HIPAA

Privacy and Security

HIPAA Topics Covered

- What is HIPAA?
- HIPAA Definitions
- Who Protects PHI?
- Consumer Rights
- Security
- Violations
- Release of Information
- Identity Verification
- Safeguarding Information
- Your Role
- Reporting Violations

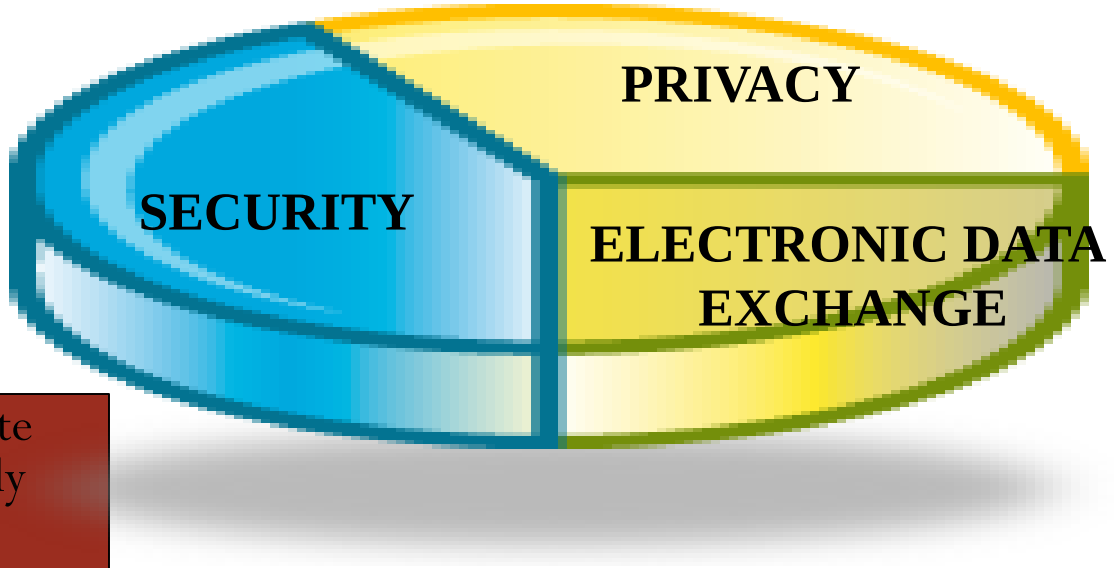
What is HIPAA?

- HIPAA is an acronym for the Health Insurance Portability & Accountability Act of 1996 (§45 C.F.R. Parts 160 & 164)
- Provides a framework for the establishment of a nationwide protection of participant confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

What is HIPAA?

- HIPAA Consists of three separate parts:

  1) Privacy, 2) Security, and 3) Electronic Data Exchange
- HIPAA mandates accountability



- Each part has separate regulations to comply with

Parts of HIPAA:
1. The Privacy Rule

- The Privacy Regulations went into effect April 14, 2003
- Privacy refers to the protection of an individual's health care data.
- Defines how participant information is used and disclosed.
- Gives individuals privacy rights and greater control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

Parts of HIPAA:
2. The Security Rule

- Security regulations went into effect April 21, 2005.
- Security means controlling:
  - The confidentiality of electronic Protected Health Information (ePHI).
  - How consumer data is electronically stored.
  - How participant data is electronically accessed.

Why Should SWMBH Comply With HIPAA?

- We must be committed to protecting our consumers' privacy.
- SWMBH is placing trust in you to follow the privacy policies. This is not an option, it is required.
- Choosing not to follow the Privacy and Security Rules and SWMBH policies:
  - Could put you at risk.
  - Could put SWMBH at risk.

HIPAA Regulations

- The HIPAA Regulations require we protect our consumers' PHI in all media including, but not limited to, PHI created, stored or transmitted in/on the following media:
  - **Verbal** discussions (i.e. in person, on the phone, etc.)
  - **Written** on paper (i.e. referral form, explanation of benefits, prescreen assessments, etc.)
  - In all of our **computer applications/systems** (i.e. Streamline SmartCare, Streamline Practice Management, Provider Access, Care Management, etc.)
  - In all of our **computer hardware/equipment** (i.e. PCs, laptops, PDAs, fax machines/servers, cell/multifunctional phones, etc.)

This training is designed to educate you on the importance of Privacy and Security

- It is everyone's responsibility to take the confidentiality of consumer information seriously. Anytime you come in contact with consumer information or any PHI that is written, spoken or electronically stored, YOU become involved with some facet of the Privacy and Security Regulations.

HIPAA Definitions

- What is Protected Health Information (PHI)?
- PHI is Individually Identifiable Health Information relating to information about:
  - Health/condition of an individual.
  - Payment for health care of an individual.
  - Reasonably identifies the individual (consumer identifiers/demographics).
    - Includes information by which the identity of a consumer can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.

Consumer Identifiers

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- License/Certification Numbers
- Vehicle Identifiers/Serial Numbers/License Plate Numbers
- Internet Protocol Addresses
- Health Plan Numbers
- Full face photographic images and any comparable images
- Web Universal Resource Locaters (URLs)
- Any dates related to any individual (date of birth)
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Biometric identifiers including finger and voice prints
- Any other unique identifying number, characteristic or code

HIPAA Definitions

- **Use**: when we review or use PHI internally (audits, training, customer service, quality improvement)
- **Disclose**: when we release or provide PHI to someone (i.e. attorney, a consumer, faxing records to a provider, etc.)

HIPAA Definitions

- What does releasing the "minimum necessary" PHI mean?
  - To use or disclose/release only the information minimally necessary to accomplish the intended purposes of the use, disclosure, or request.
  - Requests from employees within SWMBH:
    - Identify each workforce member who needs to access consumer PHI.
    - Limit the PHI provided to a "need to know" basis.
  - Requests from individuals not employed at SWMBH:
    - Limit the PHI provided to what is minimally necessary to accomplish the purpose for which the request was made.

HIPAA Definitions

- What is **TPO**?
- HIPAA allows us to **Use** and/or **Disclose** PHI for the purpose of:
  - **T**reatment – providing care to participants
  - **P**ayment – the provision of benefits and premium payment
  - **O**perations – normal business activities (reporting, quality improvement, training, auditing, customer service and resolution of grievances, eligibility checks, accreditation, etc.)
- These terms are collectively referred to as **TPO**
- PHI used outside of **TPO** is not allowed without a Release of Information form signed by the consumer/guardian
- **TPO** must be within the minimum necessary to perform the needed task

When Can Customer Information Be Disclosed?

- HIPAA allows some disclosures to be made without patient consent
  - Treatment, payment and health care operations
    - Specified in the SWMBH Privacy Notice
  - All other disclosures require patient authorization

  - However, the MI Mental Health Code has additional restrictions about the disclosure the patient information. SWMBH is obligated to follow the Mental Health Code restrictions on disclosing consumer information.

Mental Health Code

- Mental Health Code Confidentiality
  - §330.1748-general requirements and considerations
    - Information in the record of a recipient shall be kept confidential.
    - Information may be disclosed outside of the holder of the record only with customer authorization or under specific circumstances.
- Mental Health Code Confidentiality
  - §330.1748-general requirements and considerations
    - *Information in the record of a recipient shall be kept confidential.*
    - *Information may be disclosed outside of the holder of the record only with customer authorization or under specific circumstances.*
      - **Specific circumstances include**:
        - As necessary in order for the recipient to *apply* for or *receive* benefits
        - As necessary for the purpose of outside research, evaluation, accreditation, or statistical compilation. The individual who is the subject of the information shall not be identified in the disclosed information unless the identification is essential in order to achieve the purpose for which information is sought or if preventing the identification would clearly be impractical, but not if the subject of the information is likely to be harmed by the identification.
        - To a provider of mental or other health services or a public agency, if there is a compelling need for disclosure based upon a substantial probability of harm to the recipient or other individuals.

Consumer Rights: Access

- Consumers have the right to inspect and copy PHI.
- Situations where access may be denied or delayed:
  - Psychotherapy notes;
  - PHI compiled for civil, criminal or administrative action or proceedings;
  - PHI subject to CLIA Act of 1988 when access would be prohibited by law;
  - A correctional inmate's request may jeopardize health and safety of the inmate, other inmates or others at the correctional institution;
  - A research study has previously secured agreement from the individual to deny access;
  - Access is protected by the Federal Privacy Act;
  - PHI was obtained under the promise of confidentiality and access would reveal the source of the PHI.

Why Do We Need to Protect PHI?

- It's the law.
- To protect our reputation.
- To avoid potential withholding of federal Medicaid and Medicare funds.
- To build trust with or contracted providers and consumers.
  - If consumers feel that their PHI will be kept confidential, they will be more likely to share the information needed for the care.

Who Or What Protects PHI?

- The Federal Government through the HIPAA laws.
  - Civil penalties with four tiers of penalty amounts per violation for a maximum penalty amount of $1.5 million for all violations of an identical provision.
  - Criminal penalties:
    - $50,000 fine and 1 year prison **for knowingly obtaining and wrongfully sharing information.**
    - $100,000 fine and 5 years prison **for obtaining and disclosing through false pretenses.**
    - $250,000 fine and 10 years prison **for obtaining and disclosing for commercial advantage, personal gain or malicious harm.**
  - SWMBH through our Notices of Privacy Practices.
  - You by following our policies and procedures.

Enforcement

- **The public**: The public will be educated about their privacy rights and will not tolerate privacy violations.
- **Office For Civil Rights (OCR)**: This is the agency that enforces privacy and security regulations. They provide guidance and monitor for compliance through audits and investigating complaints.
- **Department of Justice (DOJ)**: This agency is involved in criminal privacy violations. May impose fines, penalties and imprisonment on offenders.

Consumer Rights: Alternative Communications

- Consumers have a right to request to receive communication by alternative means or location. Examples:
  - The consumer may request a bill be sent directly to him instead of to his insurance company.
  - The consumer may request we contact her on her cell phone instead of at her home telephone number.
    - (SWMBH Compliance Procedure: Request for Alternate Means or Location of Confidential Communication of Protected Health Information)

Consumer Rights: Special PHI Requests

- What should I do if a consumer requests we always call a family member instead of her?
  - Any consumer requesting permanent and special/unique calling and/or mailing instructions should be directed the Privacy Officer, to complete and sign a written request.
    - (SWMBH Compliance Procedure: Request for Alternate Means or Location of Confidential Communication of Protected Health Information)

Consumer Rights: Amendment Requests

- Consumers have the right to request an amendment or correct PHI.
  - Situations where a request may be denied:
    - SWMBH did not create the information.
    - The record is accurate according to the health care professional that created it.
    - Information is not part of the SWMBH consumer medical record.
  - A consumer states there is an error in his medical record and wants it corrected. What should I do?
    - Assist the consumer in completing the Request for Amendment/Correction of Health Information form and send it to the Privacy Officer (SWMBH Compliance Procedure: Customer Addendums)

Consumer Rights: Restrictions and AOD

- Consumers have a right to request a restriction on use and disclosure of their PHI (i.e. revoke a previous authorization, request to not give to certain providers, request to not provide for research purposes, etc.)
  - We are not required to approve the request but must make reasonable efforts to approve it when possible.
- Consumers have a right to an accounting of disclosures (AOD).
  - SWMBH must give information on disclosures of information released except those that were given to:
    - The consumer
    - TPO
    - Law enforcement officials, correction institutions or national security

Consumer Rights: AOD

- A consumer may request an accounting for disclosures as far back as six years before the time of the request.
- A covered entity must suspend accounting of disclosures to a consumer if an agency or law enforcement indicate the accounting is likely to impede the agency's activity.

Consumer Rights: NOPP

- What is the purpose of the Notice of Privacy Practices (NOPP)?
  - Summarizes how SWMBH may use and/or disclose the consumer's PHI.
  - Details the consumer's rights in respect to their PHI.
  - Participants must sign the Acknowledgment of Receipt of the NOPP before they see a provider for their first appointment.
  - Consumer signs the Acknowledgment of Receipt to confirm that they have been offered and/or received the NOPP.
  - If a consumer refuses to sign the Acknowledgment of Receipt of NOPP this should be noted on the form and filed in his/her medical record.

Consumer Rights: Privacy Complaints

- Consumers have the right to file a privacy complaint
- All requests or complaints regarding this right should be directed to the Privacy Officer:
  - Phone: 1-800-676-0423 dial option 5
  - SWMBH Confidential Hotline: 1-800-783-0914
  - Email: swmbhcompliance@swmbh.org
  - In writing: 5250 Lovers Lane
    Portage MI, 49002

Security

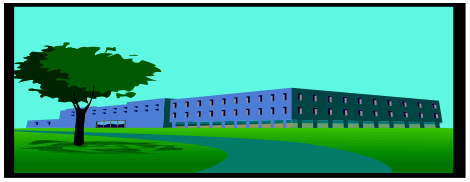
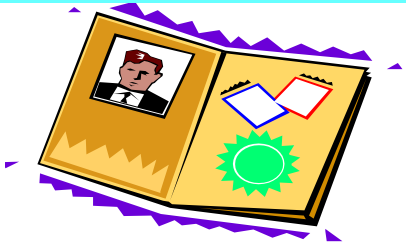
- One key element of protecting our consumers' PHI lies in maintaining the security of our systems, which house and transmit ePHI (electronic Protected Health Information).
- The HIPAA Security Rule outlines how we are to do this.
- How do we protect our computer systems and our consumers' information in them?
  - Administrative Safeguards
  - Technical Safeguards

Applying the Security Rule

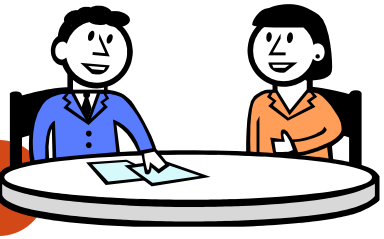
- Administrative Safeguards
  - SWMBH policies and procedures must be followed by all staff to maintain security (i.e. disaster recovery of computer systems, use of the internet, use of email, faxing, use of voicemail, computer hardware and software standards).
- Technical Safeguards
  - Many technical devices are needed to maintain security. Examples include varying levels of passwords, screen savers, data backups, disposal of media, encryption, audit trails. Computer and system processes are set up to protect, control and monitor information access.

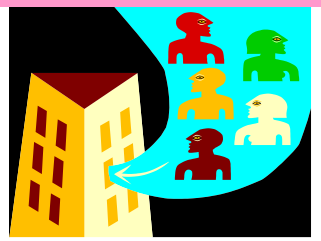
Applying the Security Rule

- **Physical Safeguards.** Many physical barriers and devices are needed to maintain security. Examples include installing locks on doors, securing buildings and rooms, identifying visitors, locking file cabinets to protect SWMBH's property and the health information.


- **Personnel Security.** SWMBH policies and procedures manage the assignment of access authority to employees and other workforce members. Procedures should address employee transfers, role changes and terminations. Effective security and privacy training must be conducted.





Access to ePHI: User Names and Passwords

- How do we control access to electronic Protected Health Information (ePHI) in our computer systems?
  - By requiring all users to utilize individually unique user names and passwords, we control access to the information in each of our computer systems and applications.
  - User names and passwords control what users are able to access and help us identify what information users accessed in our applications.
  - For these reasons, you may not share user names and passwords with anyone else.
  - When leaving your computer or workstation, ALWAYS:
    - Log off, OR
    - Lock the computer screen (Ctrl-Alt-Delete and select "lock")

Access to ePHI: User Names and Passwords

- Creating strong passwords
  - Follow SWMBH policy in terms of the number of required characters.
  - Use a combination of letters, numbers and symbols and capital and lower case letters.
  - Do not use passwords that can be easily guessed such as:
    - Names (spouse, children, pet, etc.)
    - Significant dates (birthdate, anniversary, etc.)
    - Favorite teams
    - Tip: use a "pass-phrase" to help you remember your password such as: MbdMi5yo (My black dog, Monte, is 5 years old)

Protect Your User Name and Password(s)

- Memorize your passwords. Don't post user names and passwords on your computer, notebook, tablet, under your keyboard, in an unlocked drawer, etc.
  - Secure any written user names and passwords in a locked location to prevent access to them by someone else.
- If you believe one of your user names or passwords has been compromised, request that it be changed.
  - If you think PHI may have been inappropriately accessed, discuss your concerns with the Privacy Officer.

What is Misuse of PHI?

- **Unauthorized**
  - Access to…
  - Using…
  - Taking…
  - Possession of…
  - Release of…
  - Edit of…
  - Destruction of…
    - Consumer PHI without authorization.

Privacy Violations

- Incorrect Consumer on a Form
  - Jane Doe's name, medical record number, and date of birth is placed on a medical record document and handed to June Smith. Is this considered a impermissible disclosure?
    - **Yes -** If June Smith reads Jane Doe's name on this form, or any other document, it is a breach of confidentiality.
  - Request June Smith return the incorrect document and forward it to the Privacy Officer.

Privacy Violations

- Incorrect Records Released
  - A consumer requested we send 2006 medical records to a provider. In addition to the 2006 records, we also release 2004 and 2005 records. Is this a impermissible disclosure?
    - **Yes** – This is a breach of confidentiality as more information than was requested by the consumer was released.
    - Always keep in mind we may only release the minimum necessary PHI to accomplish the purpose of the request – even when releasing to another treating provider, insurance company, etc.
      - Request the provider to return the 2004 and 2005 documents and forward them to Laura Ferrara the Privacy Officer.

Privacy Violations

- Incorrect Consumer Records Mailed
  - Medical records of one consumer are mailed to a different consumer. Is this a impermissible disclosure?
    - **Yes** – it is a breach of confidentiality if the records include a different consumer's name or information.
    - Request the consumer return the records, document the disclosure, and forward the documents to the Privacy Officer.

Privacy Violations

- Consumer's Records Sent To The Wrong Provider
  - Consumer records are sent to the wrong provider. Is this a impermissible disclosure?
    - Yes – The provider does not provide care for the consumer and therefore, does not have a need to know anything about the consumer.
    - Request the provider return the documents, document the disclosure and forward the documents to the Privacy Officer.

Release of Information: Identity Verification

- Prior to releasing PHI, ask the individual to provide you with enough information to identify the consumer, such as:
  - Name
  - Date of Birth
  - Address
  - Other identifiers such as social security number, mother's maiden name, etc.
- Identify someone other than the consumer by requesting he provide you with all the above information as well as his relationship to the consumer
  - Check a physical signature against a known one on file
  - Make a call back to the known number
  - Ask for photo ID
  - Ask for a business card
- Provide only the minimum necessary information to safeguard PHI

Release of Information: Authority Verification

- Once you know who the requestor is, be sure he or she has the right to access the information requested.
- Routine requests from employees you know in the organization who have a need to know information for business reasons are ok.
- Unusual requests from individuals you don't know can be risky, so before sharing PHI:
  - Ask the Privacy Officer or a supervisor
  - Check applicable policies/procedures

Faxing PHI

- May we fax PHI?
  - Yes, we can fax PHI but only when in the best interest of the consumer care or payment of claims.
  - We may not fax sensitive PHI (HIV status, STD status, etc.)
  - It is best practice to test a fax number prior to faxing PHI. If this is not done, then complete the following:
    - Restate the fax number to the individual providing it to you.
    - Obtain a telephone number to contact the recipient with any questions.
    - Do not include PHI on the cover sheet.
    - Verify you are including only the correct consumer's information.
    - Double check the fax number before "sending" it.
    - Ask the recipient to confirm receipt of the information faxed either by phone or email.

HIPAA Violations

- How much is enough?
- How much is too much?
- There are three types of violations:
  - Incidental
  - Accidental
  - Intentional

Incidental Violations

- If reasonable steps are taken to safeguard a consumer's information and someone happens to overhear or see PHI that you are using, this is considered an incidental disclosure. There is typically no liability for incidental disclosures.
- Incidental disclosures are going to happen…even in the best of circumstances.
- An incidental disclosure is not a privacy incident. This type of disclosure is not required to be documented.

Accidental Violations

- Mistakes happen. If you mistakenly disclose PHI or provide confidential information to an unauthorized person or if you breach the security of confidential data:
  - Acknowledge the mistake and notify your supervisor and the Privacy Officer, immediately.
  - Learn from the error and help revise procedures (when necessary) to prevent it from happening again.
  - Assist in correcting the error only as requested by your manager or the Privacy Officer. Don't cover up or try to make it "right" by yourself.
  - **Accidental disclosures are Privacy Incidents and must be reported to the Privacy Officer, immediately. We are required to document this type of disclosure.**

Intentional Violations

- If you ignore the rules and carelessly or deliberately use or disclose protected health or confidential information, you can expect:
  - Disciplinary action, up to and including termination.
  - Civil and/or criminal charges
- Examples include:
  - Accessing PHI for purposes other than your assigned job responsibilities.
  - Attempting to learn or use another person's access information.
- **If you're not sure about using or disclosing a consumer's protected health information, check with your supervisor or the Privacy Officer.**

Reporting HIPAA Violations

- If you are aware or are suspicious of an accidental or intentional HIPAA violation, it is your responsibility to report it.
  - SWMBH cannot intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone who in good faith reports a violation (SWMBH Compliance Procedure: Filing A Privacy Complaint)

How May I Report a HIPAA Privacy Violation?

- All HIPAA privacy violations should be reported to the Privacy Officer, using one of the following means:
  - Phone: 1-800-676-0423 dial option 5
  - SWMBH Confidential Hotline: 1-800-783-0914.
  - Email: swmbhcompliance@swmbh.org
  - In writing: 5250 Lovers Lane
    Portage MI, 49002

Substance Abuse Treatment

- Information regarding a person's substance abuse history is federally protected to encourage those needing treatment to seek help without fear of repercussions

42 CFR Part 2

- The regulations governing confidentiality of alcohol and drug abuse patient records
- Imposes restrictions upon the disclosure and use of patient records that are maintained in connection with the performance of any federally assisted alcohol and drug abuse program

42 CFR Part 2

- First issued 1975, revised 1987
- Designed to help deal with the stigma of addiction.
- Requires notification of confidentiality, consent forms, prohibition of re-disclosure
- "I'm sorry I cannot acknowledge whether some is or isn't in our treatment program."

*42 CFR part 2 is the set of confidentiality laws that treatment providers have been operating under since 1975, with a major revision of those rules in 1987.

They were designed to help patients avoid the stigma associated with addiction by keeping their treatment information confidential. It also allowed for patients to honestly talk about their drug and alcohol use, without fear that someone would obtain their information and then use it against them.

This law requires the treatment providers to provide patients with a "notification of confidentiality",…to sign consent forms to disclose information,…and requires the "prohibition of re-disclosure" form that is sent out with any patient information.

The law is so strict that providers cannot even acknowledge whether someone is or isn't in their treatment program. And the protection is so strong, that it survives death.

42 CFR Part 2 Requirements

- No information regarding a client will be released without a signed Authorization to Release Information.

- When information is forwarded to another agency, it must contain the following prohibition:
  - *This notice accompanies a disclosure of information concerning a patient in alcohol/drug abuse treatment, made to you with the consent of such patient. This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR, Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by 42 CFR, Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of this information to criminally investigate or prosecute a client or patient.*

RELEASING SUBSTANCE ABUSE TREATMENT INFORMATION

Rules

Rule #1

- <u>Don't release any consumer information to anyone</u>
- Three sets of exceptions:
  1. *Consumer consent / authorization*
  2. *When rule does not apply:*
     - Communication internal to agency,
     - Crimes on the program premises or against agency personnel,
     - Qualified Service Organization Agreement,
     - Reporting suspected child abuse or neglect,
     - Medical emergencies,
     - Research, and
     - Audit and evaluation
  3. *Court Order Authorizing disclosure and use*
     - Subpoena is not the same as a court order

It's Important to Report Violations…

- So that they can be investigated, managed, documented and reported as required.
- So they can be prevented from happening again in the future.
- So damages can be kept to a minimum.
- To minimize your personal risk.
- In some instances, we may have to notify affected parties of lost, stolen or compromised data.
- **Incidental disclosures need not be reported; however, if you are not sure, report them anyway.**

How May I Report a Privacy Violation?

- All privacy violations should be reported to the Privacy Officer, using one of the following means:
  - Phone: 1-800-676-0423 dial option 5
  - SWMBH Confidential Hotline: 1-800-783-0914.
  - Email: swmbhcompliance@swmbh.org
  - In writing: 5250 Lovers Lane
    Portage MI, 49002