ANNUAL COMPLIANCE & HIPAA REFRESHER TRAINING

Riverwood Center

Overview of Medicaid Program Administration for Behavioral Health Services

The Medicaid Program is funded by both the federal & state governments & is directly administered by the states with approval & oversight by the Centers for Medicare & Medicaid Services (CMS)

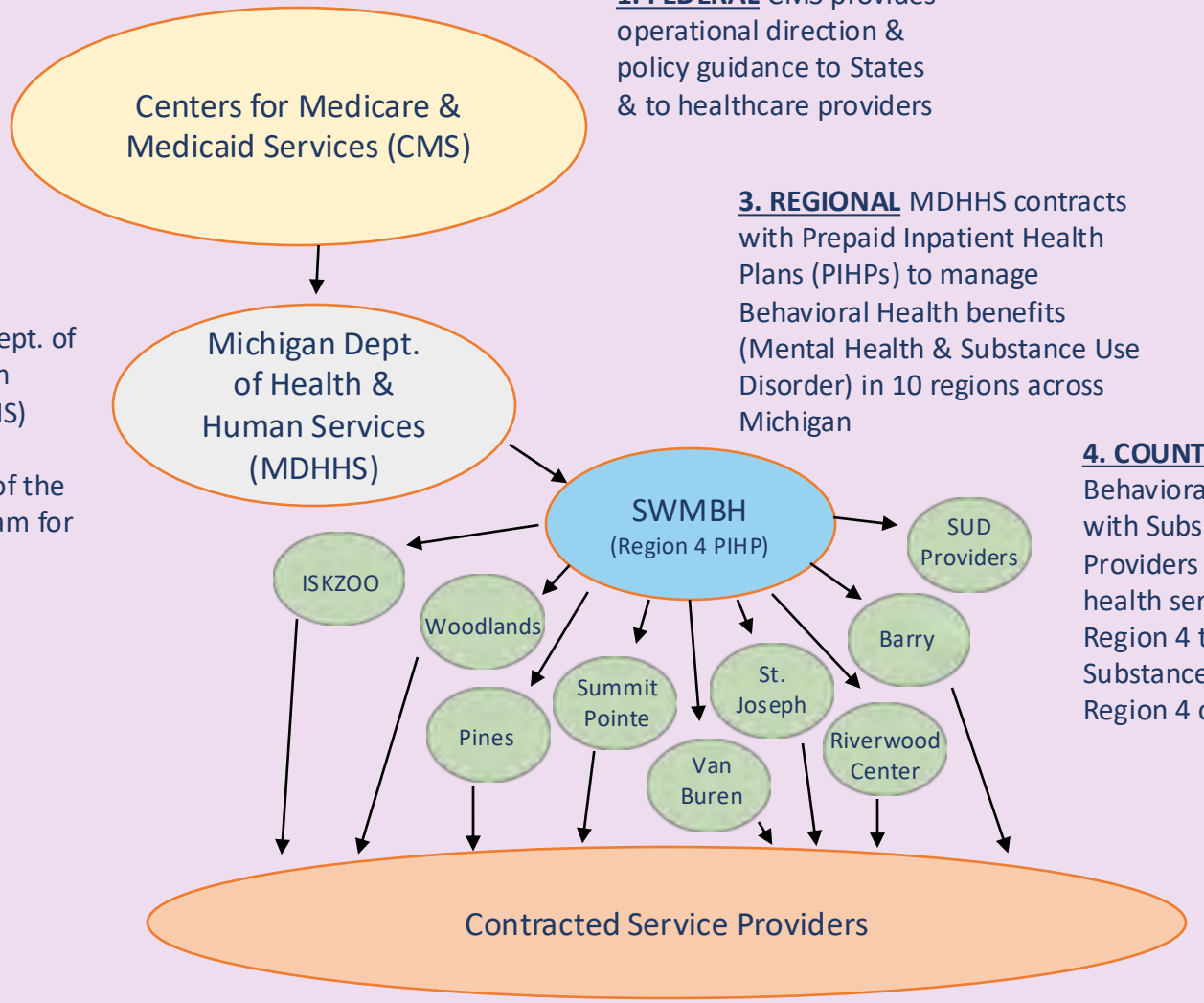
1. FEDERAL CMS provides operational direction & policy guidance to States & to healthcare providers

2. STATE
The Michigan Dept. of Health & Human Services (MDHHS) oversees the administration of the Medicaid Program for Michigan

3. REGIONAL MDHHS contracts with Prepaid Inpatient Health Plans (PIHPs) to manage Behavioral Health benefits (Mental Health & Substance Use Disorder) in 10 regions across Michigan

4. COUNTY Southwest Michigan Behavioral Health (SWMBH) contracts with Substance Use Disorder (SUD) Providers & with each community mental health service provider (CMHSP) in Region 4 to provide Mental Health & Substance Use Disorder services to Region 4 consumers

5. LOCAL Each CMHSP contracts with various service providers to provide mental health services to the consumers located in that CMHSP's county



What is Healthcare Compliance?

Doing the Right Thing!

- Conducting yourself in an honest & responsible manner
- Adhering to ethical standards & your agency's Code of Conduct
- Following the laws & rules that govern healthcare
- Preventing, detecting & reporting Fraud, Waste & Abuse (FWA) of federal & state funds
- Preventing, detecting & reporting unethical & illegal conduct
- Ensuring funds are used appropriately
- **Everyone** has a responsibility to report suspected non-compliance

Why is Healthcare Compliance Important?

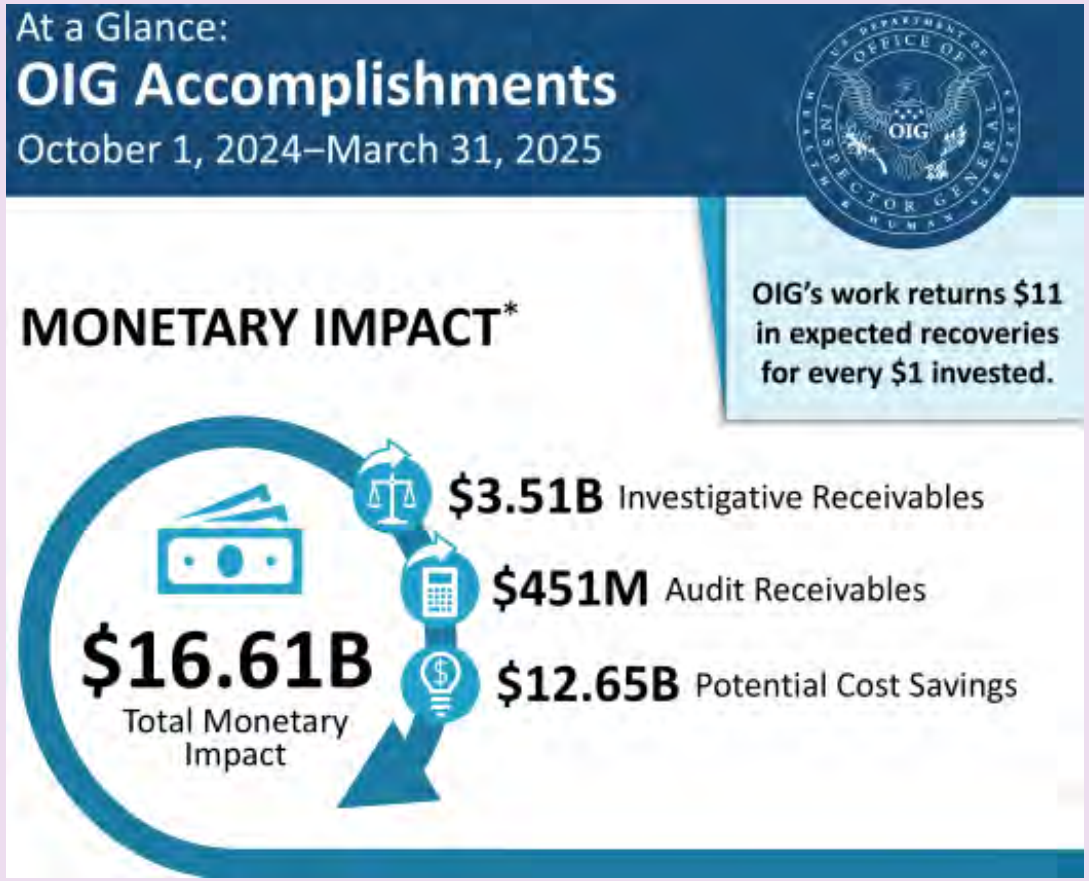
- Each year, billions of dollars are lost due to Fraud, Waste & Abuse (FWA) in the healthcare system
- FWA increases the financial strain on Medicaid & Medicare programs & could result in harm to consumers & less money for everyone
- FWA divert dollars that could otherwise be spent to safeguard the health & welfare of beneficiaries.
- Prosecuting healthcare fraud continues to be a top priority for the Dept. of Justice (DOJ) & Dept. of Health & Human Services (HHS), Office of Inspector General (OIG)
- The OIG's mission is to protect the integrity of HHS programs & the health & welfare of the people they serve

Why is Healthcare Compliance Important?

- Ensures compliance with federal & state laws, policies & procedures & ethical standards
- Promotes an organizational culture that encourages ethical conduct & commitment to compliance with the law
- Helps prevent & detect Fraud, Waste & Abuse of federal & state funds
- Ensures funds are used appropriately
- Identifies potential areas of vulnerability to help minimize risk
- Demonstrates agency commitment to honest & responsible conduct

Office of Inspector General (OIG) Enforcement

Spring 2025 Semiannual Report to Congress for 10/01/24 – 3/31/25



Total Monetary Impact: The total amount of potential savings from investigative receivables, audit receivables, and recommendations that funds be put to better use.

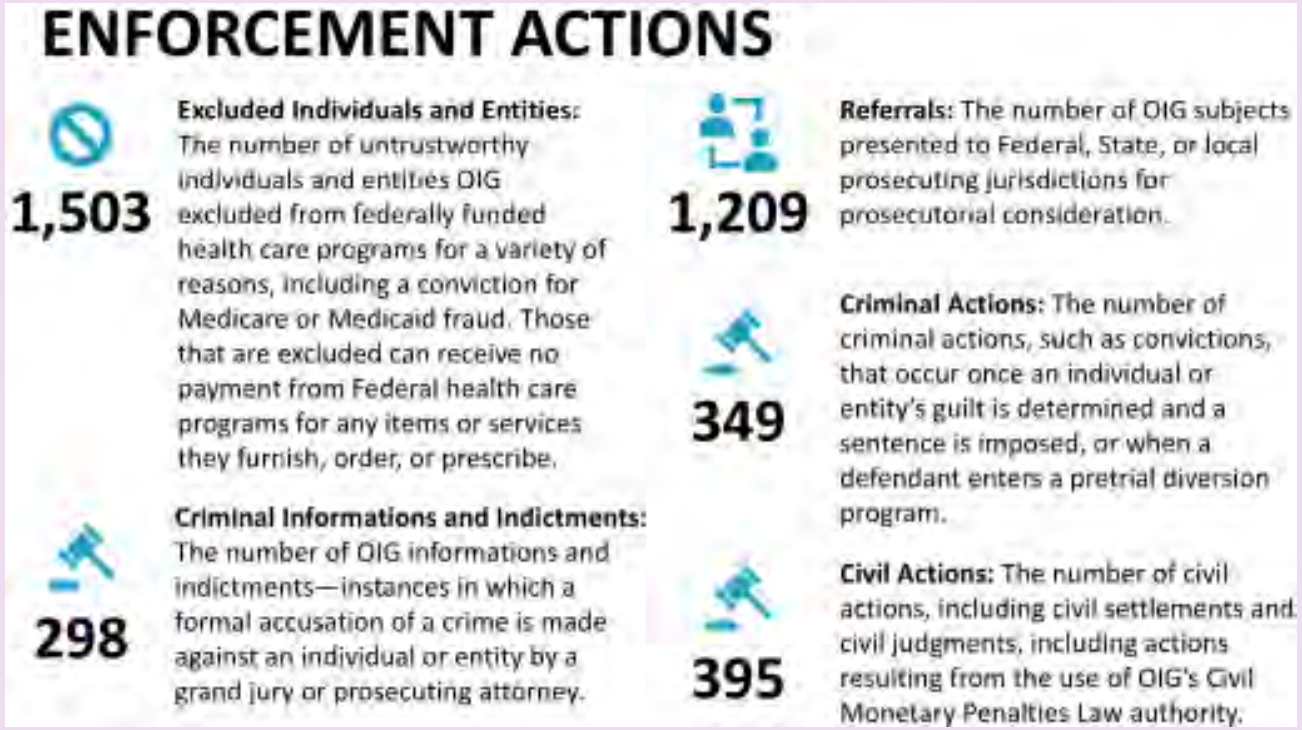
Investigative Receivables: The monies ordered or agreed upon to be returned or paid to HHS or other Federal and State entities or private individuals because of OIG investigative activity that led to criminal actions, civil and administrative settlements, civil judgments, or administrative actions. It does not reflect actual collections.

Audit Receivables: The monies identified through OIG audits that the audited entity has sustained or formally agreed should not be charged to the Government. It does not reflect actual collections.

Potential Cost Savings: Represents funds put to better use which are funds that HHS could use more efficiently if it took action to implement our recommendations.

Office of Inspector General (OIG) Enforcement

Spring 2025 Semiannual Report to Congress for 10/01/24 – 3/31/25



Recent Examples of Enforcement Action

8/25/25 – U.S. Attorney's Office, Eastern District of NC – Two former leaders of Life Touch LLC, a substance use treatment company pleaded guilty to their roles in a scheme to pay kickbacks to Medicaid patients. Their compliance director & office manager admitted to their roles in a scheme involving the payment of kickbacks to patients & tax violations

8/19/25 – U.S. Attorney's Office, Northern District of CA - American Psychiatric Centers, Inc. DBA Comprehensive Psychiatric Services agreed to pay $2.75 million to resolve allegations that they violated the False Claims Act by submitting false claims to the government for psychotherapy services

8/15/25 – State of Michigan – Saginaw physician who formerly operated PRN Urgent Care arraigned on 23 counts of Medicaid Fraud-False Claim for services billed to Medicaid that were never provided

Seven Core Elements of Compliance

Required by the Office of Inspector General (OIG)

1. Written code of conduct as well as policies & procedures that promote a commitment to compliance
2. Compliance Officer, Compliance Committee & high-level oversight
3. On-going education & training
4. Open lines of communication available for reporting issues
5. Enforcement of standards
6. On-going auditing & monitoring to identify risk areas
7. Prompt response to compliance issues & corrective action

Now, for a quick review of some of the important laws that impact Healthcare

Deficit Reduction Act (DRA) of 2005

- In 2006, President Bush signed into law provisions designed to reduce federal spending & improve oversight across a variety of government programs including Medicare & Medicaid. It includes provisions to eliminate Fraud, Waste & Abuse (FWA)
- Section 6032 requires healthcare providers who receive over $5 million in annual Medicaid payments to provide detailed information to employees including written policies on state & federal False Claims Acts, whistleblower provisions & other applicable laws
- It requires education & training for employees & contractors that contains detailed information on these laws as well as information about how to prevent & detect FWA in federal healthcare programs
- Failure to comply with these requirements may cause ineligibility to receive Medicaid payments

Anti-Kickback Statute

- Healthcare providers may not offer, pay, solicit or receive anything of value in exchange for the referral of consumers or services covered by Medicaid or Medicare
- Ensures healthcare decisions are based on medical necessity & not profit motives
- Punishable by prison time up to 10 years or fines up to $100,000 or both

Exclusion Authorities

- Healthcare providers must ensure no federal funds are used to pay for items or services furnished by an individual who is disbarred, suspended or excluded from participation in federal healthcare programs.
- The Office of Inspector General (OIG) has the authority to exclude certain individuals or entities from participation in federal healthcare programs. Fraud, abuse, neglect or unlawful distribution of controlled substances are examples of actions that could result in exclusions

Civil Monetary Penalties Law (CMPL)

- Allows the Office of Inspector General (OIG) to impose civil monetary penalties (fines) up to $100,000 or more for violations of the Anti-Kickback Statute & other violations including submitting false claims & making false statements on applications or contracts to participate in a federal healthcare program

Criminal Healthcare Fraud Statute

- Makes it a criminal offense to knowingly & willfully execute a scheme to defraud a healthcare benefit program or obtain money or property from a healthcare benefit program by false or fraudulent means
- Healthcare fraud is punishable by prison time up to 10 years & fines up to $250,000 (per individual) & fines up to $500,000 (per organization). Specific intent is not required for conviction

Federal False Claims Act (FCA)

- Federal law that imposes liability on individuals & organizations that knowingly submit false or fraudulent claims for payment to the government
- Establishes civil liability for certain acts, including:
  - Knowingly presenting a false or fraudulent claim to the government for payment
  - 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
  - Conspiring to defraud by getting a false or fraudulent claim allowed or paid
  - 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 government
- "Knowingly" means:
  - Actual knowledge of the information;
  - Acting in deliberate ignorance of the truth or falsity of the information; or
  - Acting in reckless disregard of the truth or falsity of the information
  - No proof of specific intent to defraud is required

Federal False Claims Act (FCA)

- The federal government has implemented measures to identify fraudulent practices among healthcare organizations
- The Federal False Claims Act was originally adopted by Congress in 1863 during the Civil War to discourage suppliers from overcharging the federal government
- Penalties for Violations:
  - Civil monetary penalties ranging from $13K - $27K (as of recent inflation adjustments) for each false claim
  - Treble damages – Up to 3x the amount of the government's actual losses related to the fraudulent or abusive conduct
  - Exclusions from participating in state & federal programs
  - Federal criminal enforcement for intentional participation in the submission of a false claim

What are some examples of things that would violate the False Claims Act (FCA)?

- Billing for services that were never provided to the consumer
- Billing for more time than what you spent (face-to-face) with the consumer (e.g., upcoding, padding times, rounding times)
- Billing for unnecessary services. Services must be medically necessary
- Billing for services performed by an excluded individual
- Improper documentation practices, such as:
  - Insufficient documentation (lacking detail)
  - Missing documentation
  - Submitting false documentation

"False documentation of care is not just bad patient care, it's illegal."

– Former HHS Secretary, Kathleen Sebelius & Former Attorney General, Eric Holder

Michigan False Claims Act (FCA)

- State law that makes it illegal to knowingly submit false or fraudulent claims to the Michigan Medicaid program
- Modeled after the federal False Claims Act, but applies specifically to state-funded Medicaid services
- “Knowingly” includes:
  - Actual knowledge
  - Deliberate ignorance of the truth
  - Reckless disregard of the truth
- Violations can result in civil penalties including fines of $5K - $15K per false claim + 3x damages incurred by the government, potential exclusion from Medicaid participation & additional administrative sanctions. Criminal penalties could bring felony conviction, prison time up to 10 years & fines up to $50K per offense

Whistleblowers Protection Act

- Designed to protect against the fraudulent use of public funds by encouraging people with knowledge of fraud to “blow the whistle” on wrongdoers
- Provides legal protection to employees who report violations or suspected violations of federal, state or local law, or participate in related investigations or actions
- Promotes transparency & accountability within organizations & government entities
- Employers may not discharge, threaten or discriminate against an employee regarding the employee’s compensation, terms, conditions, location, or privileges of employment
- Under the Michigan Whistleblower's Act, employers in violation could face civil fines up to $500

Review of Definitions - Fraud

- Intentional deception or misrepresentation made by a person with knowledge the deception or misrepresentation could result in benefit to said person or another person. Includes any act that constitutes fraud under applicable federal or state laws

- Examples include billing for services not provided, performing medically unnecessary services solely to obtain payment, altering documentation to obtain higher payment (upcoding), falsifying medical records to justify tests or treatments & deliberate duplicate billing

Review of Definitions - Waste

- Overutilization of services, or other practices that result in unnecessary cost to the payer. Generally, not considered to be caused by criminally negligent actions, but rather the misuse of resources

- Examples include healthcare spending that can be eliminated without reducing the quality of care, incurring unnecessary costs resulting from inefficient or ineffective practices, systems or controls, excessive tests or procedures, excessive prescriptions or conducting excessive visits

Review of Definitions - Abuse

- Practices that are inconsistent with sound fiscal, business or medical practices resulting in unnecessary cost to the payer, or in reimbursement for services that are not medically necessary or fail to meet professionally recognized standards of care

- Examples include submitting claims not in compliance with billing guidelines, misuse of billing codes, charging excessively for services or submitting bills to Medicare/Medicaid instead of the primary insurer

- Abuse can develop into fraud if there is evidence that the individual or organization knowingly & willfully (on purpose) conducted the abusive practices

Service Documentation Requirements

- The Michigan Medicaid Provider Manual, Section 14: Record Keeping states:
  - Providers must maintain, in English & in a legible manner, written or electronic records necessary to fully disclose & document the extent of services provided to beneficiaries
  - The clinical record must be sufficiently detailed to allow reconstruction of what transpired for each service billed. All documentation for services provided must be signed & dated by the rendering health care professional
- You have a responsibility to ensure that you bill accurately for the services you provide. All claims must be supported by complete & accurate documentation. ONLY bill for face-to-face services provided
- Supporting documentation should be unique to each date of service. Entries should not be duplicative (identical) for each day

Service Documentation Requirements

SWMBH Operating Policy 12.11, Section D (Progress Note Documentation) states:

- Progress note documentation must correspond to the member's IPOS/plan of care, including current status, progress toward specific goals & objectives addressed during the encounter & interventions offered by the clinician/staff during the encounter & shall include these mandatory elements (non-exhaustive list):
  - Customer's legal name
  - Service provided
  - Clinician/staff member providing the service/credentials (if applicable)
  - Other persons present during the service
  - Location or method of delivery (office, home, community, telephone)
  - Date of service
  - Start & stop time of the encounter
- Service documentation or progress notes must be completed & be part of the consumer record within a reasonable time period **after the deliver of the service & prior to the submission of the claim or encounter**

Error Protocol for Handwritten Documentation

- Proper error correction procedures should be used when an error is made on handwritten documentation

1. Draw a line through the entry
2. Make sure the inaccurate information is still legible
3. Write “error” by the incorrect entry & state the reason for the error in the margin or above the note
4. Sign/initial & date the entry
5. Document the correct information
6. If the error is in a narrative note, it may be necessary to enter the correct information on the next available line, documenting the current date & time & referring to the incorrect entry
7. Do not obliterate or otherwise alter the original entry by blacking out with marker, using whiteout or writing over the entry

- If documentation fails to clearly delineate the error correction process, a recoupment of funds may be sought

Additional Reminders

- For general rules for reporting & other helpful information regarding billing codes, code descriptions, provider qualifications, place of service (POS) codes & modifiers, please see the SFY 2025 Behavioral Health Code Sets, Charts & Provider Qualifications Document on the MDHHS website at https://www.michigan.gov/mdhhs/keep-mi-healthy/mentalhealth/reporting

- **As a provider billing for services, it is your responsibility to familiarize yourself with this document**

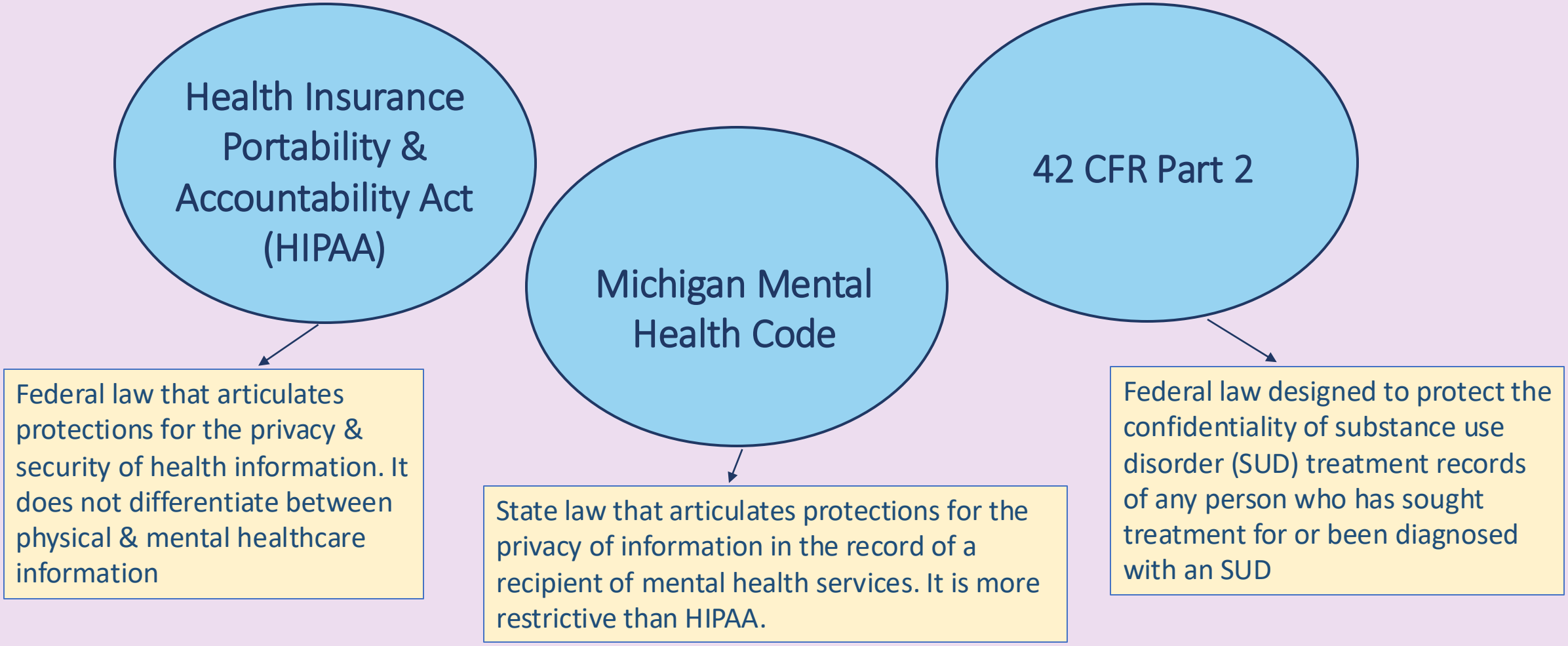
Enforcement Agencies

- Centers for Medicare & Medicaid Services (CMS) is a federal agency within the U.S. Dept. of Health & Human Services (HHS) that administers the Medicare & Medicaid programs
- Office of Inspector General (OIG) is an enforcement division of the federal HHS agency & of Michigan's Dept. of HHS
- Dept. of Justice (DOJ) is an enforcement agency in charge of criminal prosecution under applicable federal laws
- Michigan Attorney General (AG) investigates Fraud, Waste & Abuse (FWA) & prosecutes those who violate state law
- Audits of services provided to consumers are occurring at all levels

Consequences of Compliance Violations

- Civil & criminal actions brought on by law enforcement agencies
- Exclusions from participating in federal & state healthcare programs
- Penalties under the Civil Monetary Penalties Law (CMPL)
- Corporate Integrity Agreements (CIA) could be imposed
- Negative impact on service provider's reputation in the community
- Disciplinary action or termination of contract
- Reviews/audits at local, state & federal level
- Increased scrutiny
- Costly litigation/legal fees
- Recoupment of funds & Corrective Action Plans (CAP)

Privacy & Confidentiality – Three Governing Laws



Health Insurance Portability & Accountability Act (HIPAA)

- HIPAA is a federal law enacted by Congress in 1996 that provides data privacy & security provisions for safeguarding Protected Health Information (PHI)
- It gives consumers rights over their health information & limits who can look at & receive their health information
- Includes: Privacy Rule, Security Rule & Breach Notification Rule
- Applies to healthcare providers & their Business Associates
- **As individuals with access to consumer PHI, you must comply with HIPAA**

What is Protected Health Information (PHI)?

- Any individually identifiable health information transmitted or maintained in electronic, paper or oral format by a healthcare provider or its Business Associate (e.g., consumer name, address, DOB, SSN)

- Past, present or future physical or mental health condition & provision of healthcare provided to the individual

- It is any information that identifies the individual, or a reasonable assumption can be made as to the identity of the individual

HIPAA Privacy Rule

- HIPAA Privacy focuses on the rights of the individual & their ability to control their Protected Health Information (PHI)
- Healthcare providers **must** always protect PHI!
- Outlines what healthcare providers are required to do to protect PHI
- Defines how PHI can be used, distributed & shared
- HIPAA Privacy is the *overarching concept* that applies to **all** PHI. HIPAA Security is an aspect of HIPAA privacy, but it refers **specifically to the security of electronic PHI (ePHI)**

HIPAA Security Rule

- Healthcare providers must ensure the confidentiality, integrity & availability of **electronic PHI** (ePHI) such as ePHI sent via email or stored in an Electronic Health Record (EHR)
- Electronic systems that receive, maintain or send PHI **must** be secure
- Use e-mail encryption
- Avoid using free email platforms when conducting business
- Protect against threats or hazards
- Protect against anticipated misuse
- Keep an eye out for phishing scams & other hacking attempts
- Ensure workforce compliance
- Requires healthcare providers to have certain safeguards in place which include administrative, physical & technical safeguards

Security Threats in Healthcare

- Healthcare is a data goldmine. Criminals intent on selling data are ready to take advantage of & exploit vulnerabilities
- Examples of threats include, but are not limited to:
  - Malware/Ransomware/Hacking
  - Loss or theft of mobile devices
  - Email phishing attacks
- Things you can do as a user to help prevent cyber attacks:
  - Do not open or interact with suspicious emails/attachments
  - Report suspicious cyber activity to your IT Dept. immediately
  - Always keep electronic devices safe
  - Use complex passwords & two-factor authentication
  - **Think before you click! If you're unsure, ask!**

Security Threats in Healthcare

- Don’t fall victim to phishing scams & other cyberattacks!
- Phishing is a deceptive technique used to steal confidential information
- Scammers will try to trick you into providing personal or financial information
- General clues that an email isn’t legitimate to look for include:
  - Poor grammar, odd capitalization, spelling errors, odd sentence structure
  - Low-resolution logos – Scammers often cut & paste logos from banks or government agencies that will look fuzzy, indistinct or tiny
  - Emails demanding urgent action such as requests for login credentials, payment information or other sensitive information
  - Ask yourself is the email out of ordinary or unexpected
- Trust your gut! If it looks phishy, it probably is!

Health Insurance Portability & Accountability Act (HIPAA)

- HIPAA allows for the use or disclosure of Protected Health Information (PHI) for the purpose of TPO without consumer consent
- **T**reatment refers to various activities related to consumer care
- **P**ayment refers to various activities related to paying for or getting paid for healthcare services
- **O**perations refers to day-to-day activities of a healthcare provider such as planning, training, management, etc.

Michigan Mental Health Code

- "Information in the record of a recipient & other information acquired in the course of providing mental health services to a recipient, shall be kept confidential & shall not be open to public inspection…"
- Amended on April 10th, 2017, to allow for disclosure of PHI for Treatment, Payment & Coordination of care in accordance with HIPAA
- **Best practice** When in doubt, get a Release of Information signed!
- If you have questions, contact your agency's Compliance Officer or the CMHSP's Compliance Officer

Michigan Mental Health Code

- **Coordination of Care** includes activities designed to ensure needed, appropriate cost-effective care for consumers. As a component of overall care management, care coordination activities focus on ensuring timely information, communication & collaboration between those involved in the consumer's care
- Examples include care planning, linkage to community resources, monitoring, reporting & documentation, tracking & facilitating follow-up with lab tests & referrals & managing transition of care activities to support continuity of care

42 CFR Part 2 – Substance Use Disorder (SUD) Confidentiality

- A set of regulations the federal government implemented to protect the confidentiality of SUD treatment records of any person who has sought treatment for or been diagnosed with an SUD
- It applies to healthcare providers who provide SUD treatment
- There are very few exceptions when an SUD provider can say a person attends an SUD program
- Releases of information for SUD must include specific 42 CFR Part 2 language
- Modified on Feb. 8th, 2024, to bring it more in-line with HIPAA & HITECH

Need to Know Rule

- Protected Health Information (PHI) should only be accessed when necessary to perform your job duties
- PHI should never be accessed for any other reason other than to complete your job duties

Minimum Necessary Rule

- Reasonable efforts must be made to limit the use or disclosure of & requests for PHI to the minimum amount necessary to accomplish the intended purpose
- You must follow the minimum necessary rule when disclosing or requesting PHI

Protect consumer health information as if it was your own!

Breach Notification

- A breach occurs when there is an unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) that compromises the security or privacy of that information
- Depending on the circumstances, a breach may require notice to the consumer that their information was inappropriately released, mitigation efforts such as credit monitoring, notification to local media & notification to the Office for Civil Rights (OCR)
- Examples:
  - Documentation/laptop lost or stolen
  - Posting about a consumer on social media
  - Faxing documents containing PHI to the wrong place
  - Speaking to someone without a release of information in place
  - Emailing PHI to the wrong person

Consequences of a Breach

- Personal harm to the consumer if the breach results in fraud or identify theft
- Disclosure of the breach to the consumer, media & Office for Civil Rights (OCR)
- Civil monetary penalties (fines ranging from $100 to $50,000…up to $150,000 per violation)
- Loss of trust from the consumer & community
- Negative impact on service provider's reputation
- Diminished productivity & lost time
- Corrective Action Plans (CAP)
- Disciplinary action or termination of contract
- Costly litigation/legal fees

Protect Consumer PHI

Enforcement Responsibility

- The U.S. Dept. of Health & Human Services (HHS) Office of Civil Rights (OCR) is responsible for enforcing HIPAA
- The OCR may:
  - Investigate complaints filed
  - Conduct compliance reviews to determine if healthcare providers are complying with the law
  - Perform education & outreach to foster compliance with the requirements of the law
  - Work in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA

Recent Example of Enforcement Action

7/07/25 - The Office for Civil Rights (OCR) has agreed to settle alleged HIPAA violations with Texas based behavioral healthcare provider, Deer Oaks for two security incidents involving discharge summaries accidently exposed online due to a coding error & a Ransomware cyberattack that impacted 171,871 individuals

The Office for Civil Rights investigated & found Deer Oaks had failed to conduct a thorough & accurate assessment to identify risks & vulnerabilities

Deer Oaks was ordered to pay $225,000 & was given a Corrective Action Plan (CAP) which required them to complete annual risk assessments, update their IT/security policies & conduct workforce HIPAA training

HIPAA Enforcement Results as of October 31st, 2025

- Since the compliance date of the Privacy Rule in April 2003, the Office for Civil Rights (OCR) has received over 374,321 HIPAA complaints & has initiated 1,193 compliance reviews. They have resolved 99% of these cases (370,578)
- The compliance issues most often alleged in complaints are, compiled cumulatively, in order of frequency:
  - Impermissible uses & disclosures of PHI
  - Lack of safeguards of PHI
  - Lack of consumer access to their PHI
  - Lack of administrative safeguards of ePHI (electronic PHI)
  - Use or disclosure of more than the minimum necessary PHI
- As of October 31st, 2025, the OCR has settled or imposed a civil monetary penalty in 152 case resulting in a total dollar amount of $144,878,972

Reporting Responsibilities

- If you are aware of any type of Compliance or HIPAA violation including, but not limited to:
  - Fraud, Waste or Abuse (FWA)
  - Violation of Whistleblower provisions
  - Violation of HIPAA, 42 CFR Part 2 or Michigan Mental Health Code
  - Unethical or illegal conduct

It is your right & your responsibility to report it to your agency's Compliance Officer and/or the CMHSP's Compliance Officer.

You may not be intimidated, threatened, coerced, discriminated against or subjected to other retaliatory action for making a good faith report of an actual or suspected violation

Contact Information

If you have questions or concerns, please contact your agency's Compliance Dept. or Riverwood Center's Compliance Officer

Cynthia Bingaman	269.934.1632 or clb@riverwoodcenter.org
Anonymous Hotline	800.876.2501

Sources:

http://www.hhs.gov/ocr/office/index.html

https://docs.google.com/file/d/0BykanqtE5GqnOTdrbXRldTRvMFE/edit?pli=1

www.HealthIT.gov/mobiledevices

www.hipaasurvivalguide.com

www.oig.hhs.gov www.ahrg.gov

www.Michigan.gov/mdch/

www.dir.ca.gov/chswc/CAResearchColloquium/P5/StephanieTeleki.pdf

https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNGenInfo/index.html

www.cms.gov www.ncqa.org

iom.nationalacademies.org/ www.swmbh.org