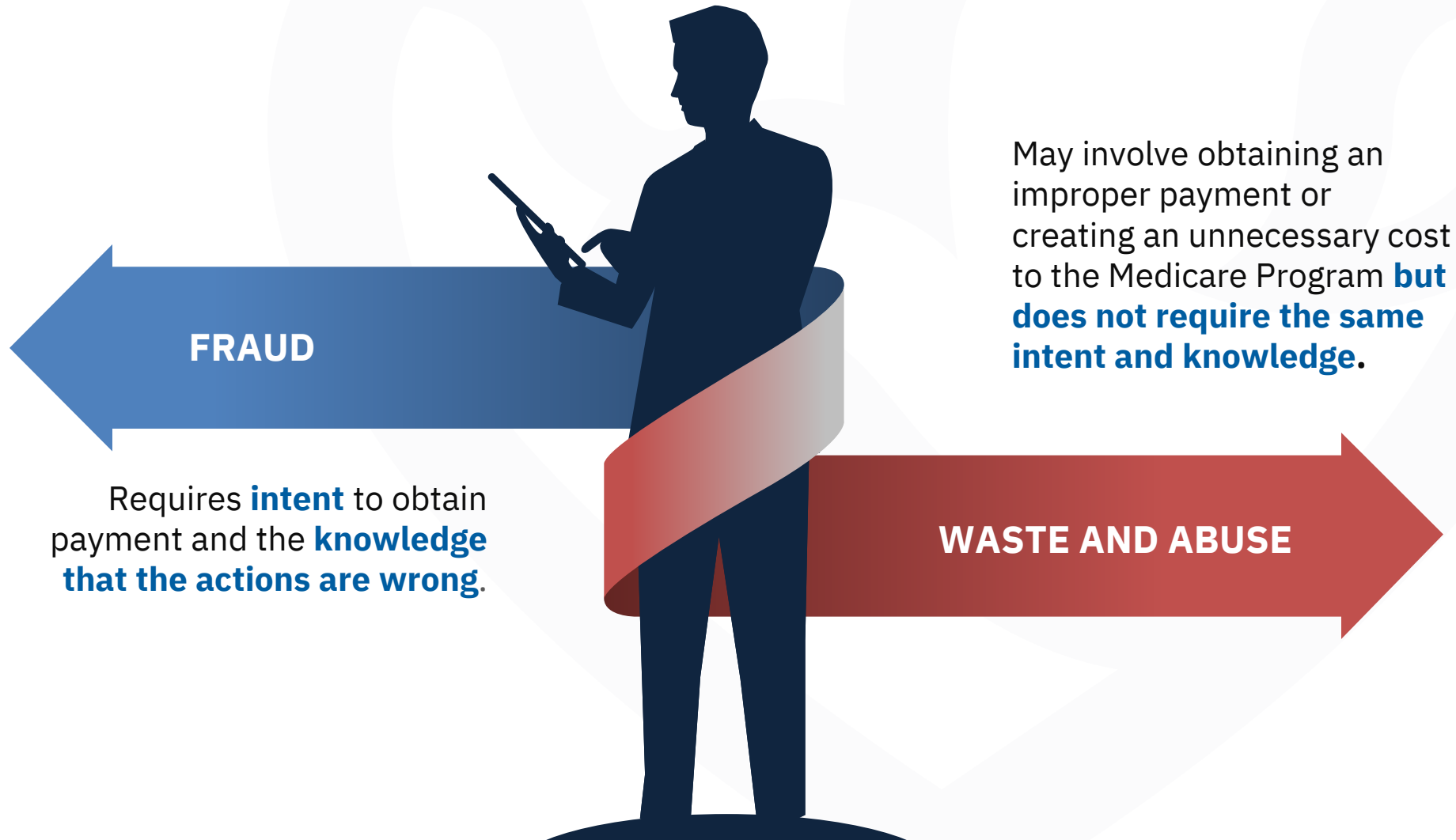
Abuse

Actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse involves payment for items or services when there is no legal entitlement to that payment.



Fraud, Waste & Abuse (FWA)

There are differences among fraud, waste, and abuse. One of the primary differences is **intent** and **knowledge**.





Fraud, Waste & Abuse (FWA)

Examples of **Fraud**:

- Any dishonest action conducted with the intent to deceive
- Forgery or improper alteration of any report and/or its supporting documentation
- Authorizing or receiving payment for hours not worked
- Improper write-off of an account of a relative or friend
- Impropriety in the handling or reporting of money or financial transactions



Fraud, Waste & Abuse (FWA)

Examples of **Fraud**:

- Accepting or seeking anything of material value from vendors or persons providing services/materials to the company [exception: personal individual gifts with a total estimated value of \$75 and consumable (food) gifts given to a department or group on an occasional basis are not subject to any limits]
- Authorizing or receiving payments for goods not received or services not performed
- Failing to disclose a potential conflict of interest situation
- Billing Medicare for appointments that patients don't keep



Fraud, Waste & Abuse (FWA)

Examples of **Waste**:

- Ordering excessive laboratory tests
- Not taking advantage of available vendor prompt payment discounts
- Conducting excessive office visits or writing excessive prescriptions
- Prescribing more medication than necessary for treating a specific condition



Fraud, Waste & Abuse (FWA)

Examples of **Abuse**:

- Unknowingly charging excessively for services or supplies
- Using MHS equipment or supplies to conduct personal business
- Using non-confidential information to get new customer(s) for own outside business
- Billing unnecessary medical services
- Misusing codes on claims, like upcoding or unbundling codes



PREVENTING FRAUD, WASTE AND ABUSE

How to **Prevent** Fraud, Waste and Abuse (FWA)

- Look for suspicious activity
- Conduct yourself in an ethical manner
- Ensure accurate and timely data/billing
- Ensure you coordinate with other payers
- Know FWA policies and procedures, standards of conduct, laws, regulations, and CMS guidance
- Verify all received information
- Act in accordance with the Code of Conduct



REPORTING FRAUD, WASTE AND ABUSE

Reporting

The False Claims Act is a federal law that allows a civil lawsuit to be brought against a healthcare provider who does any of the following:



Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval to the government or a government agency

Knowingly conceals or retains an over-payment made by the government or a government agency

Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim

Conspires to defraud the government by getting a false or fraudulent claim allowed or paid



REPORTING FRAUD, WASTE AND ABUSE

Nebraska and Iowa each have a state-specific false claims act and additional whistleblower protections. **MHP will not retaliate against you if you inform MHP or the federal government of a possible false claims act violation.**

Nebraska law prohibits employers from discriminating against employees who oppose any practice or refuse to carry out any action unlawful under federal or state law.

Iowa law protects whistleblowers who in good faith report fraud. Iowa Code requires that the Department of Inspections and Appeals keep all information confidential unless necessary for the proceedings of the case.



REPORTING FRAUD, WASTE AND ABUSE

See Something? Say Something.

Reporting Compliance Issues, including suspected instances of Fraud, Waste and Abuse:

- Follow your Companies Compliance Notification Policy.
- Contact your supervisor or manager

You're not required to report a possible false claims action violation to Company first. You may report directly to the federal Department of Justice by phone at (202) 514-2000 or by email at AskDOJ@usdoj.gov.



REPORTING FRAUD, WASTE AND ABUSE

Reporting FWA **Outside MHP:**

If warranted, Sponsors and First Tier, Downstream & Related Entities (FDRs) must report potentially fraudulent conduct to government authorities, such as the Office of Inspector General, the Department of Justice, or CMS.

Individuals or entities who wish to voluntarily disclose self-discovered potential fraud to OIG may do so under the Self-Disclosure Protocol (SDP).

Self-disclosure gives providers the opportunity to avoid the costs and disruptions associated with a government directed investigation and civil or administrative litigation.



REPORTING FRAUD, WASTE AND ABUSE

Reporting FWA **Outside Company:**

HHS Office of Inspector General:

Phone: 1-800-HHS-TIPS (1-800-447-8477)

TTY 1-800-377-4950

Fax: 1-800-223-8164

Email: HHSTips@oig.hhs.gov

Online: <https://oig.hhs.gov/fraud/report-fraud/>

Medicare website:

<https://www.medicare.gov/basics/reporting-medicare-fraud-and-abuse>



CORRECTING FRAUD, WASTE AND ABUSE

Corrective Action Plan

Once fraud, waste, or abuse has been detected, Compliance will promptly correct it. A corrective action plan will be developed to correct the underlying issue that results in FWA program violations and prevent future noncompliance. Corrective actions may include:

- Adopting new prepayment edits or document review requirements
- Conducting mandated training
- Providing educational materials
- Revising policies and procedures
- Warning letters, disciplinary action(s)
- Termination



CORRECTING FRAUD, WASTE AND ABUSE

FWA Responsibilities

All employees play a vital part in preventing, detecting, and reporting potential FWA, as well as Medicare non-compliance.

FIRST

You must comply with all applicable statutory, regulatory, and other Medicare Part C or Part D requirements, including adopting and using an effective compliance program.

SECOND

You have a duty to the Medicare Program to report any compliance concerns and suspected or actual violations of which you may be aware.

THIRD

You have a duty to follow the MHS Code of Conduct that articulates your and the organization's commitment to standards of conduct and ethical rules of behavior.





MHS CULTURE OF COMPLIANCE

MHS Culture of Compliance

- Stay alert to red flags
- Know the rules, follow the laws
- Protect patient data and billing integrity
- When in doubt, ask, report, act
- We don't just follow the rules we lead with them



ANNUAL SAFETY AND COMPLIANCE 2026

HIPAA Privacy and Information Security



HIPAA PRIVACY AND INFORMATION SECURITY

Upon completion of the HIPAA privacy and IT security training, you will understand:

- HIPAA and various regulations that apply to your job
- The significance of incident reporting and the potential sanctions associated with breaches
- The safety and security protocols in place to adhere to HIPAA
- How PHI is used and disclosed at Methodist
- Secure texting and email
- Identifying and reporting phishing email
- Managing secure passwords
- Protecting mobile devices
- Securing your data and devices
- Handling removable media
- Remote user best practices
- Acceptable use
- Malware
- Use of Artificial Intelligence Systems



HIPAA PRIVACY AND INFORMATION SECURITY

Health Insurance Portability and Accountability ACT (HIPAA) Privacy

Privacy programs manage risks to individuals associated with data processing throughout the information lifecycle, ensuring compliance with privacy requirements.



We will also discuss:



The Privacy Rule, which sets national standards for the use and disclosure of PHI

01



The Security Rule, which specifies safeguards that covered entities and their business associates must use to protect the confidentiality, integrity, and availability of electronic protected health information (e-PHI)

02



The Breach Notification Rule, which requires covered entities to notify affected individuals, the department of Health and Human Services, and, in some cases, the media of a breach of unsecured PHI

03

We will also discuss:



The Omnibus Rule,
Ensure business
associates are aware of
HIPAA safeguards

04



The Enforcement Rule,
focuses on how HIPAA rules
are applied to enforce
investigations of potential
violations and
enforcing penalties

05



HIPAA PRIVACY AND INFORMATION SECURITY

The Privacy Officer serves as the first point of contact for all issues related to HIPAA privacy and security at Methodist Health System. The Privacy Officer supports employees and patients by:

- Providing guidance on HIPAA requirements and privacy questions
- Helping to resolve questions or concerns about how health system information is shared
- Assisting teams with preventing privacy issues before they occur
- Supporting a culture of respect, confidentiality and safety
- Responding to privacy-related questions from patients and staff



HIPAA PRIVACY AND INFORMATION SECURITY

The **Privacy Officer** is the first point of contact for employees when privacy issues arise and supports teams by:

- Leading responses to suspected data breaches and privacy concerns
- Working closely with Information Security regarding data security issues



HIPAA PRIVACY AND INFORMATION SECURITY

The Health Insurance Portability and Accountability Act, Security, and Breach Notification Rule and the associated Privacy and Security Regulations, apply to almost every organization or person that provides or pays for health services or exchanges health-related information, including:

- Physicians
- Nurses
- Health care facilities (and people who work there)
- Health Plans
- Any other organization/person that handles PHI
- Business associates (any company that has access to, or uses, PHI in order to perform a service for a doctor, nurse, hospital, or other covered entity)



HIPAA PRIVACY AND INFORMATION SECURITY

The rules protect the privacy, security, and individuals' rights to their health information. HIPAA establishes standards for covered entities and their business associates to safeguard the Protected Health Information (PHI) of patients.

Failure to abide by HIPAA rules and regulations can lead to increased healthcare costs, civil monetary penalties, lawsuits, and disciplinary action.

Protecting privacy shows respect for patients and ensures their trust in the health system.



HIPAA PRIVACY AND INFORMATION SECURITY

The **Privacy Rule** protects PHI held or transmitted by a covered entity or its business associates, in any form, whether electronic, paper, or verbal.

Records containing PHI need to be secured so they are not readily available to those who do not need to see them. Records are to be accessed on a “need to know basis” or within one’s job scope.





HIPAA PRIVACY AND INFORMATION SECURITY

Protected Health Information Includes:



**Common identifiers,
such as name,
address, birth date,
and Social Security
Number**



**Information about
past, present, or
future physical or
mental health or
conditions**



**Information about
the provision of
health care to the
individual**



**Information about
the past, present, or
future payment for
the provision of
health care**



HIPAA PRIVACY AND INFORMATION SECURITY

The Privacy Rule distinguishes between the use or disclosure of PHI:

Use

- When PHI is used internally for Treatment, Payment, or other Healthcare Operations (audits, training, customer service, internal analysis, etc.)

Disclosure

- To release or provide access to a patient's PHI to someone like a physician, an attorney, insurance company, etc., outside of Methodist Health System



HIPAA PRIVACY AND INFORMATION SECURITY

There are 18 specific identifiers that must be removed from any information set for the information to be considered de-identified:

1. Names
2. Any dates (except years) that are directly related to the individual
3. Fax numbers
4. Social security
5. Address
6. Telephone numbers
7. Email addresses
8. Medical record numbers
9. Health Plan beneficiary numbers
10. Certificate/license numbers
11. Device identifiers and serial numbers
12. Internet protocol (IP) address numbers
13. Account numbers
14. Vehicle identifiers and serial numbers, including license plate numbers
15. Web universal resource locators (URLS's)
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other characteristic that could uniquely identify the individual



HIPAA PRIVACY AND INFORMATION SECURITY

Confidentiality is the safekeeping of information by individuals who have a need, reason and permission to access such information. The MHS Confidentiality Policy states:

- Employees with access to confidential patient, employee, and/or proprietary information have a duty to maintain the confidentiality of all information obtained during employment and after employment
- This includes patient medical, personal, and financial information
- Local, state, and federal laws protect the confidentiality of such information, and employees will be personally liable for any breach of this duty





HIPAA PRIVACY AND INFORMATION SECURITY

Confidentiality is the safekeeping of information by individuals who have a need, reason and permission to access such information. The MHS Confidentiality Policy states:

- Releasing confidential information without permission may result in disciplinary action, suspension, and/or termination - employees are accountable for their actions on and off duty
- You must maintain the confidentiality of patient health information even if you are no longer employed with MHS





HIPAA PRIVACY AND INFORMATION SECURITY

Protecting Patient Confidentiality Includes:

Notifying your supervisor if someone requests to have a patient's chart duplicated

Only discussing patient information in areas where other patients, visitors, and employees cannot overhear

Releasing verbal and/or written information only with proper or written consent

Directing reporters/news media to Methodist Marketing/Public Relations, if they are requesting information about a patient



HIPAA PRIVACY AND INFORMATION SECURITY

Notice of Privacy Practices

The Notice of Privacy Practices is displayed in a prominent location and made available to all patients to help patients understand their rights under HIPAA.

The Notice of Privacy Practices informs the patients of:



**MHS's pledge to
keep their
information private**



**How information
about them may be
used or disclosed**



**Options if they feel
their rights have
been violated**



HIPAA PRIVACY AND INFORMATION SECURITY

HIPAA Privacy Rule

Under HIPAA, patients have a right to:



Right to receive a copy of the Notice of Privacy Practices (NPP), even if they have previously received it electronically



Right to inspect records and receive a copy of their medical records, including an electronic copy of their electronic medical records



Right to request a correction or amendment if they believe their medical record is inaccurate



Right to request an alternative means of communication or choose how PHI is received



HIPAA PRIVACY AND INFORMATION SECURITY

HIPAA Privacy Rule

Under HIPAA, patients have a right to:



Right to opt-out of the facility directory if an inpatient



Right to request a restriction on the use or disclosure of PHI



Right to receive an Accounting of Disclosures - Patients can request a list of all parties to whom we have released PHI



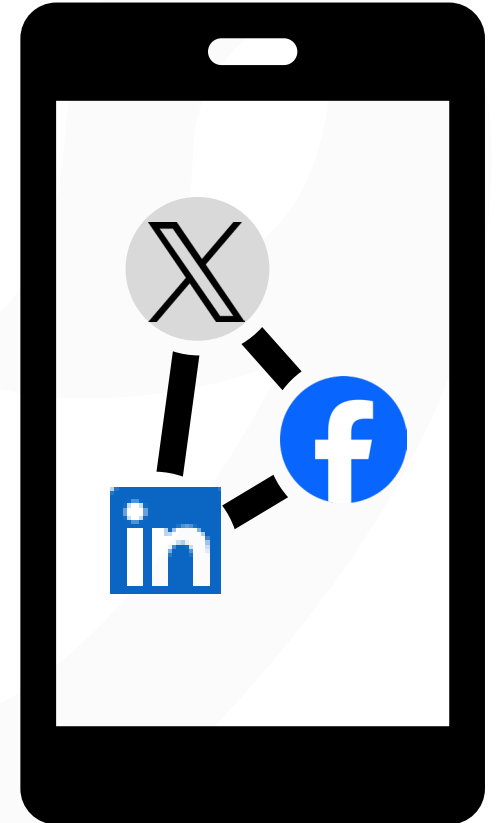
Right to file a complaint without fear of discrimination or retaliation



HIPAA PRIVACY AND INFORMATION SECURITY

Social Media/HIPAA Privacy

HIPAA prohibits the use and disclosure of protected health information (PHI) on social media. This means healthcare professionals must be extremely cautious about what they share. Disclosing PHI without consent is a HIPAA violation. This includes names, photos and any information that could identify a patient or their medical condition. Inappropriate posts can seriously damage Methodist Health System's reputation.





HIPAA PRIVACY AND INFORMATION SECURITY

Examples of HIPAA violations on social media:

- Discussing patient cases on personal social media accounts, even in a general way
- Failing to obtain proper authorization before posting patient testimonials or stories – MHS Marketing Department will help you share your testimonials in a HIPAA compliant manner
- Posting a fun photo of yourself and a coworker from your workplace without discretion could unintentionally capture a patient, a family member, or sensitive patient information in the background
- Friending patients on social media and engaging in medical discussions with patients
- Commenting on a patient's health status or treatment, even if initiated by the patient
- Sharing information that could indirectly identify a patient, such as their room number or diagnosis



HIPAA PRIVACY AND INFORMATION SECURITY

Searching for patients on social media is not automatically a breach of ethics; however, concerns arise when healthcare professionals utilize information obtained from these searches to influence patient care decisions or share details with others without the patient's consent. Always prioritize providing patient care based on the information shared by patients while they are in your care.



HIPAA PRIVACY AND INFORMATION SECURITY

Example – Cadia Healthcare

What Happened:

Cadia Healthcare Facilities had impermissibly disclosed a patient's name, photograph and information pertaining to the patient's conditions, treatment, and recovery in the form of a "success story" posted to Cadia Health Facilities' website. OCR's investigation confirmed that Cadia Healthcare Facilities had posted the patient's PHI to its public facing website without first obtaining a valid, written HIPAA authorization from the patient. OCR's investigation also determined that Cadia Healthcare Facilities disclosed PHI of 150 patients to its website through its "success story" program without first obtaining valid, written HIPAA authorizations.



HIPAA PRIVACY AND INFORMATION SECURITY

Example – Cadia Healthcare

Consequences of HIPAA violations

On September 30, 2025, the U.S. Department of Health and Human Services (HHA), Office for Civil Rights (OCR) announced a settlement with five health care providers, collectively known as Cadia Healthcare Facilities, for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Breach Notification Rule. The Cadia Healthcare Facilities are rehabilitation, skilled nursing, and long-term care services providers located in Delaware.

HHS Corrective Action Plan

Cadia Healthcare Facilities agreed to implement a corrective action plan that will be monitored by OCR for two years and paid **\$182,000** to OCR.



HIPAA PRIVACY AND INFORMATION SECURITY

Consequences of HIPAA violations

- Fines and penalties for the healthcare organizations and potentially for individuals involved
- Loss of reputation and public trust
- Violation of the social media policy may result in disciplinary action, which may include suspension, restriction of access, or termination of employment

All employees are expected to conduct themselves in a manner that reflects integrity, as well as shows respect and concern for others, including the use of social media.



HIPAA PRIVACY AND INFORMATION SECURITY

The Security Rule

Specifies safeguards that covered entities, and their business associates must use to protect electronic protected health information (e-PHI).

The Security Regulation applies to the same entities as the Privacy Regulation.

We must:

- Ensure the confidentiality, integrity, and availability of e-PHI
 - **Confidentiality:** e-PHI cannot be available or disclosed to unauthorized persons
 - **Integrity:** e-PHI cannot be altered or destroyed in an unauthorized manner
 - **Availability:** e-PHI must be accessible and usable on demand by authorized persons



HIPAA PRIVACY AND INFORMATION SECURITY

The Security Rule

We must:

- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures – we do this by maintaining reasonable and appropriate administrative, physical, and technical safeguards



HIPAA PRIVACY AND INFORMATION SECURITY

Administrative Safeguards

We are required to implement administrative safeguards to identify, analyze, and mitigate risks to e-PHI.

How do we do this?

- IT security personnel
- Information security policies and procedures
- Information security training

The IT security staff develops policies and procedures, monitors systems, tests processes, and trains employees.



HIPAA PRIVACY AND INFORMATION SECURITY

Failure to follow information security policies or complete required training will result in disciplinary action.

Sanctions may include, but are not limited to:

Verbal or written
warning

Suspension

Termination

Suspension of the
right to access the
MHS IT Network
and/or termination of
other privileges.



HIPAA PRIVACY AND INFORMATION SECURITY

MHP may also notify law enforcement officials, and regulatory, accreditation, and licensure organizations.

Verbal or written
warning

Suspension

Termination

Suspension of the
right to access the
MHS IT Network
and/or termination of
other privileges.



HIPAA PRIVACY AND INFORMATION SECURITY

Physical Safeguards

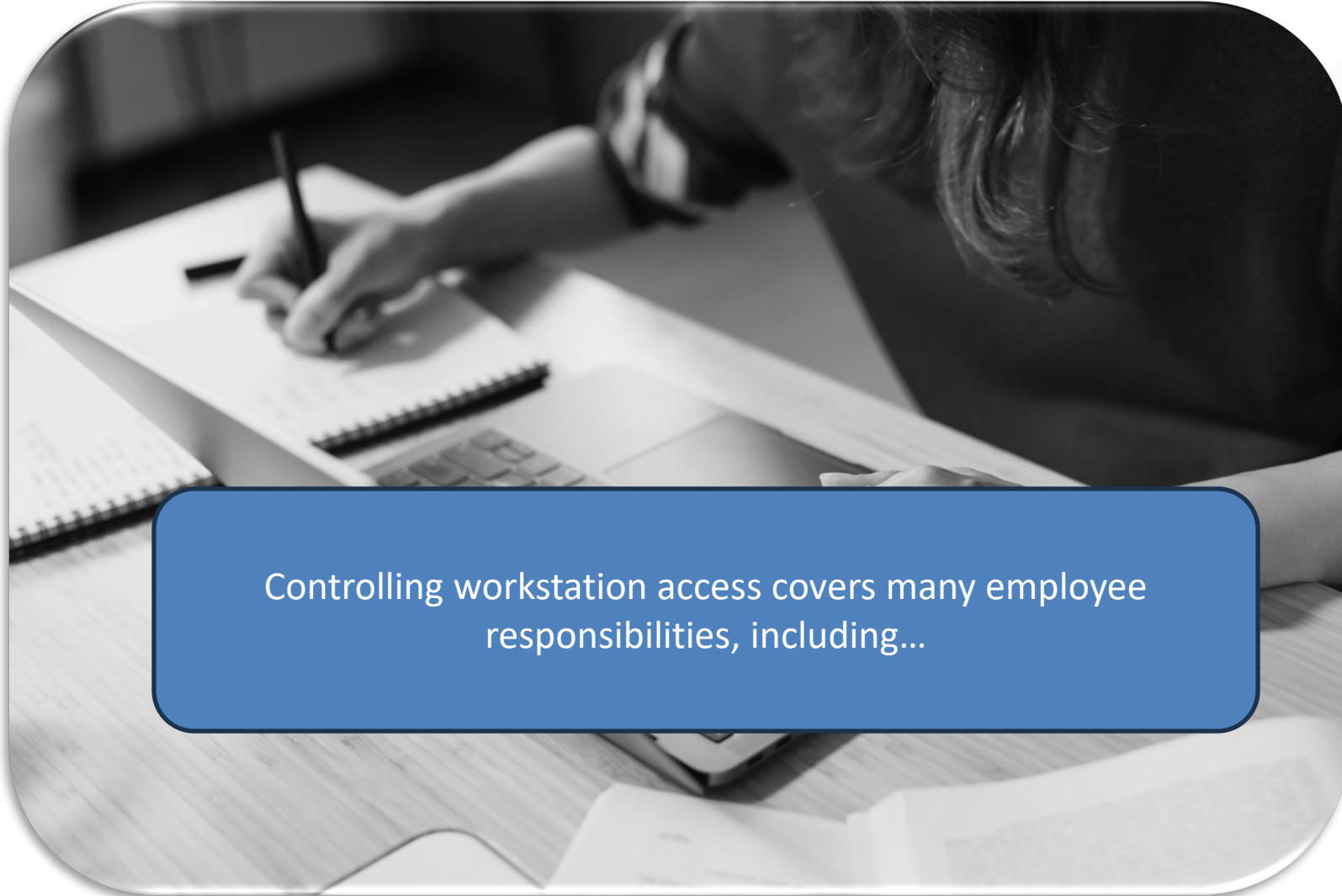
Items that control facility and workstation access. Facility access is controlled by our use of name badges with employee photos and security badge scanners on doorways that lead to areas containing PHI.

Workstation access is controlled by a combination of facility access and staff diligence.

You can do your part to protect PHI, and other private and confidential information, by keeping access-controlled doors closed, picking up your documents from printers right away, or using Secure Print, and always using a shred bin when you're done with a document. To ensure the security of sensitive documents awaiting shredding, be sure you insert the paper all the way into the bin.



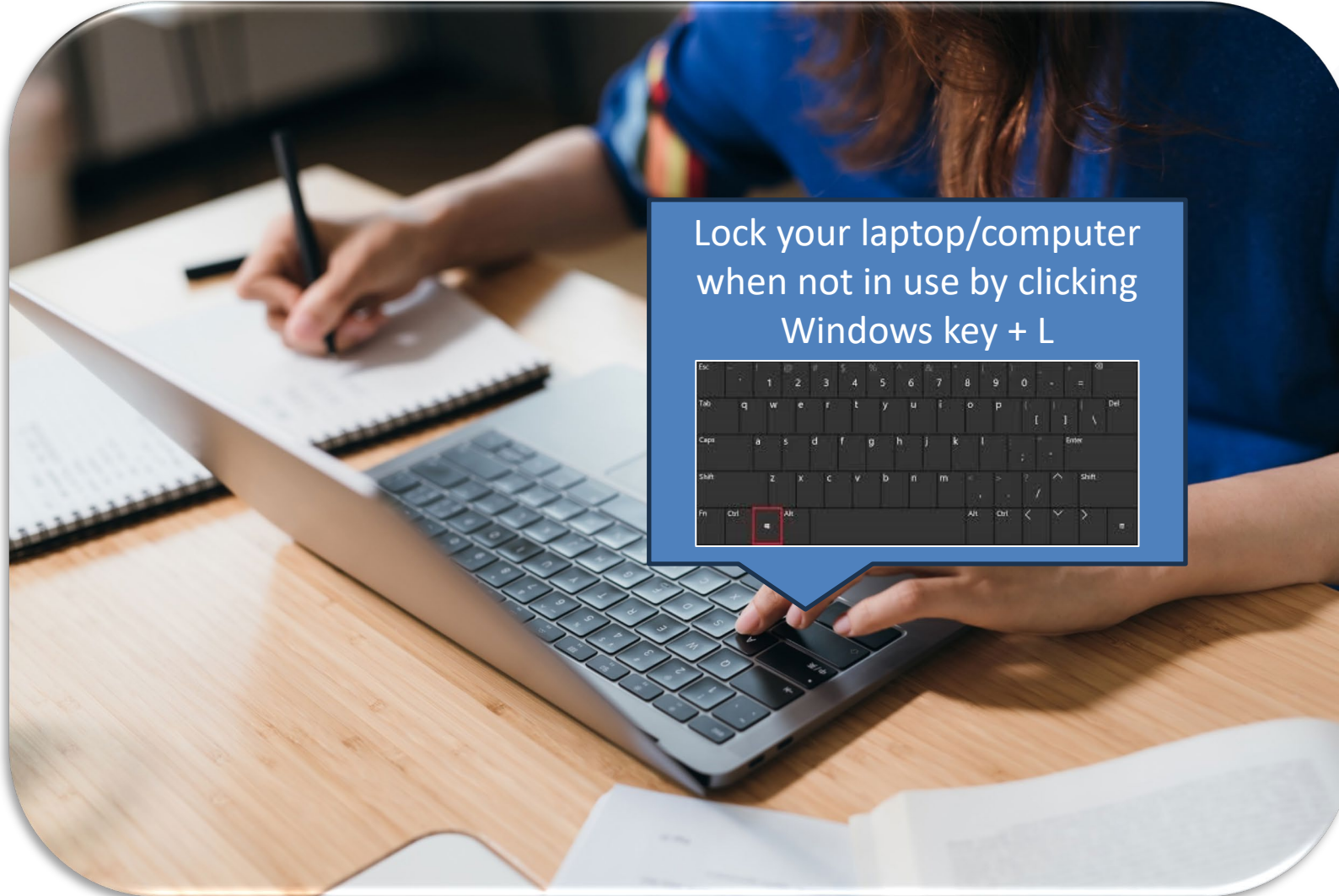
HIPAA PRIVACY AND INFORMATION SECURITY



Controlling workstation access covers many employee responsibilities, including...



HIPAA PRIVACY AND INFORMATION SECURITY





HIPAA PRIVACY AND INFORMATION SECURITY

Keep your passwords
secret - don't leave
them written down or
on your desk





HIPAA PRIVACY AND INFORMATION SECURITY



Secure your home workspace the same way you would at the office - keep the space private and PHI locked up when not in use



HIPAA PRIVACY AND INFORMATION SECURITY





HIPAA PRIVACY AND INFORMATION SECURITY

Monitoring for unauthorized or unknown individuals joining meetings where private or confidential information is discussed





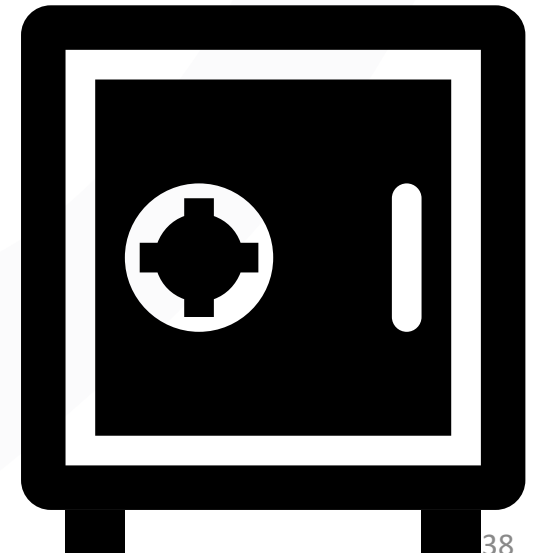
HIPAA PRIVACY AND INFORMATION SECURITY

Technical Safeguards

Technical safeguards are the systems MHS IT has put into place to implement access controls for e-PHI, to monitor and/or audit Information Systems, and to establish our network and secure all network traffic.

We also have controls in place to back-up critical data and ensure that e-PHI is not improperly altered or destroyed.

Any data kept on any Information System is the property of MHS. This information, including emails, may be examined by MHS employees or designees at any time, without notification, and used in any acceptable manner.





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

Reporting Suspected HIPAA Violations

Protecting patient data is a shared responsibility.

Reporting suspicious activity is a crucial component of the organization's overall HIPAA Privacy and Security programs and general cybersecurity defense.





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

Reporting Suspected HIPAA Violations

Cybersecurity defense is vitally important because cyberattacks are on the rise:

- Total annual cost to companies worldwide projected to reach \$10.5 trillion in 2025
- Cyber attacks on the healthcare sector have increased at more than twice the rate of other industries with a 45% rise in attacks since November of 2020
- 40 million individuals were affected by healthcare cyber attacks in 2023





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Breach Notification Rule

HIPAA rules define a breach as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule that compromises PHI security or privacy.





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Breach Notification Rule

HIPAA rules define a breach as the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule that compromises PHI security or privacy.

- When PHI is disclosed without consent or used without permission, all covered entities must notify affected individuals of the breach





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Breach Notification Rule

When you are aware of a potential breach, notify:

- Your manager
- Compliance Hotline at (877)640-0005 (English), (800)216-1288 (Spanish), or www.lighthouse-services.com/nmhs



Scan with your phone:





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Omnibus Rule

The Omnibus Rule is a set of modifications to the Health Insurance Portability and Accountability Act (HIPAA).

The Omnibus Rule addresses the following:

- Business Associates and subcontractors are liable for HIPAA compliance are responsible for their own breaches
- Patients have increase right to access and receive electronic copies of their protected health information (PHI) – as well as more control over restricting disclosures of their PHI, especially for out-of-pocket payments for health plans





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Omnibus Rule

The Omnibus Rule addresses the following:

- Stricter limits in using PHI for marketing purposes, require patient consent before use of their information
- Health plans cannot use genetic information (GINA) to determine eligibility or set premiums, and they are generally prohibited from collecting it for underwriting purposes
- Enhances aspects of the Privacy and Security Rule related to research, authorizations, and data security
- The Office of Civil Rights (OCR) enforces HIPAA and the Omnibus Rule clarifies penalties for violations





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Enforcement Rule

The Enforcement Rule emphasizes the role for the Office for Civil Rights (OCR) and their responsibility for enforcing HIPAA, including the right to investigate complaints involving covered entities and imposing penalties.

- Patients have the rights to file complaints with OCR.
 - OCR handles the complaints by conducting investigations and potentially refers investigations to the Department of Justice for criminal violations if appropriate – covered entities must cooperate fully with OCR investigations





HIPAA PRIVACY AND INFORMATION SECURITY

See Something? Say Something!

HIPAA's Enforcement Rule

- Enforces “minimum necessary” standard, which requires covered entities to disclose or use only the minimum amount of PHI
- OCR may seek voluntary compliance, corrective actions, or resolution agreements from covered entities to resolve violations





HIPAA PRIVACY AND INFORMATION SECURITY

Information System programs are responsible for managing and supporting the organization's technology infrastructure, ensuring systems run smoothly, securely, and efficiently.

Information Security programs are responsible for protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction, ensuring compliance with Information Security requirements.

Privacy and Information Security have similar disciplines with complimentary and overlapping objectives.



HIPAA PRIVACY AND INFORMATION SECURITY

The **Chief Information Security Officer** (CISO) serves as the first point of contact for all issues related to Cybersecurity at Methodist Health System. The primary functions of the CISO include:

- Assesses risks and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Health System
- Establishes and maintains a process for planning, implementing, evaluating, and documenting remediation efforts to address any deficiencies in the information security controls, policies, procedures, and practices of the Health System



HIPAA PRIVACY AND INFORMATION SECURITY

The primary functions of the CISO also include:

- Oversees the assessment of new and emerging technologies to determine “best fit” with enterprise business and IT strategies and gauges applicability to business processes by providing an architecture that fulfills business goals and objectives
- Serves as the designated HIPAA Security official responsible for the development and implementation of the HIPAA Security Rule policies and procedures to meet HIPAA Security Rule requirements
- Serves as the Qualified Individual (QI) responsible for the GLBA information security program

**Providing a safe
environment for our patients
also means protecting our
systems and their
information.**





HIPAA PRIVACY AND INFORMATION SECURITY

Email Usage

MHS email, instant messaging or other electronic communications systems may not be used to create or distribute any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

If you receive offensive email from another employee, please immediately report the matter to your manager or the Compliance Hotline at (877)640-0005 (English), (800)216-1288 (Spanish), or www.lighthouse-services.com/nmhs.



HIPAA PRIVACY AND INFORMATION SECURITY

Email Usage

Any email you send could be forwarded on to others without your knowledge or consent. All emails sent or forwarded outside of the MHS network have a Privacy and Intended Use Disclaimer footer. Use caution whether you're emailing internally or externally.



HIPAA PRIVACY AND INFORMATION SECURITY

Look out for these phishing “**red flags**” in email messages:

Email from unknown senders or unanticipated/suspicious attachments

- If you don't know the sender or aren't expecting the message or attachment, proceed with extreme caution

A Sense of Urgency

- The email asks you to take action, click a link, or divulge information immediately to claim a reward or avoid penalty

Generic Greetings

- Phishing emails often contain very generic greetings or even no greeting at all



HIPAA PRIVACY AND INFORMATION SECURITY

Look out for these phishing “**red flags**” in email messages:

Spelling and Grammar Mistakes

- Many phishing emails contain obvious spelling and grammar mistakes such as “accounts”

Inconsistent Links, Email Addresses & Domain Names

- The email address of the sender or the included link address does not match the purported affiliated company (www.go0gle.com)



HIPAA PRIVACY AND INFORMATION SECURITY

Look out for these phishing “**red flags**” in email messages:

Offers “Too Good To Be True”

- A message that claims you have been offered money or a ridiculous discount

Personal Information Requests

- Such as login credentials, financial information, SSN's, or other sensitive data



HIPAA PRIVACY AND INFORMATION SECURITY

On average, approximately **1.1 million emails per month** make it through the filters and into employees' inboxes!

That means we block approximately **6.5 million potentially malicious emails** each month for a variety of reasons. Email is the #1 attack surface for bad actors – be careful because we can't catch everything.





HIPAA PRIVACY AND INFORMATION SECURITY

**Our people are the best
defense against a breach**





HIPAA PRIVACY AND INFORMATION SECURITY

Secure Texting and Email

Texting Policy Highlights:

- Unencrypted texting of Protected Health Information (PHI), Primary Account Numbers, Personally Identifiable Information (PII), and/or Social Security Numbers (SSNs) is strictly prohibited
- Texting PHI can only occur between caregivers and only with an approved NMHS secure texting application
- Anyone requiring texting functionality for business purposes must have the approval of Information Security





HIPAA PRIVACY AND INFORMATION SECURITY

Secure Texting and Email

Email Policy Highlights:

- Information considered “Restricted” or “Sensitive” by the Information Technology Data Management Standard must not be sent via E-mail, regardless of the recipient, without proper email encryption controls
- Encryption is required for E-mails containing PHI, Primary Account Numbers, PII, SSNs, usernames and passwords or credit card holder data sent to any non-MHS E-mail recipient





HIPAA PRIVACY AND INFORMATION SECURITY

Passwords should be designed and secured properly.

Passwords must be a minimum of 15 characters long and have 3 of the 4 following requirements:

- Upper case character(s)
- Lower case character(s)
- Numeric character(s)
- Special characters(s)

Avoid using “keyboard pattern” passwords that satisfy minimum requirements but can be easily guessed.

Example: 1qaz2wsx#EDC\$RFV

Note: Consider creating a passphrase instead of a password if it assists in being easier to remember.



HIPAA PRIVACY AND INFORMATION SECURITY

When it comes to password security, ensure that you:

Never write down or store passwords on your desktop, computer or mobile device.

Never reuse passwords from other sites.

Change temporary passwords upon logging in.

Don't include personal information in your passwords.

Contact IT promptly if you suspect your passwords have been compromised to assist with resetting your account.

Never share your passwords with anyone. This includes colleagues, family members, external contacts, or even IT staff.





HIPAA PRIVACY AND INFORMATION SECURITY

Mobile Device Protection

Be smart! Mobile devices store a ton of personal and professional data.



Treat Your Devices Like Cash

You wouldn't leave money sitting out in the open – don't do it with your devices either



Lock Every Device, Every Time

A six-digit PIN is the minimum safeguard – use complex passwords and fingerprint IDs



Make Trusted Connections

Be extra cautious about GPS tracking, open Wi-Fi networks, and Bluetooth pairing

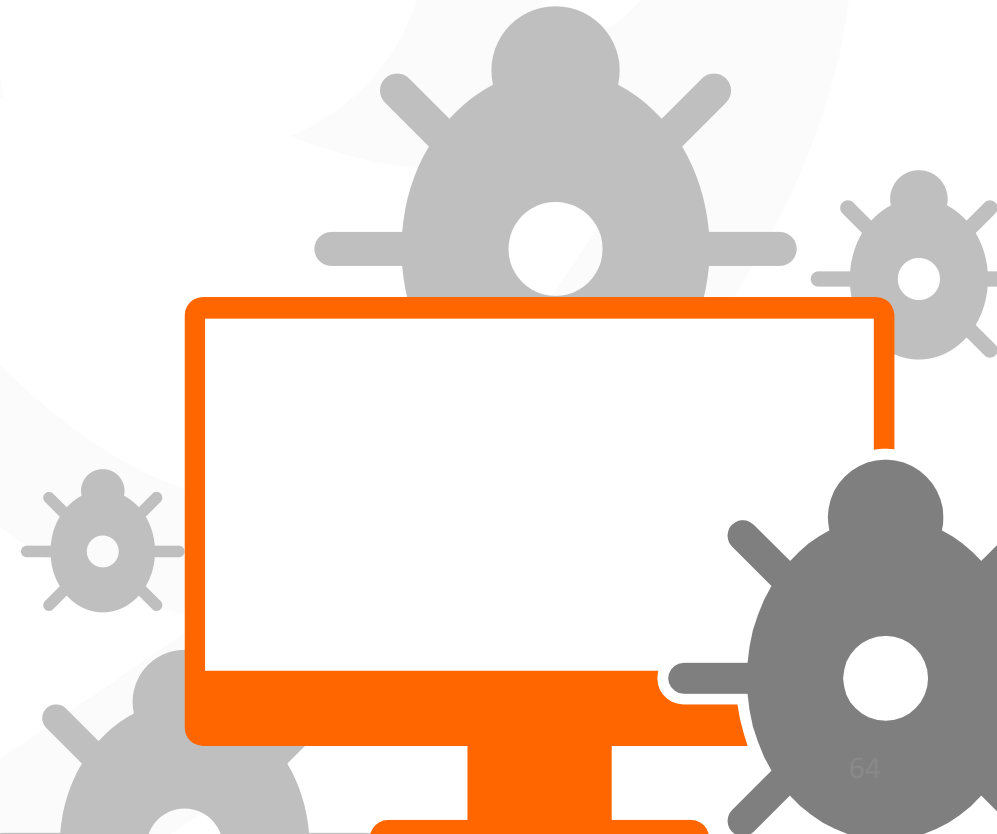


HIPAA PRIVACY AND INFORMATION SECURITY

Do you know about the **Clear Desk Clear Screen** policy?

It's a system-wide standard for securing the information stored on desks and computers. The critical steps each employee needs to follow are as follows:

- Lock your computer when you step away and log off at the end of the day
- Lock up any restricted or sensitive information when not in use
- Lock away passwords - do not post on a sticky note in plain sight
- Treat DVD, USB, and other removable media as sensitive....lock them up
- Erase sensitive and restricted information from whiteboards





HIPAA PRIVACY AND INFORMATION SECURITY

Removable Media Management

In today's world, removable media poses a significant risk to the confidentiality of information due to its ease of transportation. Removable media includes USB flash drives, CD/DVD, BluRay disks – anything that can be removed from a computer while it's running.



HIPAA PRIVACY AND INFORMATION SECURITY

Secure Printing

Employees are encouraged to scan and store documents electronically in an IT supported location rather than on individual computers or attached in emails and restrict access by job need.

If you need to print a document, pick up the printed documents right away to prevent mix-ups and protect confidential information that may be included in the document.



HIPAA PRIVACY AND INFORMATION SECURITY

Computer Theft & Recovery

Be cautious about leaving portable devices out in the open where they could be easily stolen. Make sure that any laptop, tablet, or phone with sensitive and confidential information is secure at all times. Do not allow children or family members to use your issued portable devices.

What should you do if your device is stolen?

Notify your supervisor as soon as you realize it's missing!



HIPAA PRIVACY AND INFORMATION SECURITY

Computer Theft & Recovery

Time is of the essence to secure confidential information. Mistakes happen and this is understood under a Just Culture. However, failure to report a missing device in a timely manner is a violation of the Information Security policy.

The potential for theft is why it's so important to never ever share your username and/or password.

Report stolen or missing equipment as soon as you are aware of the problem. IT will work with you to try and remove or wipe any sensitive information from the device. We need your help to keep our information secure.



HIPAA PRIVACY AND INFORMATION SECURITY

Remote User Best Practices

General Tips:

- Hand carry instead of checking in laptops to maintain positive control especially when travelling through foreign airports
- Do not leave laptops in plain view in vehicles, even when locked
- Store laptops in hotel safe when not in the room
- Travel with the least amount of data required to do your work to minimize the impact if your laptop is lost or stolen
- Ensure PHI, PII, and other sensitive data is encrypted
- Avoid connecting to public Wi-Fi and verify SSID with vendor/provider



HIPAA PRIVACY AND INFORMATION SECURITY

Remote Users in Foreign Countries

- Ensure you coordinate PRIOR to your trip
- Before departing, provide the following information to the IT:
 - Type of access required – email only, full access, Intranet, specific websites, etc
 - Systems requiring access (phones, laptops, tablets, etc.) and if they are company or personal devices; if using a phone, indicate if it is an iPhone or Android phone
 - Countries visiting
 - Dates of visit
- There may be additional information required that can only be obtained at your destination such as your assigned IP address.



HIPAA PRIVACY AND INFORMATION SECURITY

Social Media / Networking / Internet

The Internet:

To protect personal safety and privacy, Internet users should not give out personal information to others on public resources, without taking into consideration the risks of doing so.

Registering company email accounts for any social media site for personal use is prohibited.

Personal usage of company systems to access the Internet is permitted during, before, and after business hours, if such use follows pertinent policies and guidelines and does not have a detrimental effect on company, or on the User's job performance.



HIPAA PRIVACY AND INFORMATION SECURITY

Social Media / Networking / Internet

Streaming Services:

Streaming video or audio content unrelated to working roles and responsibilities will be continually monitored and reported for impact on network performance.

Blogging, Social Networking and Social Media:

Blogging and other use of Social Networking, Social Media and Internet-based interpersonal communications by Users are subject to the terms and restrictions set forth in the Company Policy.



HIPAA PRIVACY AND INFORMATION SECURITY

Prohibited Activities

- Accessing or using someone else's account, files, or data without permission
- Malicious network activity such as intercepting data, disrupting service, altering data or data flow
- Installing unauthorized software on information systems
- Port scanning, security scanning, and password cracking
- Attaching unauthorized hardware to the NMHS Infrastructure
- Attempting to break into another computer or computer resource
- Copying software in violation of the vendor's license agreement
- Sending or posting "confidential" information
- Improper or illegal use of the Internet



HIPAA PRIVACY AND INFORMATION SECURITY

Malware

Malware, short for malicious software, is a computer program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.



HIPAA PRIVACY AND INFORMATION SECURITY

The following are common categories of malware:

- **Viruses** self-replicate by inserting copies of itself into host programs or data files. Viruses are often triggered through user interaction, such as opening a file or running a program
- **Worms** are self-replicating, self-contained programs that usually executes itself without user intervention
- **Trojan Horses** are self-contained, nonreplicating programs that appear benign but have a hidden malicious purpose
- **Malicious Mobile Code** is software with malicious intent transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction
- **Blended Attacks** use multiple infection or transmission methods – most malware today are blended attacks



HIPAA PRIVACY AND INFORMATION SECURITY

Is My Computer Infected?

The following are possible signs that your computer may be infected with malware:

- Computer behaves strangely
- Computer or web browser often freezes
- Unexpected messages or image
- Random sounds
- Programs run slowly or start unexpectedly
- Operating System doesn't load upon startup
- People you know receive emails from you that you didn't send
- You receive lots of system or error messages
- Files or folders have been deleted or changed

If you suspect your computer is infected, report it as a Security Incident.



HIPAA PRIVACY AND INFORMATION SECURITY

Security Incident Reporting

Examples include data breaches, compromises, malware, hacks.

- Disconnect your system from the Internet, lock, and leave powered on.
 - Wired: remove network cable from computer
 - Wireless: place computer into “airplane” mode
- Do not attempt to fix system
- Call the ITOC and await further instruction from Information Security



HIPAA PRIVACY AND INFORMATION SECURITY

Security Incident Reporting

Examples include data breaches, compromises, malware, hacks.

- Provide the following info:
 - Callback number
 - Location/Floor/Unit/Office
 - Computer Name
 - Detailed description of observations or indications of the suspected Information Security Incident

For suspected Information Security Incidents, contact your IT department.



HIPAA PRIVACY AND INFORMATION SECURITY

Artificial Intelligence Systems

Artificial Intelligence (AI): The application of computer systems to accomplish tasks that mimic human intelligence. This includes a broad array of programs and systems including machine learning algorithms, natural language processing, robotics, and other tools to process images or data sets.

Use of Artificial Intelligence Systems:

- NMHS supports the safe, responsible, and ethical use of AI in its operations and administration
- The user of an AI system is responsible for acquiring and maintaining the necessary competency with AI to ensure safe, responsible, and ethical use of the AI system
- Providing PHI and/or Sensitive or Restricted Data to an AI system exposes that PHI/Data to possible breaches of the AI system



HIPAA PRIVACY AND INFORMATION SECURITY

Use of Artificial Intelligence Systems:

- A Business Associate Agreement (BAA) must be in place for any AI system into which PHI and/or Sensitive or Restricted Data will be stored or accessed
- AI systems and AI generated content must not be used as a substitute for professional, medical, or ethical judgement
- Treatment related AI generated content that has not been reviewed and validated by clinical decision makers
- The user must take into consideration AI-related bias, transparency, and security risks and is responsible for verifying the accuracy and veracity of all AI content they generate for NMHS business purposes
- Use of an AI system must comply with the Information Technology (IT) Acceptable Use Standard and other IT and Information Security (IS) policies, procedures, and practices
- Evaluation of AI systems will be performed by IS



ANNUAL SAFETY AND COMPLIANCE 2026

Medicare Part C & D and Fraud, Waste, and Abuse



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Upon completion of the business compliance training, you will understand:

- MHS Commitment to Compliance
- Combating Medicare C&D Fraud, Waste and Abuse (FWA)
- Major Laws, Regulations and Penalties pertaining to FWA
- Indicators of Potential FWA



MHS Compliance Commitment

As a participant in the Medicare Program, employees are expected to uphold the highest standards of ethical and legal behavior. Simply put – it's about doing the right thing, even when no one is watching. The Centers for Medicare & Medicaid Services (CMS) requires MHS and their affiliates to implement and maintain an effective compliance program for its Medicare Parts C and D plans

At MHP, we're committed to conducting business in a way that's fair, honest, and respectful. Every action we take should reflect integrity, competence, and professionalism.

Whether you're working with patients, providers, or partners, your words and actions should always inspire trust and confidence.



Non-Compliance

Non-compliance is conduct that does not conform to the law, Federal health care program requirements, or an organization's ethical and business policies. CMS has identified the following Medicare Parts C and D high risk areas:

- Agent/broker misrepresentation
- Appeals and grievance review (for example, coverage and organization determinations)
- Beneficiary notices
- Conflicts of interest
- Claims processing
- Credentialing and provider networks
- Documentation and Timeliness requirements
- Ethics
- FDRs (First-Tier, Downstream, or Related Entity) oversight and monitoring
- Health Insurance Portability and Accountability Act (HIPAA)
- Marketing and enrollment
- Pharmacy, formulary, and benefit administration
- Quality of care



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Medicare Part C

Also known as Medicare Advantage (MA), is a health plan choice available to Medicare beneficiaries. Private, Medicare-approved insurance companies run MA programs. These companies arrange for, or directly provide, health care services to the beneficiaries who elect to enroll in an MA plan.

MA plans must cover all services Medicare covers with the exception of hospice care. They provide Part A and Part B benefits and may also include prescription drug coverage and other supplemental benefits.

Medicare Part D

Known as the Prescription Drug Benefit, provides prescription drug coverage to all beneficiaries enrolled in Part A/Part B who elect to enroll in a Medicare Prescription Drug Plan (PDP) or an MA Prescription Drug (MA-PD) plan.

Medicare approved insurance and other companies provide prescription drug coverage to individuals who live in a plan's service area.



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

A person who provides health or administrative services to a Medicare Part C or Part D enrollee is likely an employee of a:

Sponsor

(Medicare Advantage Organization [MAO] or a Prescription Drug Plan [PDP])

First-Tier Entity

(ex: Pharmacy Benefit Management [PBM]; hospital or health care facility; provider group; doctor's office; clinical laboratory; customer service provider; claims processing and adjudication company; a company that handles enrollment, disenrollment, and membership functions; and contracted sales agents)



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

A person who provides health or administrative services to a Medicare Part C or Part D enrollee is likely an employee of a:

- **Downstream Entity** (ex: pharmacies, doctor's office, firms providing agent/broker services, marketing firms, and call centers)
- **Related Entity** (ex: Entity with common ownership or control of a Sponsor, health promotion provider, or SilverSneakers®)

CMS expects all Sponsors will apply their training requirements and effective lines of communication to their FDRs (First-Tier, Downstream, or Related Entity).

Having effective lines of communication means employees of the Sponsor and the Sponsor's FDRs have several avenues to report compliance concerns.



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

To detect, you need to know the Laws:

Federal Civil False Claims Act (FCA)

As defined in prior slides, FCA liability can arise in situations such as improperly avoiding an obligation to pay the government. Conspiring to commit any of these acts is also a violation of the FCA.

Example – a Florida Part C Plan:

- Hired an outside company to review medical records to find additional diagnosis codes it could submit to increase CMS risk capitation payments
- Was informed by the outside company that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported
- Failed to report the unsupported diagnosis codes to Medicare
- Agreed to pay \$22.6 Million to settle FCA allegations

Damages & Penalties

Penalties for violating the civil FCA may include recovery of up to 3 times the amount of the government's damages due to the false claims, plus \$11,000 per false claim filed.



To detect, you need to know the Laws:

Criminal Health Care Fraud Statute

As defined in prior slides, the Criminal Health Care Fraud Statute makes it a criminal offense to knowingly and willfully execute a scheme to defraud a health care benefit program.

Example – a Pennsylvania pharmacist:

- Submitted Part D claims for nonexistent prescriptions and drugs not dispensed
- Pleaded guilty to health care fraud
- Got a 15-month prison sentence and was ordered to pay more than \$166,000 in restitution to the plan

Damages & Penalties

Health care fraud is subject to criminal fines up to \$250,000. It's also punishable by imprisonment up to 10 years, or up to 20 years if the violation results in serious bodily injury. If the violation results in death, a person could be imprisoned for any term of years, up to and including life.



To detect, you need to know the Laws:

Anti-Kickback Statute (AKS)

The AKS makes it a crime to knowingly and willfully offer, pay, solicit, or get any remuneration directly or indirectly to encourage or reward patient referrals or business generation involving any item or service payable by a federal health care program. When a provider offers, pays, solicits, or gets unlawful remuneration, they violate the AKS.

The Safe Harbor regulations describe various payment and business practices that, although they potentially implicate the AKS, aren't treated as AKS offenses if they meet certain regulatory requirements. People and entities remain responsible for complying with all other laws, regulations and guidance that apply to their businesses.



To detect, you need to know the Laws:

Anti-Kickback Statute (AKS)

Example – a Physician operating a Rhode Island Pain Management Practice:

- Conspired to solicit and get kickbacks for prescribing a highly addictive version of the opioid fentanyl
- Reported patients had breakthrough cancer pain to secure insurance payments
- Got \$188,000 in speaker fee kickbacks from the drug manufacturer
- Admitted the kickback scheme cost Medicare and other payers more than \$750,000
- Was required to pay more than \$750,000 in restitution

Damages & Penalties

- Violations are punishable by 1 or both:
- A fine up to \$100,000
- Imprisonment up to 10 years



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

To detect, you need to know the Laws:

Physician Self-Referral Law (Stark Law)

Example

A California hospital was ordered to pay more than \$3.2 million to settle Stark Law violations for maintaining 97 financial relationships with physicians and physician groups outside the fair market value standards or what were improperly documented as exceptions.

Damages & Penalties

Medicare will not pay for claims tainted by an arrangement that doesn't comply with the Physician Self-Referral Law. The federal government may impose a penalty of not more than \$15,000 for each service provided and may also fine people not more than \$100,000 for each unlawful arrangement or scheme entered.



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

To detect, you need to know the Laws:

Civil Monetary Penalties Law (CMPL)

The CMPL authorizes the Office of Inspector General (OIG) to seek civil monetary penalties (CMPs) and sometimes exclusion for a variety of health care fraud violations. Some violations that may justify CMPs include:

- Arranging for an excluded person's or entity's services or items
- Failing to grant OIG timely record access
- Filing a claim you know, or should know, is for an item or service that wasn't provided as claimed or is false or fraudulent
- Filing a claim you know or should know is for an item or service that won't be paid by Medicare
- Violating the AKS
- Violating Medicare assignment provisions
- Violating the Medicare physician agreement
- Providing false or misleading information expected to influence a discharge decision
- Failing to provide an adequate medical screening exam for patients who come to a hospital emergency department with an emergency medical condition or in labor
- Making false statements or misrepresentations on applications or contracts to participate in federal health care programs.



To detect, you need to know the Laws:

Civil Monetary Penalties Law (CMPL)

Example

A California pharmacy and its owner agreed to pay more than \$1.3 million to settle allegations they submitted unsubstantiated Part D claims for brand name prescription drugs the pharmacy couldn't have dispensed based on inventory records.

Damages & Penalties

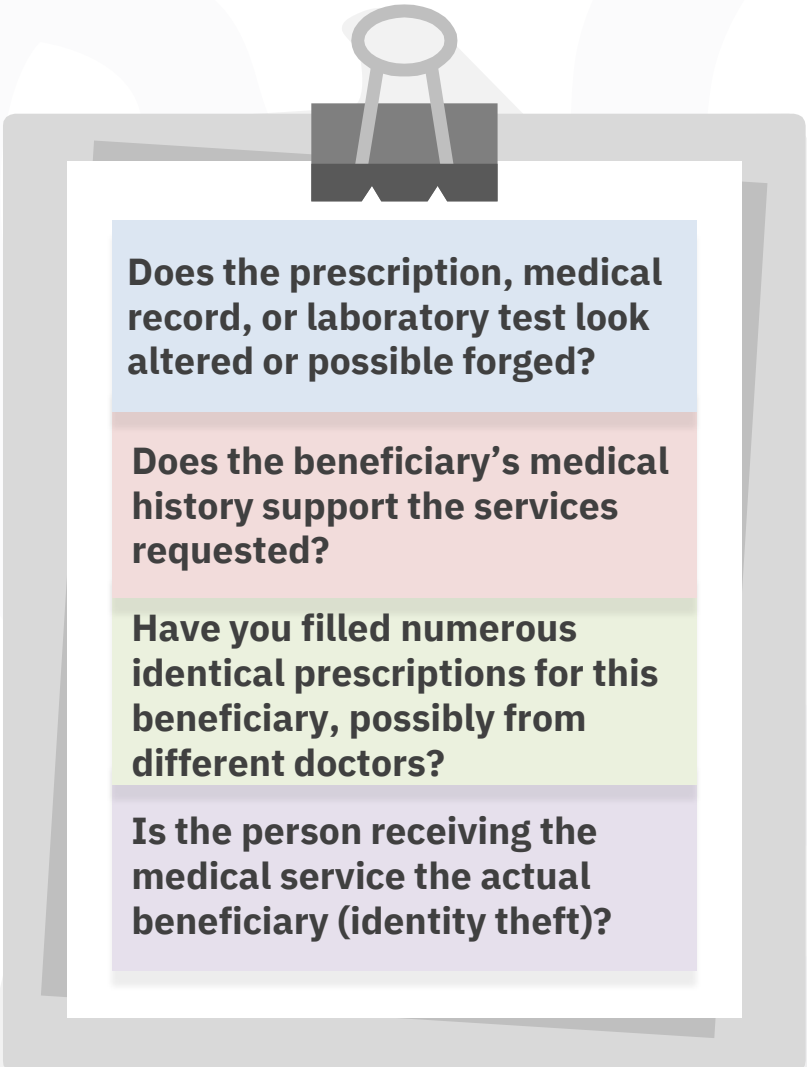
Penalties and assessments vary based on the type of violation. Penalties can be approximately \$10,000 - \$100,000 per violation. CMPs may also include an assessment of up to 3 times the amount claimed for each item or service or up to 3 times the amount of remuneration offered, paid, solicited, or received.



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues:
Beneficiary

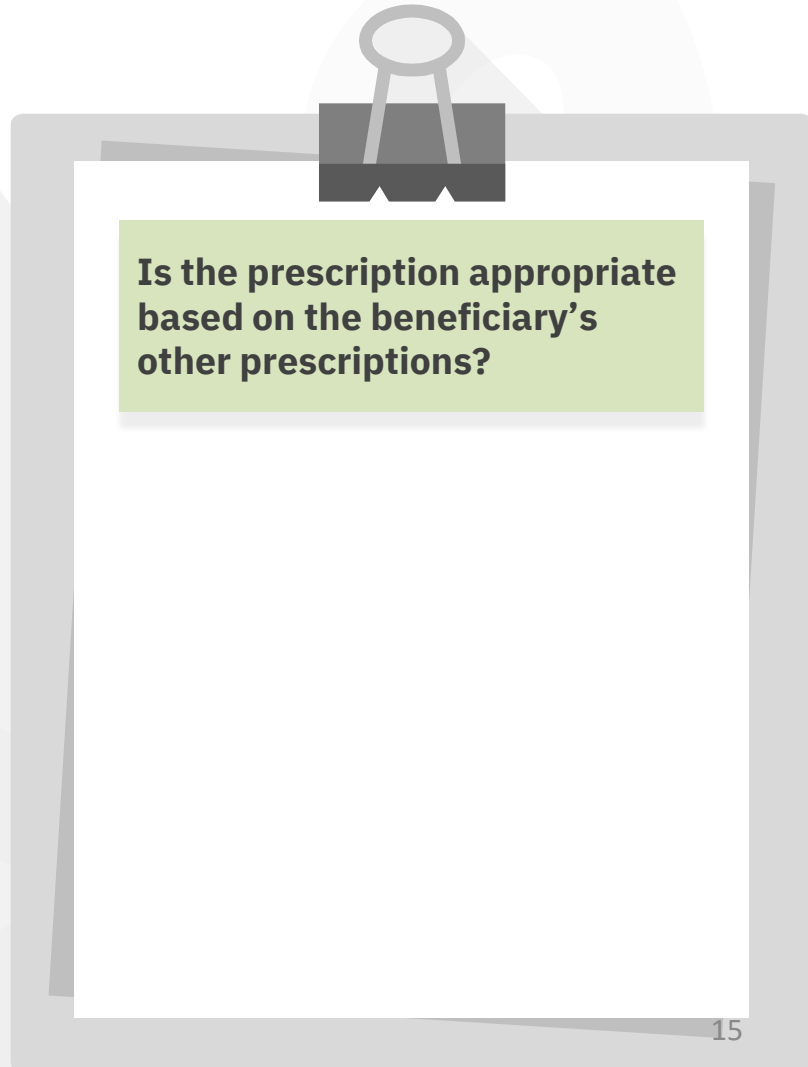


Does the prescription, medical record, or laboratory test look altered or possible forged?

Does the beneficiary's medical history support the services requested?

Have you filled numerous identical prescriptions for this beneficiary, possibly from different doctors?

Is the person receiving the medical service the actual beneficiary (identity theft)?



Is the prescription appropriate based on the beneficiary's other prescriptions?



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues: **Provider**

Are the provider's prescriptions appropriate for the member's health condition (medically necessary)?

Does the provider bill the Sponsor for services not provided?

Does the provider write prescriptions for diverse drugs or primarily for controlled substances?

Is the provider performing medically unnecessary services for the member?

Is the provider prescribing a higher quantity than medically necessary for the condition?

Is the provider's diagnosis for the member supported in the medical record?



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues:
Pharmacy

Are drugs being diverted (drugs meant for nursing homes, hospice, and other entities being sent elsewhere)?

Are the dispensed drugs expired, fake, diluted, or illegal?

Are generic drugs provided when the prescription requires that brand drugs be dispensed?

Are PBMs being billed for prescriptions that are not filled or picked up?

Are proper provisions made if entire prescriptions cannot be filled (no additional dispensing fees for split prescriptions)?

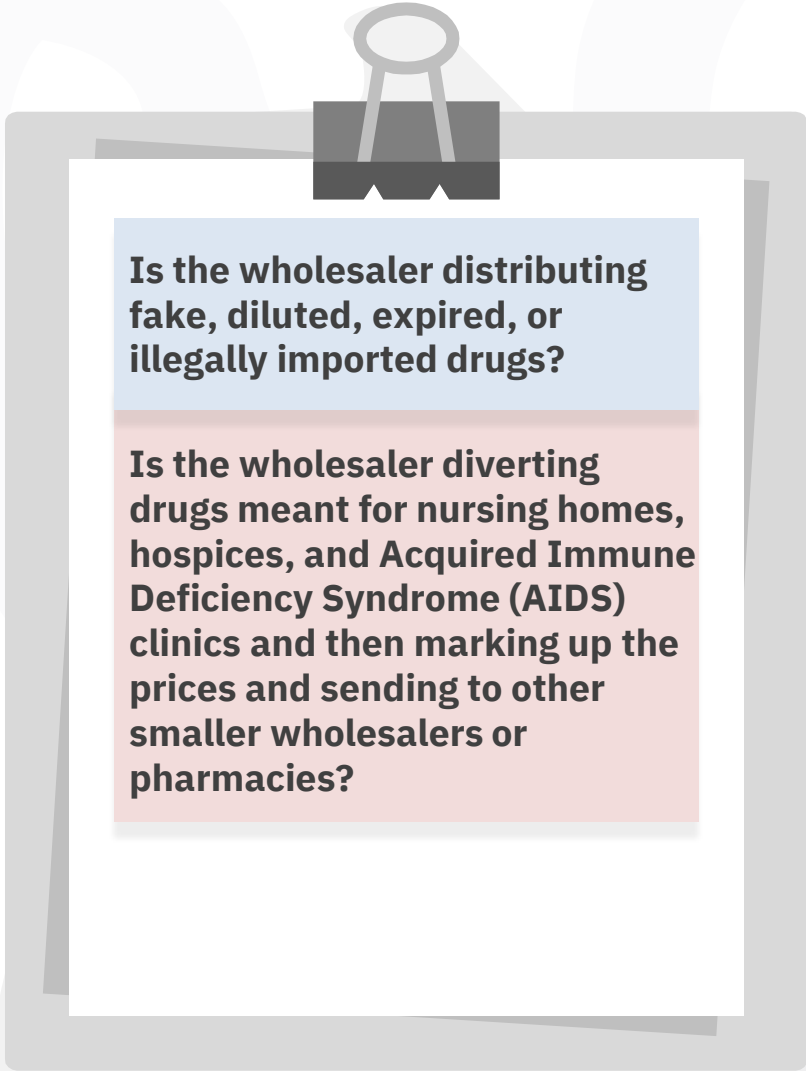
Do you see prescriptions being altered (changing quantities or Dispense As Written)?



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues:
Wholesaler



Is the wholesaler distributing fake, diluted, expired, or illegally imported drugs?

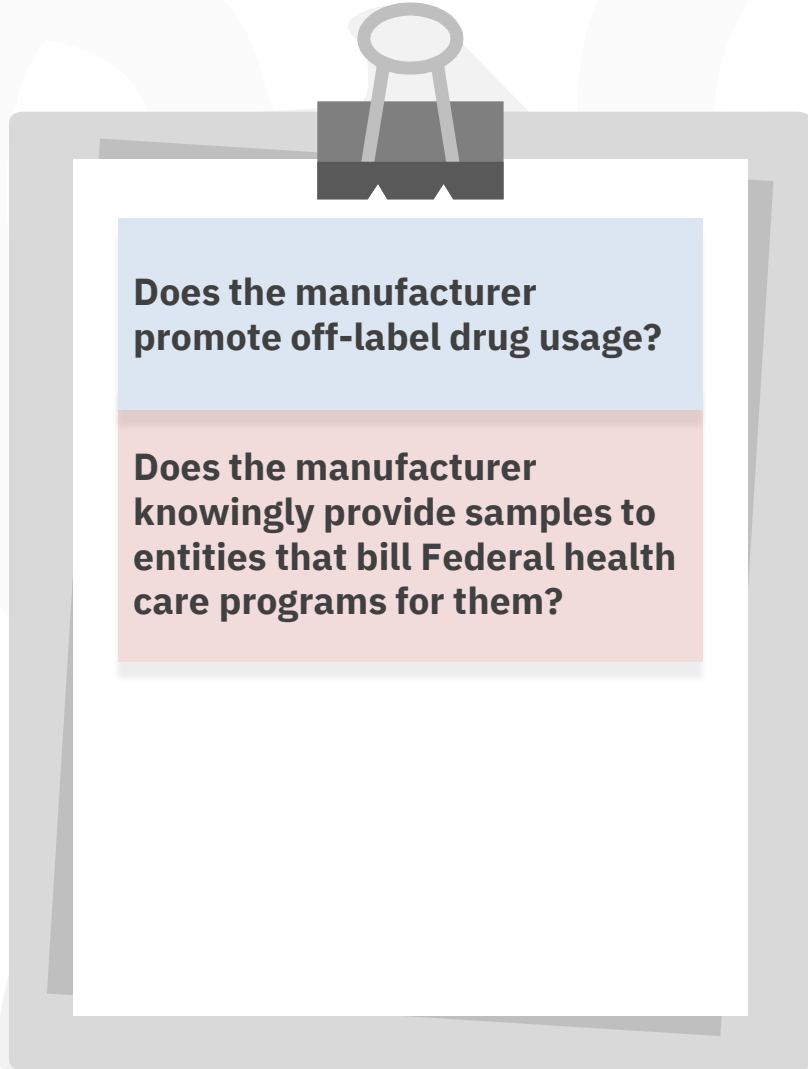
Is the wholesaler diverting drugs meant for nursing homes, hospices, and Acquired Immune Deficiency Syndrome (AIDS) clinics and then marking up the prices and sending to other smaller wholesalers or pharmacies?



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues:
Manufacturer



**Does the manufacturer
promote off-label drug usage?**

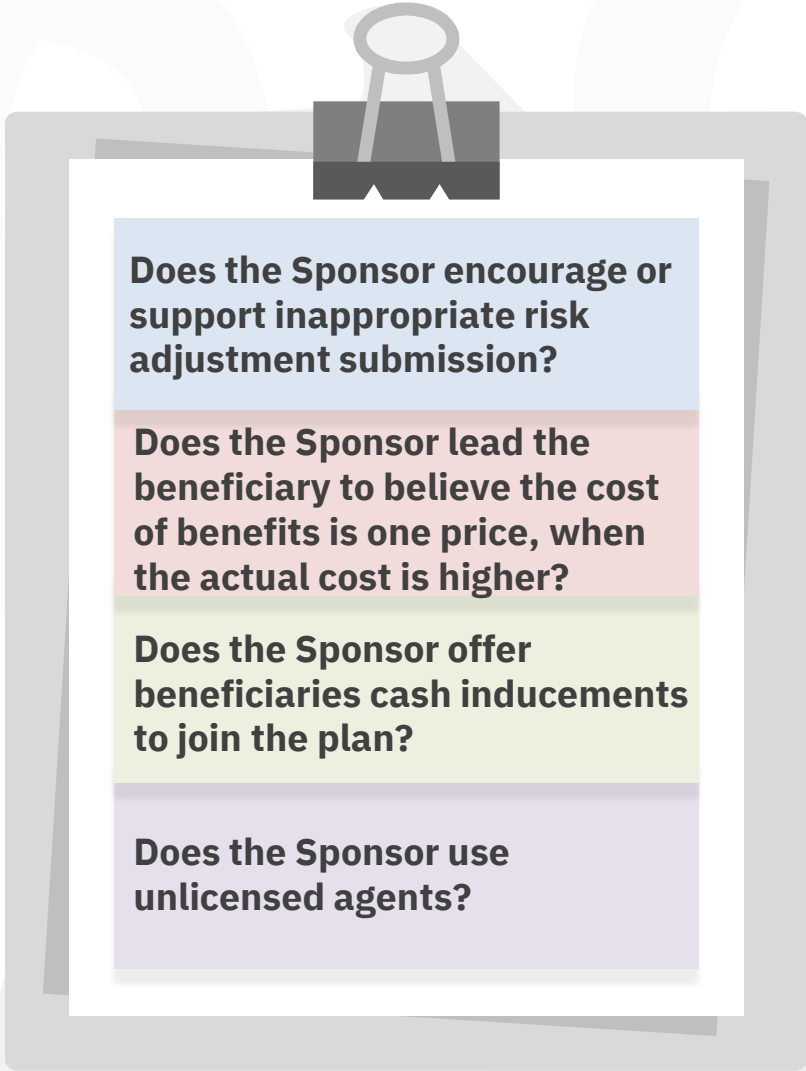
**Does the manufacturer
knowingly provide samples to
entities that bill Federal health
care programs for them?**



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

Indicators to help you recognize signs of someone committing FWA.

Potential Issues:
Sponsor



Does the Sponsor encourage or support inappropriate risk adjustment submission?

Does the Sponsor lead the beneficiary to believe the cost of benefits is one price, when the actual cost is higher?

Does the Sponsor offer beneficiaries cash inducements to join the plan?

Does the Sponsor use unlicensed agents?



MEDICARE PART C & D AND FRAUD, WASTE, AND ABUSE

As a person providing health or administrative services to Medicare Part C or D enrollees, **you play a vital role in preventing fraud, waste, and abuse (FWA)**. Conduct yourself ethically, stay informed of MHS policies and procedures, and keep an eye out for potential compliance issues.

Report potential compliance issues. MHS has mechanisms for reporting potential FWA and other compliance issues. We have options for anonymous reporting, and we will never retaliate against you for making a report in good faith. We will promptly correct identified compliance issues with effective corrective action plans that include ongoing monitoring and auditing.