Compliance Training

LMH Health

Revised 07/06/2022

Patient First

We consider the patient first in everything we do.

Innovate!

We actively explore new ideas and approach change with agility and an open mind.

Better Together

We actively strive to be a diverse LMH Health team who works together to achieve excellence.

Own It/Solve It

We hold ourselves accountable for our actions and we collaborate for solutions

Listen/Speak Up

We embrace a diverse culture of open, respectful, well-intended communication, where we listen, share, and value ideas to create equitable solutions.

In Joy

We create a workplace that is both fun and meaningful.

Content

Introduction

Sponsor, First Tier, Downstream, and Related Entities

Sponsor	Medicare Advantage Organization (MAO) or a Prescription Drug Plan (PDP)
First Tier Entity	Any party that enters into a written arrangement, acceptable to CMS, below the level of a First Tier arrangement (pharmacy, claim or billing company).
Downstream Entity	Any party that enters into a written arrangement acceptable to CMS with a sponsor or applicant to provide administrative or healthcare services for a Medicare eligible individual under Part D (hospital, provider, PBM).
Related Entity	Any entity that is related to the Sponsor by common ownership or control and performs some of the sponsor's management functions under contract or delegation; Furnishes services to Medicare members under an oral or written agreement; or Leases real property or sells materials to the sponsor at a cost of more than $2,500 during a contract period. 42 CFR 422.2 & 423.4

Compliance Program

An effective compliance program fosters a culture of compliance within an organization and

1. Prevents, detects, and corrects non-compliance
2. Is fully implemented and is tailored to an organization's unique operations and circumstances
3. Has adequate resources
4. Promotes the organization's Standards of Conduct
5. Establishes clear lines of communication for reporting non-compliance

An effective compliance program is essential to prevent, detect, and correct Medicare non-compliance, as well as Fraud, Waste, and Abuse (FWA).

Compliance Program

LMH Health and their first tier, downstream and related entities are obligated to have a Compliance Program to guard against potential fraud, waste, and abuse. The plan must include

1. Written policies, procedures, and standards of conduct articulating the organization's commitment to comply with all applicable Federal and State standards
2. The designation of a compliance officer and compliance committee
3. Effective training and education between the compliance officer and the MA/Part D plan and the MA/Part D plan sponsor's first tier, downstream, and related entities
4. Effective lines of communication between the compliance officer, members of the compliance committee, the MA/Part D plan sponsor and first tier, downstream, and related entities
5. Enforcement of standards through well-publicized disciplinary guidelines
6. Procedures for internal monitoring and auditing
7. Procedures for ensuring prompt responses to detected offenses and development of corrective action initiatives relating to the organization's contract as a MA/Part D plan sponsor

Your Role in Compliance

Do the right thing

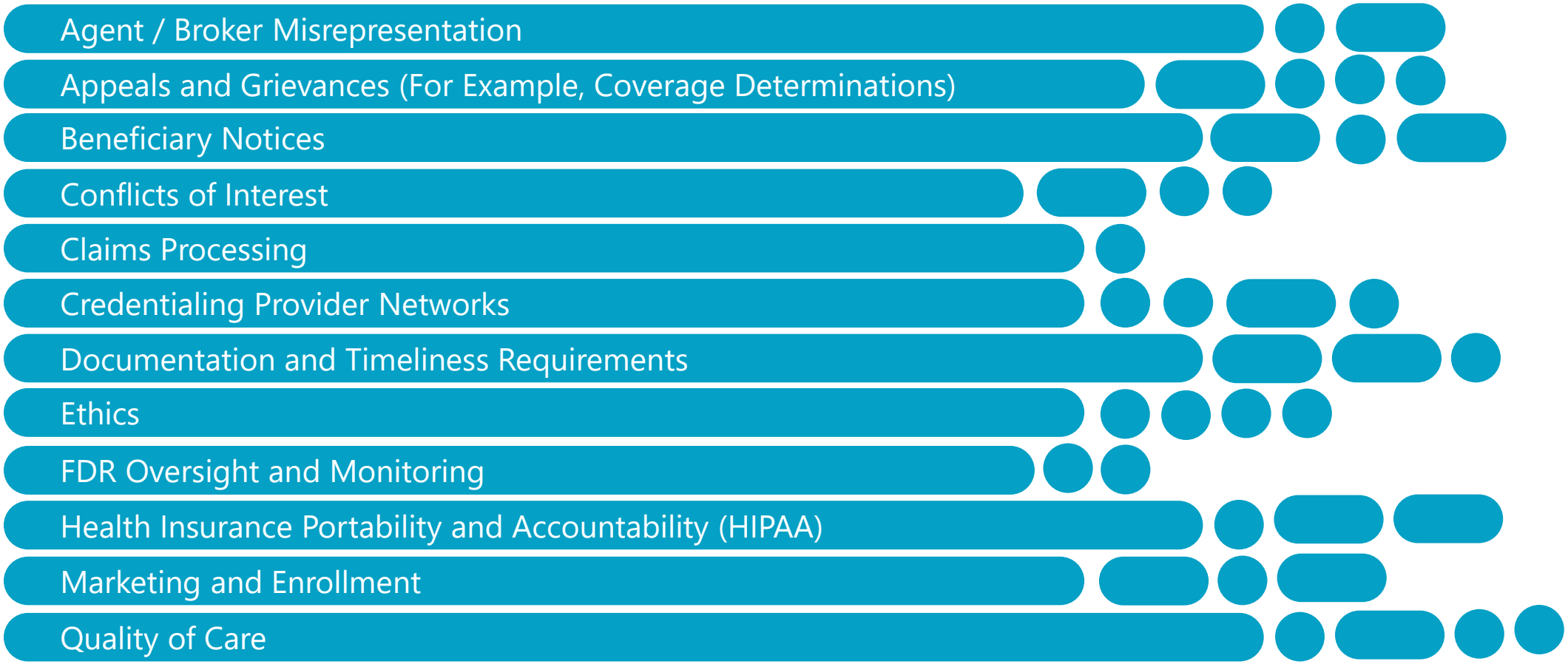
Comply with all applicable laws, regulations, and CMS requirements; and Report suspected violations

Know what is expected

Beyond following the general ethical guidelines, how do you know how to handle a specific situation? Standards of Conduct state compliance expectations and principles and values by which an organization operates.

Non Compliance

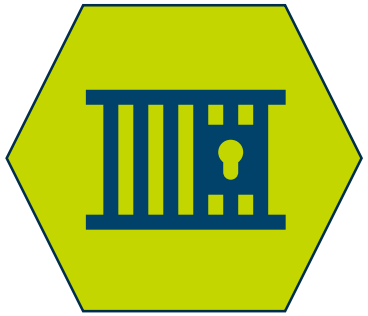
Non-compliance is conduct that does not conform to the law, Federal healthcare program requirements, or an organization's ethical and business policies. The following are high risk areas of non-compliance:



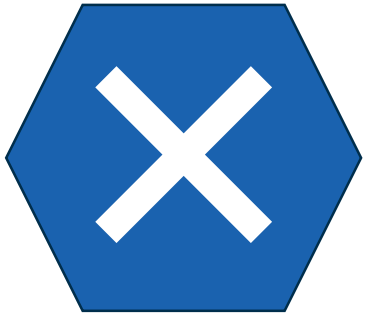
Consequences of Non-Compliance

Failure to follow requirements can lead to serious consequences

Contract Termination



Criminal Penalties



Exclusion from participation in all Federal health care programs

Civil monetary penalties

Additionally, your organization has disciplinary standards for non-compliance including, but not limited to mandatory training or retraining, disciplinary action; or termination.

Reporting Compliance Concerns

If you think a law, policy, or our Standards of Conduct is not being followed, you must report it to our Compliance Department. You should also report it to your LMH point of contact. If you feel uncomfortable talking to your LMH point of contact, voice your concern to the next supervisory level, up to and including the highest level of management. In following our cultural belief of Speak Up, LMH Health encourages open and honest discussion of issues with management. We are committed to providing an environment that allows reporting in good faith without fear of retaliation.

You can report compliance concerns to the Compliance Department in one of the following ways:

Contact the Compliance Officer directly by calling 785-505-4905

Email your concern to compliance@lmh.org

Call the Compliance and Privacy 24-hour Hotline at 877-474-1363

Fraud, Waste, and Abuse

Fraud, Waste and Abuse

Fraud

Fraud is an intentional deception or misrepresentation that the individual knows to be false or does not believe to be true, and makes knowing that the deception could result in some unauthorized benefit to himself/herself or some other person.

Waste

Waste is the extravagant, careless, or needless expenditure of funds or consumption of property that results from deficient practices, system controls, and wrong decisions.

Abuse

Abuse describes provider practices that are inconsistent with generally accepted business or medical practices and that result in an unnecessary cost to the Medicare program or in the reimbursement for goods or services that are not medically necessary or that fail to meet professionally recognized standards for health care/ or recipient practices that result in unnecessary cost to the Medicare program.

Abuse

Many times abuse appears quite similar to fraud except that it is not possible to establish that abusive acts were committed knowingly, willfully, and intentionally. Although these types of practices may initially be categorized as abusive in nature, under certain circumstances they may develop into fraud if there is evidence that the subject was knowingly and willfully conducting an abusive practice.

FWA in our Healthcare System

The National Healthcare Anti-fraud Association (NHCAA) cites an average of 3 percent (at the low end) and 10 percent (at the high end) of healthcare spending is lost due to fraud. That's between $67 Billion and $230 Billion lost each year to fraud, waste or abuse. That estimates to between $184 million and $630 million dollar loss per day, and this number is expected to increase every year as healthcare costs rise.*

Healthcare fraud is believed to be the second largest white-collar crime in the United States. It is often mistaken for a victimless crime, but it affects everyone. Fraud causes insurance premiums to rise, and victims may be put through unnecessary or unsafe procedures. Victims of identity theft may find their insurance information used to submit false claims. This is a staggering cost, and we are committed to battling these unnecessary expenditures every step of the way.

* The National Healthcare Anti-fraud Association (NHCAA). "Anti-Fraud Resource, Consumer Info & Action"; available at: http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=ConsumerAndActionInfo

Types of Fraud, Waste, and Abuse

Examples of fraud committed by beneficiaries may include:

- Identify theft
- Resale of drugs on the black market
- Falsely reporting loss or theft of drugs to receive replacements
- Doctor shopping
- False and inaccurate information to Medicare/Medicaid

Beneficiary Fraud

Fraud can be found in some day-to-day operations within any medical practice. Some forms of fraud may include:

- Billing for items or services not rendered or not provided
- Submitting claims for equipment or supplies and services that are not reasonable and necessary
- Double billing resulting in duplicate payments
- Unbundling
- Failure to properly code using coding modifiers or up-coding the level of service provided, inappropriate use of place of service codes
- Altering medical records
- Kickbacks

Provider Fraud

Fraud committed by a PBM may include:

- Unlawful remuneration in order to steer a beneficiary toward a certain plan or drug, or for formulary placement
- Not offering a beneficiary the negotiated price of a drug

Pharmacy Benefit Manager (PBM) Fraud

Fraud committed by a PBM may include:

- Forgery: bogus prescriptions, bogus invoices
- No prescription - phantom billings
- Altering prescriptions (+ Drugs, Quantity, Refills)
- Shorting quantity dispensed with full billings
- IOU - partial fills for full billings
- Over billed quantities
- Billing one drug and dispensing another
- Overstating cost or billing for a commercially available product when compounding the product (e.g., inhalation drugs)
- Dispensing samples or expired drugs
- Using a single dose vial for multiple prescriptions and billings
- Returns to stock not credited
- Authorized refills billed but not dispensed
- Ignoring payer of last resort policy

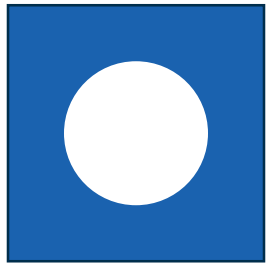
Pharmacy Fraud

Healthcare Fraud Laws and Regulations

False Claims Act
Fraud Enforcement & Recovery Act of 2009 (“FERA”)
Health Care Fraud Statute
Anti-Kickback Statute
Physician Self-Referral Prohibition Statute (“Stark Law”)

Fraud, Waste and Abuse Laws and Regulations

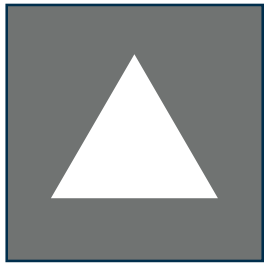
False Claims Act



Knowingly submitting a false or fraudulent claim to the government

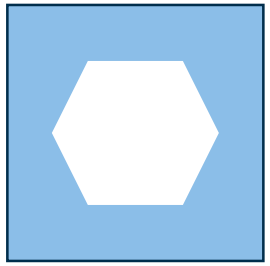
- Acting in deliberate ignorance of the truth
- Reckless disregard of the truth

Anti-Kickback Statute



Prohibits knowingly and willfully offering, paying, soliciting or receiving any remuneration to induce referrals of service reimbursable by a federal health care program

Stark Law



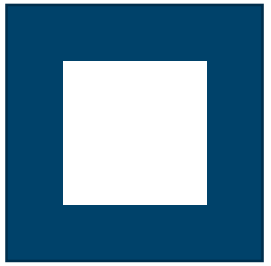
Prohibits physicians from referring Medicare beneficiaries for certain designated health services to an entity in which the physician or their immediate family member has an ownership/investment interest

Healthcare Fraud Statute

A person can be held liable for a scheme to intentionally

1. Defraud any healthcare benefit program
2. Use false statements to obtain funds held by a federal healthcare program

Fraud Enforcement & Recovery Act



Strengthened the enforcement of criminal and civil fraud laws to prevent and recover losses resulting from fraudulent activities

The False Claims Act

The False Claims Act (FCA) prohibits knowingly filing a false or fraudulent claim for payment to the government, knowingly using a false record or statement to obtain payment on a false or fraudulent claim paid by the government, or conspiring to defraud the government by getting a false or fraudulent claim allowed or paid. See 31 U.S.C. 3729(a) of the Act for additional details, exclusions, and statutory exceptions.

Administrative Remedies for False Claims

- Under 31USC §§ 3801-3812, federal agencies have the right for administrative recoveries. If a person submits a claim that the person knows or has reason to know is false or contains false information, or omits material information, then the agency receiving the claim may impose a penalty of up to $5,000 for each claim. The agency also may recover twice the amount of the claim.

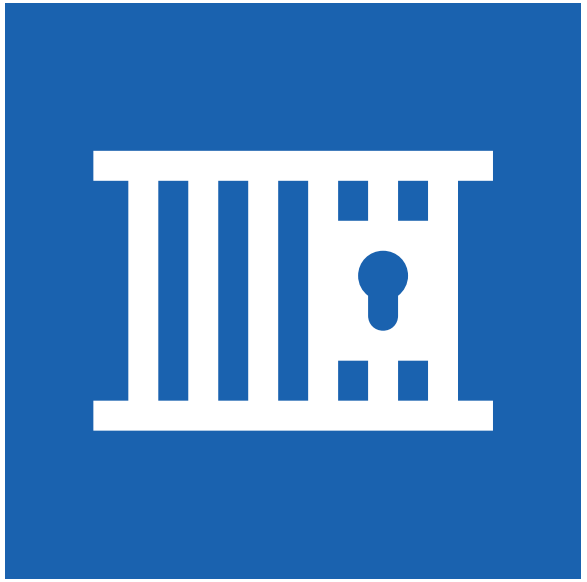
- Unlike the FCA, the determination of whether a claim is false, and the imposition of fines and penalties is made by the administrative agency, not by litigation through the federal court system. Also, unlike the FCA, a violation of this law occurs when a false claim is submitted, rather than when it is paid.

False Claims Act Examples

A person is in violation of the False Claims Act if they have:

1. Purposefully supplied false information on a application for a Medicare benefit or payment
2. Known about, but did not disclose, any event affecting the right to receive a benefit
3. Knowingly submitted a claim for a physician service that was not rendered by a physician
4. Supplied items or services and asked for, offered, or received a kickback, bribe, or rebate

False Claim Fines



Under the 42 U.S.C section 1320a-7b(a), if an individual participates in an activity above, they will be found guilty of a felony and upon conviction shall be fined a maximum of $50,000 per violation or imprisoned for up to five years per violation or both.

Kansas False Claims Act

The Kansas False Claims Act ("KFCA") is a civil statute that helps the state combat fraud and recover losses resulting from fraud in the Kansas Medicaid program. In addition, Kansas has a criminal statute, the Kansas Medicaid Fraud Control Act ("KMFCA"), which provides criminal sanctions in cases of Medicaid fraud. K.S.A § 75-7501.

Kansas False Claims Act Violations

Violations of the KCFA include, but are not limited to, the following:

- Knowingly presenting or causing to be presented to any employee, officer or agent of the state or political subdivision thereof or to any contractor, grantee or other recipient of state funds or funds of any political subdivision thereof, a false or fraudulent claim for payment or approval
- Knowingly making, using or causing to be made or used a false record or statement to get a false or fraudulent claim paid or approved
- Defrauding the State or any political subdivision thereof by getting a false claim allowed or paid by knowingly making, using or causing to be made or used, a false record or statement to conceal, avoid or decrease an obligation to pay or transmit money or property to the state or to any political subdivision thereof
- Having possession, custody or control of public property or money used or to be used by the state or any political subdivision thereof and knowingly delivering or causing to be delivered less property or money than the amount for which the person receives a certificate or receipt
- Being the beneficiary of an inadvertent submission of a false claim to any employee, officer or agent of the State or political subdivision thereof, or to any contractor, grantee or other recipient of the State funds or funds of any subdivision thereof, who subsequently discovers the falsity of the claim and fails to disclose the false claim
- conspiring to commit any violation of the above acts.

Penalties imposed for KFCA violations include actual damages, plus a fine of $1,000 to $10,000 per claim and treble

The Anti-Kickback Statute

The Anti-Kickback Statute prohibits the following actions: Soliciting or receiving, offering, paying remuneration for referrals of Medicare or Medicaid patients, or referrals for services or items which are paid for, in whole or in part, by Medicare or Medicaid. Soliciting or receiving, offering or paying remuneration in return for purchasing, leasing, ordering, or arranging for, or recommending purchasing, leasing, or ordering any goods, facility, service, or item for which payment may be made in whole or in part, by Medicare or Medicaid. Discounts, rebates, or other reductions in price may violate the anti-kickback statute because such arrangements induce the purchase of items or services payable by Medicare or Medicaid.

The statute ascribes criminal liability to parties on both sides of an impermissible "kickback" transaction. Violations are punishable by up to a fine of $25,000, imprisonment for up to 5 years, or both. However, certain arrangements are clearly permissible if they fall within a "safe harbor."

Remuneration

The transfer of anything of value, directly or indirectly, overtly or covertly in cash. When this happens, both parties are held in criminal liability of the impermissible “kickback” transaction.

Physician Self-Referral Prohibition

- The Physician Self-Referral Law, 42 U.S.C. Section 1395nn, commonly referred to as the "Stark Law."
- Prohibits physicians from referring Medicare patients for certain designated health services to an entity with which the physician or a member of the physician's immediate family has a financial relationship – unless an exception applies.
- Prohibits an entity from presenting or causing to be presented a bill or claim to anyone for a designated health service furnished as a result of a prohibited referral.
- Penalties: Penalties for physicians who violate the Stark Law may include fines, CMPs up to $24,478 (in 2018) for each service, repayment of claims, and potential exclusion from participation in the Federal health care programs

Stark Joint Venture Agreement

Under Arrangement Agreements

CMS finalized changes to the definition of "entity" that will prohibit physician ownership of entities that provide services to hospitals "under arrangements." Under the revised definition of "entity", a person or entity is considered to be furnishing DHS if the person or entity either "performs" the DHS or presents a claim or causes a claim to be presented to Medicare for the DHS.

Healthcare Fraud Statute

States that “whoever knowingly and willfully executes, or attempts to execute, a scheme to … defraud any health care benefit program … shall be fined … or imprisoned not more than 10 years, or both.”

Conviction under the statute does not require proof that the violator had knowledge of the law or specific intent to violate the law

Fraud Enforcement & Recovery Act of 2009

- Signed into law May 20, 2009 and amends the False Claims Act.
- Makes it illegal to “knowingly conceal or knowingly and improperly avoid” an obligation to repay federal funds that have been paid in error, even if the erroneous payment was not caused by the submission of a false record or statement.
- Expands the definition of “claim” to include:
  - Demands for payments made by subcontractors to companies receiving federal funds.
  - Any request for money made to any “recipient” of funds provided, in whole or in part, by the government, “to advance a Government program or interest.”

Exclusion Statute

The Department of Health and Human Services Office of Inspector General (OIG) is legally required to exclude from participation in all Federal Health Care programs individuals and entities convicted of the following types of criminal offenses:

- Medicare or Medicaid fraud
- Patient abuse or neglect
- Felony convictions for other health related fraud, theft, or other financial misconduct
- Felony convictions for unlawful manufacture, distribution, prescription or dispensing of controlled substances

The OIG has discretion to exclude on several other grounds, including misdemeanor convictions related to the list above.

Exclusion Statute

If a Provider is excluded by OIG from participation in Federal Health Care programs, then Medicare, Medicaid, TRICARE and/or VA will not pay for items or services furnished, ordered or prescribed by the excluded provider.

Excluded providers may not bill directly for treating Medicare and Medicaid patients, nor may their services be billed indirectly through an employer or a group practice.

The online database may be accessed at: http://oig.hhs.gov/fraud/exclusions.asp

The List of Excluded Individuals/Entities (OIG) contains just the exclusion actions taken by the OIG.

Corrective Action

Once Fraud, Waste, or Abuse has been detected, it must be promptly corrected. Correcting the problem saves the Government money and ensures compliance with CMS regulations.

To correct the Fraud, Waste, or Abuse, a corrective action plan will be developed. The actual plan will vary depending on the specific circumstances.

- Corrective Action must correct underlying problem that resulted in non-compliance
- Corrective Action will be tailored to address the particular FWA, problem, or deficiency
- Corrective Action will include consequences for failure of associates to implement the plan
- Corrective Action must contain a continuously monitor component to ensure effectiveness

HIPAA Privacy and Security

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), addresses the right to privacy for an individual patient's medical records.

Privacy Rule	Defines protected health information and provides individuals more control over how their health information is used and disclosed.
Security Rule	Establishes controls for safeguarding the integrity, availability and confidentiality of private information. The Office for Civil Rights is responsible for implementation and enforcement of the privacy and security regulations.

What is Protected

Patient information such as medical office patient charts, hospital records, radiographs, lab work and testing procedures are considered Protected Health Information (PHI). It also protects information that is maintained by a health care provider or health plan. HIPAA protects a patient's right to access and make changes to their PHI.

Protected information includes identification of a patient by name, social security number, birth date or address. It includes all data in a patient's medical record such as health status, diagnosis, treatment information and test results. Information relative to provisions for or payment of health care is also protected.

18 Identifiers of PHI

- Names
- Geographic subdivisions
- Elements of Dates (except for year)
- Phone Numbers
- Fax Numbers
- Electronic Mail Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate or License Numbers
- License Plates, Serial Numbers, or VINs
- Device Identifiers and Serial Numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) Addresses
- Biometric Identifiers (Fingerprints)
- Full Facial Photos / Identifying Photos
- Unique Numbers, Characteristics, Codes

Information that Contains PHI

- Encounter or Visit Documentation
- Lab Results
- Appointment Dates, Times, or Locations
- Invoices
- Radiology Reports and Images
- Images of Patients

Data Security

Safeguarding Protected Health Information (PHI) - A covered entity must have administrative, technical, and physical safeguards in place to protect the privacy of Protected Health Information from the intentional or unintentional use or disclosure.

Health Information Technology for Economic and Clinical Health

HITECH ACT of 2009

HITECH Act introduced several new security provisions including:

- Time frame requirement to notify members and Health and Human Services (HHS) of Protected Health Information (PHI) security breaches;
- New stricter HIPAA regulations regarding business associates and enforcement of penalties;
- Restrictions on the sale and marketing of PHI;

Health Information Technology for Economic and Clinical Health

HITECH ACT of 2009

When a breach occurs, a covered entity must notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been breached, accessed, acquired, used or disclosed as a result of such breach. A covered entity must notify HHS and the media in the event of a breach of unsecured PHI involving 500 or more individuals. A business associate must notify the covered entity of any breach of unsecured PHI.

Violation of PHI and PHI Breach Disclosures

For knowingly obtaining or disclosing identifiable health information relating to an individual in violation of the Rule:

- Up to $50,000 & 1 year imprisonment
- Up to $100,000 & 5 years if done under false pretenses
- Up to $250,000 & 10 years if intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm

LMH Health must notify the Secretary of Health and Human Services of all unauthorized disclosures of PHI; and follow the required process of notification to the individual, client, business associate and when indicated, the media.

Permitted Uses and Disclosures

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- "Incident to"
- Limited data sets
- As authorized by the individual

Information Blocking

Information Blocking noun

\ in-fər-ˈmā-shən \ ˈbläk ēŋ \

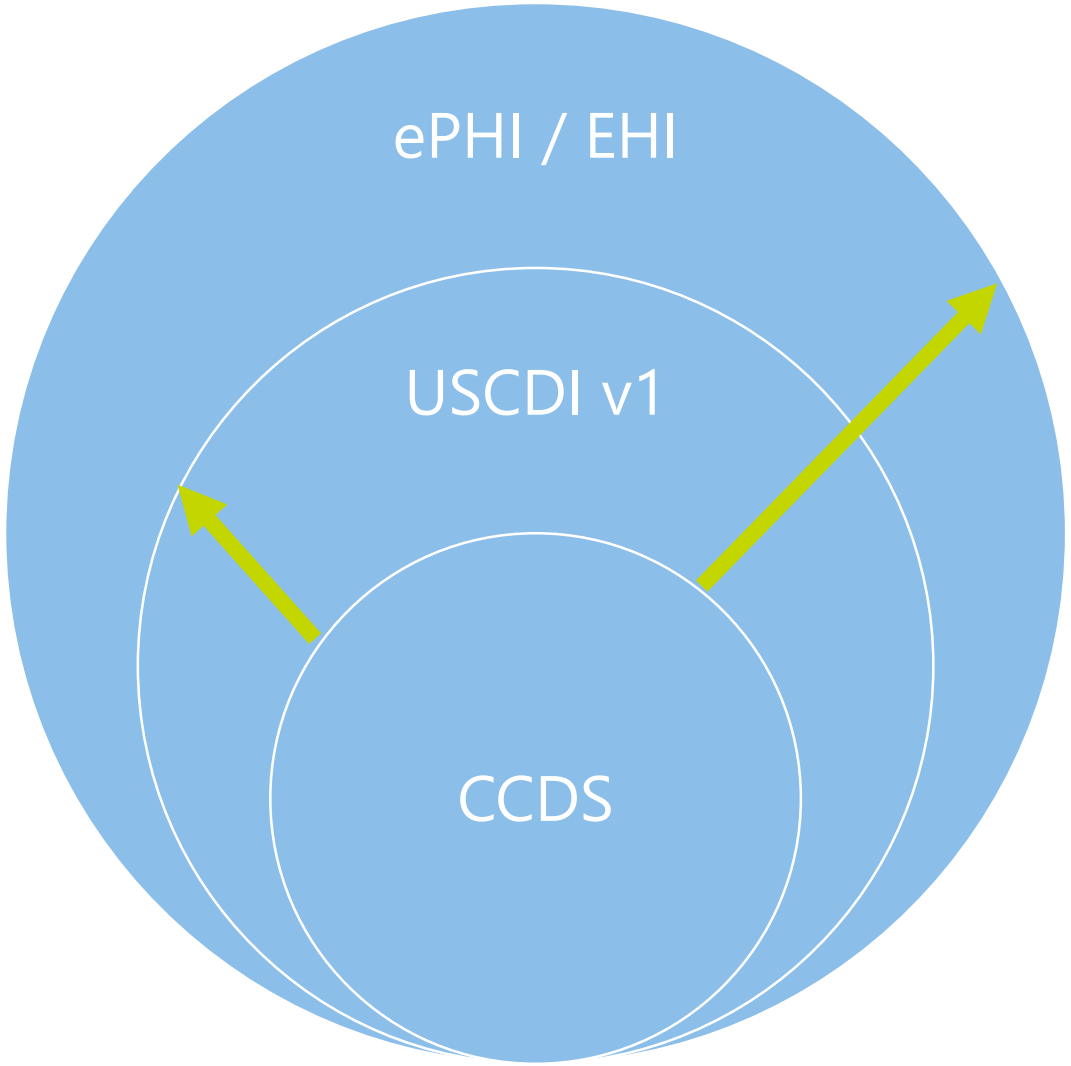
1. a. : Found in the 21st Century Cures Act § 4004
2. a. : A practice that is likely to interfere with, prevent, or materially discourage the access, exchange, or use of Electronic Health Information (EHI) unless required by law or specified by the Secretary pursuant to rulemaking and;
   b. : If conducted by an HIT Developer, Health Information Exchange, or Health Information Network, and such developer, exchange or network knows or should have known, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of Electronic Health Information; or
   c. : If conducted by a health care provider and such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage the access, exchange, or use of Electronic Health Information

Who Is Subject to Information Blocking Provisions

Actors

- Health Care Providers (includes LTPAC and Behavioral Health)
- HIT Developers (CEHRT and Non-CEHRT)
- Health Information Exchanges (HIEs)
- Health Information Networks (HINs) (this could include population health solutions for sharing patient information)

Scope of Data under Information Blocking



EHI is electronic protected health information (ePHI) under HIPAA to the extent the EHI would be included in a designated record set (DSR) as defined by HIPAA, regardless of whether the group of records are used or maintained by or for a covered entity under HIPAA, but EHI shall not include:

1. Psychotherapy notes as defined by HIPAA's individual right of access; or
2. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

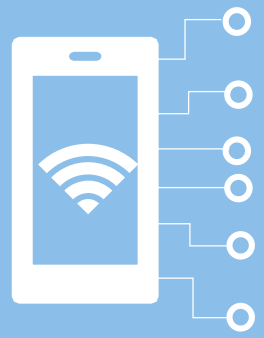
Exceptions

EXCEPTIONS TO INFORMATION BLOCKING

8

EXCEPTIONS THAT INVOLVE

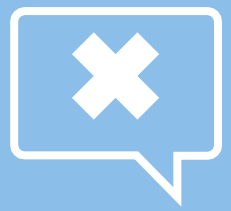
Not fulfilling requests to access, exchange, or use EHI



HEALTH IT PERFORMANCE

SECURITY

PREVENTING HARM



INFEASIBILITY

PRIVACY

EXCEPTIONS THAT INVOLVE

Procedures for fulfilling requests to access, exchange, or use EHI

LICENSING

COSTS

CONTENT AND MANNER

EXCEPTIONS THAT INVOLVE

Not fulfilling requests to access, exchange, or use EHI

PREVENTING HARM

1

- Must have reasonable belief the practice will substantially reduce the risk of harm to a patient or another person and must make the practice no broader than necessary.
- The risk of harm must:
  - Arise from data that is known/reasonable believe to be misidentified/mismatched, corrupt due to technical failure, or otherwise erroneous; OR
  - An individual determination based in the exercise of professional judgement by a licensed health care professional who has a relationship with the patient
- The type of harm must be one that could serve as grounds for a Covered Entity to deny access to an individual's PHI under 45 CFR 164.524(a)(3)(i), (ii), or (iii) – HIPAA's Right of Denial to Individuals on Reviewable Grounds
- Must be based on organizational policy should that is in writing, based clinical, technical and other expertise, and nondiscriminatory or based on the individual facts and circumstances of the request known at the time
- Actor must comply with the patient's right to request review of the circumstances of denial under 164.524(a)(4r

EXCEPTIONS THAT INVOLVE

Not fulfilling requests to access, exchange, or use EHI

PRIVACY

2

- Pre-Condition is not satisfied:
  - Must be based on a written organizational policy or documented on a case by case basis
  - Should attempt to obtain consent from an individual when it is a precondition
  - When operating in multiple places with multiple laws, a policy geared toward the most restrictive can be used across the organization
- When the actor is a HIT Developer of Certified HIT that is not covered by the HIPAA privacy rule
- Denial of an individual's right of to EHI in compliance with 45 CFR 164.524(a)(1) or (2)
  - These are exceptions to what an individual has a right to under HIPAA and denials of information requests that cannot be reviewed
  - Denial of information requests that can be reviewed are under the Prevention of harm exception
- Respecting an individual's request not to share information
  - Must be documented
  - Can be terminated by the individual or the actor

EXCEPTIONS THAT INVOLVE

Not fulfilling requests to access, exchange, or use EHI

SECURITY

3

- Must be directly related to safeguarding the confidentiality, integrity, and availability of EHI
- Must be tailored to the specific security risk being addressed
- Must be implemented in a consistent and non-discriminatory manner
- Exception must be based on
  - A written organizational security policy, aligned with applicable consensus based standards, with objective timeframes, and based on an assessment of the organization; OR
  - A fact specific determination of the request that the denial is necessary to mitigate a security risk to EHI and there are no reasonable and appropriate alternatives to denial that would mitigate the security risk and provide access, exchange, or use of EHI

EXCEPTIONS THAT INVOLVE

Not fulfilling requests to access, exchange, or use EHI

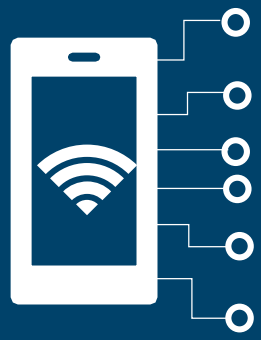
INFEASIBILITY

4

- Uncontrollable Events
  - Natural or man-made disaster, public health emergency, public safety incident, war, terrorist attack, strike or labor unrest, telecommunication or internet service interruption
- Segmentation
  - Cannot unambiguously segment the requested EHI from EHI that cannot be made available because of: privacy restrictions, individual request, or prevention of harm
- Infeasibility under the Circumstances
  - Must consider: the type of EHI and the requested purposes; the cost to the actor of complying with the request in the manner requested; the financial and technical resources available to the actor; whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of electronic health information to persons with whom it has a business relationship; whether the actor owns or has control over the technology, platform, HIE, or HIN through which EHI is accessed or exchanged; and why unable to provide access, exchange, or use of EHI consistent with the content and manner exception
- Actors must respond in writing in 10 business days with reasons for infeasibility

EXCEPTIONS THAT INVOLVE

Not fulfilling requests to access, exchange, or use EHI



HEALTH IT PERFORMANCE

5

- Maintenance and Improvements of HIT
  - Planned and Unplanned downtime, for no longer than necessary, that meets service level agreements
- Assured Level of Performance
  - Allows an actor to take action against a third-party application negatively impacting HIT performance
- Practices that Prevent Harm
  - If initiated in response to risk of patient harm, must meet Patient Harm Exception
- Security Related Practices
  - If initiated in response to a security risk, must meet the Security exception

CONTENT AND MANNER

6

EXCEPTIONS THAT INVOLVE

Procedures for fulfilling requests to access, exchange, or use EHI

- Content (The What)
  - Any EHI can be requested
  - EHI is limited to USCDI for first 18 months of compliance with Information Blocking
- Manner (The How)
  - Manner Requested – Does not need to meet Cost and Licensing Exceptions
  - Alternate Manner – Without undue delay
    - Does need to meet the Cost and Licensing Exceptions
    - Outlines priority of how to offer an alternative manner
      1. CHIT/CEHRT,
      2. Nationally accepted content and transport standards, or
      3. Alternative machine-readable format including the means to interpret
  - Based in technical ability to perform and agreement on the request

COSTS

7

EXCEPTIONS THAT INVOLVE

Procedures for fulfilling requests to access, exchange, or use EHI

- Acceptable Fees (including reasonable profit)
  - Based on objective and verifiable criteria and uniformly applied
  - Reasonably related to the costs of providing access, exchange, or use as requested
  - Reasonably allocated among similarly situated technology
  - Based on costs not otherwise recovered for the same instance of service to a provider and a third-party
- Fees should not be based on
  - Services to a competitor
  - Sales, profit, or revenue others may derive from the service
  - Costs for non-standard design or implementation
  - Opportunity costs
  - Costs related to royalties for use of IP (Licensing exception)
- Costs Specifically Excluded
  - Fee prohibited by HIPAA's individual right of access or based on patient access through internet based services
  - A fee to export or convert EHI from an EHR that was not agreed to in writing when the EHR was acquired
  - Use of EHI Export functionality certified under 170.315(b)(10)

LICENSING

8

EXCEPTIONS THAT INVOLVE

Procedures for fulfilling requests to access, exchange, or use EHI

- **Must** enter negotiations within 10 business day and close them in 30 business days
- Conditions the license must meet
  - License must provide rights necessary to enable and achieve intended access, exchange, or use
  - Allowed to charge a reasonable royalty for IP that was not already covered under the Fees exception
  - License terms cannot discriminate against competitors or potential competitors
  - Allows for limited Non-Disclosure Agreement (NDA) of trade secrets/IP
  - Restricts terms that would create additional fees outside the Fee exception, require a non-compete, or require the requestor or third-party to turn over related IP or provide additional services
- Additional Requirements
  - Must apply licensing in a non-discriminatory manner
  - Cannot “Break” compatibility or degrade performance after licensing
  - If HIT Vendor is a developer of CHIT, must meet Conditions of Certification

Your Responsibilities

You Responsibilities

Everyone plays a vital part in preventing, detecting, and reporting potential compliance violations.

1. **You must comply with all applicable statutory, regulatory, or other Medicare requirements, including following the Compliance Program**
2. **You have a duty to report any compliance concerns and suspected or actual violations of which you are aware**
3. **You have a duty to follow the Code of Conduct that articulates the standards of conduct and ethical rules of behavior**

Fraud, Waste, and Abuse Prevention

- Look for suspicious activity
- Conduct yourself in an ethical manner
- Ensure accurate and timely data and billing
- Ensure coordination with payers
- Know Fraud, Waste, and Abuse policies and procedures, standards of conduct, laws, regulations, and CMS guidance
- Verify all information received

Whistleblower Protection

Whistleblowers who file a False Claims Act lawsuit or report a compliance concern are protected and may not be:

- Discharged
- Demoted
- Suspended
- Threatened
- Harassed
- Discriminated against as a result of reporting fraud or abuse

Whistleblower Protection

Qui Tam Actions

The FCA contains whistleblower or qui tam provisions that allow individuals who become aware of fraud against the government to sue on behalf of the government. A person who brings a qui tam action that a court later finds was frivolous may be liable for fines, attorney fees and other expenses.

Non-Retaliation

LMH Health does not retaliate against any employee or entity that reports suspected fraudulent insurance activities. LMH Health ensures that identities are protected for individuals reporting in good faith alleged acts of fraud and abuse.

Reporting Compliance Concerns

If you think a law, policy, or our Standards of Conduct is not being followed, you must report it to our Compliance Department. You should also report it to your LMH point of contact. If you feel uncomfortable talking to your LMH point of contact, voice your concern to the next supervisory level, up to and including the highest level of management. In following our cultural belief of Speak Up, LMH Health encourages open and honest discussion of issues with management. We are committed to providing an environment that allows reporting in good faith without fear of retaliation.

You can report compliance concerns to the Compliance Department in one of the following ways:

Contact the Compliance Officer directly by calling 785-505-4905

Email your concern to compliance@lmh.org

Call the Compliance and Privacy 24-hour Hotline at 877-474-1363

Penalties for Violating Medicare Civil Monetary Penalties

42 USC § 1320a-7a

Penalties range from $10,000 to $50,000 per violation and includes exclusion from the Medicare program for a minimum of five years or more, these are:

- Presenting a claim that the person knows or should know is for an item or service that was not provided or is false or fraudulent or for which payment may not be made.
- Making false statements or misrepresentations on application or contracts to participate in Federal Health Care programs.
- Violation of the Medicare assignment provisions
- Violation of a Medicare physician or supplier agreement
- Violation of assignment requirement for certain diagnostic clinical laboratory tests
- Violation of requirement of assignment for nurse-anesthetist services
- Refusal of any supplier to provide rental Durable Medical Equipment (DME) supplies without charge after rental payments may no longer be made
- Physician billing for assistants at a cataract surgery without prior approval of the Quality Improvement Organization (QIO)
- Hospital unbundling of outpatient surgery costs
- Hospital and responsible physician "dumping of patients" based upon their inability to pay, or lack of resources.
- False or misleading information expected to influence a discharge decision
- Violations of the Anti-Kickback statute and/or Stark Law.

Resources

Resources

- Centers for Medicare and Medicaid Services (CMS) (www.cms.hhs.gov)
- Medicare Managed Care Manual and Medicare Prescription Drug Benefit Manual (www.cms.hhs.gov/Manuals/IOM)
- CMS Prescription Drug Manual – Chapter 9 (http://www.cms.gov/manuals/downloads/Pub100_18.pdf)
- Fraud & Abuse General Information (www.cms.hhs.gov/MDFraudAbuseGenInfo)
- Office of Inspector General (OIG) (www.oig.gov)
- Physician Self Referral Law (www.cms.hhs.gov/PhysicianSelfReferral)
- Social Security Administration (www.ssa.gov/oig/guidelin.htm)
- Office of Inspector General Department of Health and Human Services (http://oig.hhs.gov)
- HIPAA (http://www.hhs.gov/ocr/privacy)