

Welcome to the HIPAA

Privacy and Security Training Session!



Privacy and Security Training Sections

1. What is HIPAA?
2. Why is HIPAA Important?
3. HIPAA Definitions
4. HIPAA Enforcement
5. Patient Rights
6. HIPAA Privacy Requirements
7. The Breach Notification Rule
8. Release of Information (ROI)
9. HIPAA Security Rule
10. PHI Safeguarding Tips
11. Business Associate Agreements
12. HIPAA Violations and Complaints
13. Discussion Slides

*Section I

Introduction **What is HIPAA?**

The Rules

*What is HIPAA?

- * Acronym for Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164).
- * Provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.





What is HIPAA?

Health Information Privacy and Portability Act of 1996

- 1 • **Privacy Rule**
- 2 • **Security Rule**
- 3 • **Electronic Data Exchange**



Each part of HIPAA is governed by different laws

Privacy Rule

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



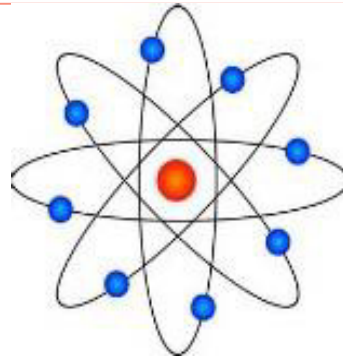
*Security Rule

- * Security (IT) regulations went into effect **April 21, 2005.**
- * Security means controlling:
 - * **Confidentiality** of electronic protected health information (ePHI).
 - * **Storage** of electronic protected health information (ePHI)
 - * **Access** into electronic information



Electronic Data Exchange (EDI)

- * Defines transfer format of electronic information between providers and payers to carry out financial or administrative activities related to health care.
- * Information includes coding, billing and insurance verification.
- * Goal of using the same formats is to ultimately make billing process more efficient.



*Why Comply With HIPAA?

- *To show our commitment to protecting privacy
- *As an employee, you are obligated to comply with HealthSmart MSO privacy and security policies and procedures
- *Our patients/members are placing their trust in us to preserve the privacy of their most sensitive and personal information
- *Compliance is not an option, it is required.
- ***If you choose not to follow the rules:**
 - *You could be put at risk, including **personal** penalties and sanctions.
 - *You could put HealthSmart MSO at risk, including financial and reputational harm.

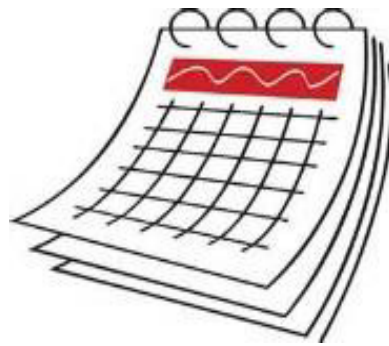
HIPAA Regulations

HIPAA Regulations require we protect our patients' 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 or on the phone)
- * **Written** on paper (i.e. chart, progress notes, encounter forms, prescriptions, x-ray orders, referral forms and explanation of benefit (EOBs) forms)
- * **Computer Applications and Systems** (i.e. electronic health record (EHR), Practice Management)
- * **Computer Hardware/Equipment** (i.e. PCs, laptops, PDAs, pagers, fax machines, servers and cell phones)

Section II

Why is HIPAA Important?



This training session provides you with **REMINDERS** of our organizational **POLICIES** and how **YOU** are required to **PROTECT** PHI

*

* Why is Privacy and Security Training Important?

- * Outlines ways to prevent accidental and intentional misuse of PHI.
- * Makes PHI secure with minimal impact to staff and business processes.
- * **It's not just about HIPAA – it's about doing the right thing!**
- * Shows our commitment to managing electronic protected health information (ePHI) with the same care and respect as we expect of our own private information



* Why is Privacy and Security Training Important?

- *It is everyone's responsibility to take the confidentiality of patient information seriously.
- *Anytime you come in contact with patient information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations.
- *The law requires us to train you.
- *To ensure your understanding of the Privacy and Security Rules as they relate to your job.

* Section III

HIPAA Definitions



*HIPAA Definitions

What is Protected Health Information (PHI)?

* Protected Health Information (PHI) is individually identifiable health information that is:

* Created or received by a health care provider, health plan, employer, or health care clearinghouse and that:

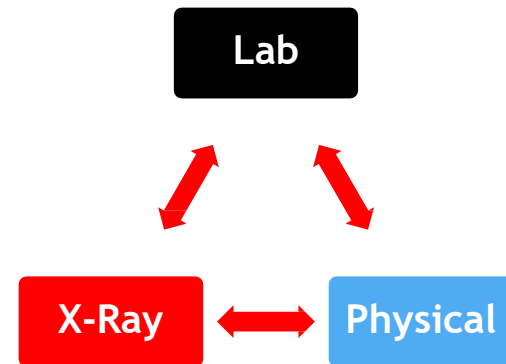
- Relates to the past, present, or future physical or mental health or condition of an individual;
- Relates to the provision of health care of an individual or the past, present or future payment for the provision of health care to an individual.

HIPAA Definitions

* What Does PHI Include?

* Information in the health record, such as:

- * Encounter/visit documentation
- * Lab results
- * Appointment dates/times
- * Invoices
- * Radiology films and reports
- * History and physicals (H&Ps)
- * Patient Identifiers



HIPAA Definitions

What are Patient Identifiers?

PHI includes information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.



HIPAA Definitions



* What Are Some Examples of Patient 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

What Are Uses and Disclosures?

* **Uses:**

When we review or use PHI internally (i.e. audits, training, customer service, or quality improvement).



* **Disclosures:**

When we release or provide PHI to someone (i.e. attorney, patient or faxing records to another provider).

HIPAA Definitions

What is Minimum Necessary?

- * To use or disclose/release only the minimum necessary to accomplish intended purposes of the use, disclosure, or request.
- * Requests from employees at HSMSO:
 - Identify each workforce member who needs to access PHI.
 - Limit the PHI provided on a **“need-to-know”** basis.
- * Requests from individuals not employed at HSMSO:
 - Limit the PHI provided to what is needed to accomplish the purpose for which the request was made.



HIPAA Definitions

What is Treatment, Payment and Health Care Operations (TPO)?

- * HIPAA allows Use and/or Disclosure of PHI for purpose of:
- **Treatment** – providing care to patients.
 - **Payment** – the provision of benefits and premium payment.
 - **Health Care Operations** – normal business activities (i.e. reporting, quality improvement, training, auditing, customer service and resolution of grievances data collection and eligibility checks and accreditation).



* Section IV

HIPAA Enforcement



* 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 between providers and patients.



If patients feel their PHI will be kept confidential, they will be more likely to share information needed for care.

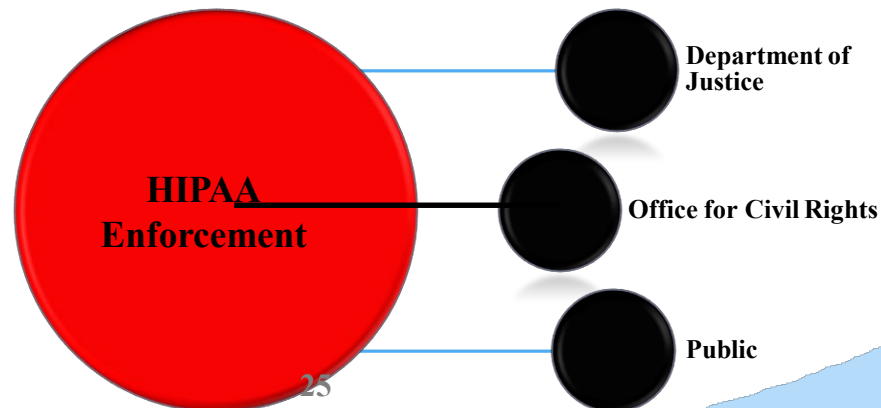
Who or What Protects PHI?

- * **Federal Government** protects PHI through HIPAA regulations
 - * Civil penalties up to \$1,500,000/year for identical types of violations.
 - * Willful neglect violations are mandatory!
 - * 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.
- * **Our organization**, through privacy practices.
- * **You**, by following our policies and procedures.

*Enforcement

How are the HIPAA Regulations Enforced?

- ***The Public.** The public is educated about their privacy rights and will not tolerate violations! They will take action.
- ***Office For Civil Rights (OCR).** The agency that enforces the privacy regulations providing guidance and monitoring compliance.
- ***Department of Justice (DOJ).** Agency involved in criminal privacy violations. Provides fines, penalties and imprisonment to offenders.



* Section V

Patient Rights



* HIPAA Regulations

What Are the Patient's Rights Under HIPAA?

- * The Right to Individual Privacy
- * The Right to Expect Health Care Providers Will Protect These Rights



Other Patient Rights Include: Access, Communications, Special Requests, Amendment, Accounting of Disclosures, Notice of Privacy Practices and Reminders, and the Right to File Complaints.

*Patient Rights

Access and Inspect PHI

- * Patients have the right to inspect and copy their PHI.
- * However, there are some situations where access may be denied or delayed:
 - * PHI compiled for civil, criminal or administrative action or proceedings.
 - * If access would endanger a person's life or safety based upon professional judgment.
 - * If a correctional inmate's request may jeopardize health and safety of the inmate, other inmates or others at the correctional institution.
 - * If a research study has previously secured agreement from the individual to deny access.
 - * If access is protected by the Federal Privacy Act.
 - * If PHI was obtained under promise of confidentiality and access would reveal the source of the PHI.

*Patient Rights

Request Alternate Communication

- *Patient has the right to request to receive communication by alternative means or location. For example:
 - *The patient may request a bill be sent directly to him instead of to his insurance company.
 - *The patient may request we contact her on cell phone instead of home telephone number.

*Patient Rights

Request Amendment

- * Patient has the right to request an amendment or correction to PHI
- * However, there may be a situation when requests may be denied, including:
 - ✓ HSMSO did not create the information.
 - ✓ Record accurate according to health care professional who wrote it.
 - ✓ Information is not part of the HSMSO record.
- * If a patient indicates there is an error in his/her record, the approved amendment will be directed to Privacy Officer

*Patient Rights

Request Restriction

- * **Record Restriction** may be requested by the patient if he/she wishes to change or restrict how your organization uses and discloses your PHI.
- * HSMSO must honor request to restrict disclosure to a health plan:
 - * If the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
 - * The PHI pertains to items and services paid by the patient or patient representative in-full.
- * For all other requests for restrictions, HSMSO must make reasonable effort to honor request, but approval is not required
- * Patient may later revoke a request for record restriction.

*Patient Rights

Accounting of Disclosures

- * **Accounting of Disclosures** is a request for a list of disclosures of a patient's PHI that did not require an authorization or the opportunity for the patient to agree or object.
 - * The HIPAA rules require the organization to provide certain information about the disclosure, such as date, name of person who received the PHI, a description of the PHI and the purpose of the disclosure.
- * Individual may request accounting of disclosures as far back as six years before the time of the request.
 - * Organization must provide the first accounting without charge. Subsequent requests for accountings by the same individual within a 12 month period may be charged a reasonable, cost-based fee, as long as the organization provides notice to the individual.

* Patient Rights

Accounting of Disclosures (cont'd)

Accounting of Disclosures Does Not Include Disclosures For:

- * Treatment (to persons involved in the individual's care), payment or health care operations.
- * Individual subject of PHI.
- * Incident to an otherwise permitted disclosure.
- * Disclosure based on individual's signed authorization.
- * For facility directory.
- * For national security or intelligence purposes.
- * To correctional facilities or law enforcement on behalf of inmates.



* Patient Rights

Accounting of Disclosures (cont'd)

Accounting of Disclosures Does Include Disclosures For:

- * Required by law
- * For public health activities
- * Victims of abuse, neglect, violence
- * Health oversight activities
- * Judicial/Administrative proceedings
- * Law enforcement purposes
- * Organ/eye/tissue donations
- * Research purposes
- * To avert threat to health and safety
- * For specialized government functions
- * About decedents
- * Workers' compensation
- * Releases made in error to an incorrect person/entity (i.e. breach)

* Section VI

HIPAA Privacy Requirements



* Personnel Designation Privacy Officer

* Privacy Officer Responsibilities

- * Development and implementation of the policies and procedures of the entity
 - * Designated to receive and address complaints regarding Privacy
 - * Provide additional information as requested about matters covered by the Notice of Privacy Practices
- * Designation of the Privacy Officer must be documented



*Training

- *Members of the workforce who handle PHI require training
 - *Required upon hire and recommended annually
 - *As material changes are implemented, training to appropriate workforce members affected by that change
 - *Documentation of the training, who attended, the topic covered and date the training was held



* Safeguards

- * Implementation of administrative, physical and technical safeguards (work in tandem with Security rule).
- * Safeguard PHI from any intentional or unintentional use or disclosure.
- * Limit incidental uses and disclosures that occur as a result of otherwise permitted or required uses and disclosures.
 - * Example: create safeguards to prevent others from overhearing PHI.



*Patient Right

File Privacy Complaint

- * Individuals may file complaints with HSMSO's Privacy Official regarding health information privacy violations or HSMSO's privacy compliance program.
- * Individuals may file complaints with the Department of Health and Human Services Office of Civil Rights.



*Sanctions

- *Develop and apply appropriate sanctions for the non-compliance with HSMSO's policies and procedures.
- *Document sanctions that are applied.
 - *NOTE: "Sanctions" can be referred to as discipline or corrective action.



* Mitigation



* HSMSO must mitigate, to the extent practicable, any harmful effects known to HSMSO of a use or disclosure of PHI (by the Covered Entity or Business Associate) in violation of the HSMSO's policies and procedures or the requirements of the Privacy Rule.

*Refraining From Intimidating or Retaliatory Acts

- * HSMSO may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:
 - * Individuals for exercising their rights or filing a complaint;
 - * Individuals and others for:
 - * Filing a complaint;
 - * Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
 - * Good faith opposition to a prohibited act or practice



Waiver of Rights

*HSMSO cannot require an individual to waive their rights provided under this rule for the purpose of providing treatment, payment or enrollment in a health plan or eligibility for benefits.



Policies and Procedures

- * HSMSO must implement policies and procedures designed to comply with the Breach and Privacy Rules.
- * HSMSO must change policies and procedures as necessary and appropriate to comply with changes in the law and maintain consistency between policies, procedures and privacy practices.
- * HSMSO must train employees on changes made to policies and procedures.



Documentation

- * HSMSO must maintain all documentation for 10 years from the date of its creation, including:
 - * Policies and procedures in written or electronic form;
 - * Communications in written or electronic form when such communications are required in writing;
 - * Written or electronic records of actions, activities, or designations as required.



* Definition of PHIMisuse

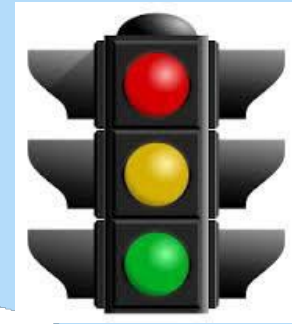
- ▶ The following activities occurring in the absence of patient authorization are considered misuse of protected health information (PHI):

**No! You must
have
authorization
first!**

- Access
- Using
- Taking
- Possession
- Release
- Editing
- Destruction



*Types of Privacy Violations



* **Type I -- Inadvertent or Unintentional Disclosure**

- * Inadvertent, unintentional or negligent act which violates policy and which may or may not result in PHI being disclosed.
- * Disciplinary action for a Type I disclosure will typically be a verbal warning, re-education, and review and signing of the Confidentiality Agreement. However, disciplinary action is determined with the collaboration of the Privacy Officer, Director of Human Resources and the department manager.

* **Type II – Intentional Disclosure**

- * Intentional act which violates the organization's policies pertaining to that PHI which may or may not result in actual harm to the patient or personal gain to the employee.
- * Breach notification processes will be followed as described in the Breach Notification Rule.

* Section VII

Breach Notification Rule



*Breach Notification

Definition of Breach (45 C.F.R. 164.402)

Impermissible use or disclosure of (unsecured) PHI is assumed to be a breach unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised based on a risk assessment.



*Breach Notification

Unsecured PHI

“Unsecured protected health information” means protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology required by the Breach Notification Rule.



*Breach Notification



Risk Assessment

Risk Assessment under the Final Rule requires consideration of at least these four factors:

- * The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- * The unauthorized person who used the PHI or to whom the disclosure was made;
- * Whether the PHI was actually acquired or viewed; and
- * The extent to which the risk to the PHI has been mitigated

*Breach Notification

Risk Assessment Factor #1

Evaluate the nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification of the PHI:

- Social security number, credit card, financial data (risk of identity theft or financial or other fraud)
- Clinical detail, diagnosis, treatment, medications
- Mental health, substance abuse, sexually transmitted diseases, pregnancy



*Breach Notification

Risk Assessment Factor #2

- * Consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made:
 - * Does the unauthorized person who received the information have obligations to protect its privacy and security?
 - * Is that person part of the workforce of a covered entity or a business associate?
 - * Does the unauthorized person who received the PHI have the wherewithal to re-identify it?



*Breach Notification

Risk Assessment Factor #3

- * Consider whether the PHI was actually acquired or viewed or if only the opportunity existed for the information to be acquired or viewed
- * Example:
 - * Laptop computer was stolen, later recovered and IT analysis shows that PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised
 - * The entity could determine the information was not actually acquired by an unauthorized individual, although opportunity existed.



*Breach Notification

Risk Assessment Factor #4

- * Consider the extent to which the risk to the PHI has been mitigated:
 - * Example: Obtain the recipient's satisfactory assurance that information will not be further used or disclosed.
 - * Confidentiality Agreement
 - * Destruction, if credible
 - * Reasonable Assurance



*Breach Notification



Risk Assessment Conclusion

- * Evaluate the overall probability that the PHI has been compromised by considering all the factors in combination (and more, as needed)
- * Risk assessments should be:
 - * Thorough
 - * Performed in good faith
 - * Conclusions should be reasonably based on the facts
- * If evaluation of the factors fails to demonstrate low probability that the PHI has been compromised, breach notification is required

*Breach Notification

When Risk Assessment Not Required

A covered entity or business associate has the discretion to provide the required notifications following an impermissible use or disclosure of protected health information without performing a risk assessment



*Breach Notification

Safe Harbor

- *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.
- *No breach notification required for PHI that is encrypted in accordance with the guidance.



*Breach Notification

Discovery of Breach

- * A breach is treated as discovered:
 - * On first day the breach is known to the covered entity, or
 - * In the exercise of reasonable diligence, it should have been known to the covered entity.
- * Notification time period for a breach begins when the organization did or should have known it existed



*How Do Privacy Violations Happen?

➤ Fax Document to Wrong Location

➤ “Hello, this is Pizza Plaza on Stark Street. Did you mean to fax me this lab result for Fred Flintstone?”

➤ Enter Incorrect Medical Record Number

➤ “I guess I was just typing too fast.”

➤ Forgetting to Verify Patient Identity

➤ “There were seven patients with the name Barney Rubble. I should have confirmed his date of birth.”



Section VIII

Release of Information



*Release of Information (ROI)

- *When releasing PHI, it is important to know when a patient's authorization is required. Patient authorizations are governed by state and federal law.



*Release of Information

Applying the Steps

I received a request to release PHI. What now?

- * Is the individual's authorization required before HSMSO can release PHI?
 - * Under certain circumstances (e.g., treatment, payment, or health care operations), the individual's authorization is not required (more on this later).
 - * An authorization is required for disclosures of PHI not otherwise permitted by the Privacy Rule or more stringent state law.
- * If so, has the authorization been filled out completely and correctly?





*Release of Information

Elements of a Valid Authorization

1. Individual's name;
2. HSMSO (or a HSMSO employee or department) as the party authorized to make the disclosure;
3. Name of the person, organization or agency to whom the disclosure is to be Made;
4. Purpose of the disclosure;
5. Specific and meaningful description of the information to be disclosed
 - A. Note: If the release includes sensitive information (e.g., alcohol or drug abuse treatment records, developmental disability records, HIV test results, reproductive health), these must be affirmatively specified by the individual;
6. The individual's right to revoke the authorization and either the exceptions on the right to revoke and a description of how to revoke or a reference to HSMSO's Notice of Privacy Practices as appropriate;
7. Statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits.

*Release of Information

Elements of a Valid Authorization (cont'd)

8. Statement on the potential for re-disclosure
9. If the release will involve marketing remuneration to HSMSO a statement outlining this
10. Expiration date or event
11. Time period during which the authorization is effective
12. Signature and date signed and
If signed by a personal representative, a description of his/her authority to sign and relationship to individual must be provided
13. Must be written in plain language

If any element is missing, the authorization is not valid. Also, a copy of the authorization must be provided to the individual.



*Release of Information

Evaluating Authorizations



- * Evaluating Authorizations:
 - * Should the access be denied? Has the access been denied?
 - * Is HSMSO providing only the information specified in the authorization?
 - * Is the authorization combined with another type of document to create an inappropriate compound authorization?
 - * In what form/format should the information be provided?
 - * How much time does HSMSO have to respond to the request?
 - * What fees can/should be applied?

Note: If you are uncertain about any of these steps, ask HSMSO's Privacy Officer.

*Release of Information

An Authorization Mishap

- * The patient's Authorization to Release Information stated only the records from 2002 to 2006 should be sent to the attorney. The Release of Information (ROI) Technician didn't notice the limitation and sent documentation of a motor vehicle accident in 2010. She lost her court case and was fined \$50,000.

The patient later filed a complaint with the ROI Technician's employer and the Office for Civil Rights (OCR) and the ROI Technician was fired.



*Release of Information

When Authorization Not Required

Sometimes an authorization is not needed.



Read on to learn more.....

*Release of Information

Permitted Uses and Disclosures of PHI Without Authorization

- * Uses and disclosures of PHI for(**TPO**):
 - * Treatment
 - * Payment
 - * Health Care Operations
- * Disclosures required or permitted by law.
- * If use of the information does not fall under one of these categories you must have the patient's signed authorization (written permission) before sharing that information with anyone.



*Release of Information

When Authorization Is and Is Not Required



When Authorization IS Required:

- Except in limited circumstances, use and disclosure of PHI for marketing purposes

When Authorization IS NOT Required:

- Disclosures to the individual
- Uses and disclosures for treatment by their physician
- Uses and disclosures for quality assurance activities

*Release of Information

Identity Verification

- * Prior to releasing PHI, ask the individual to provide you with enough information to identify the patient, such as:
 - * Name
 - * Date of Birth
 - * Address
 - * Other identifiers: Social security number, mother's maiden name
- * Identify someone other than the patient by requesting he or she provide you with all the above information, as well as his or her relationship to the patient.
 - * Check a physical signature against a known one on file
 - * Make a call-back to a known number
 - * Ask for a photo ID
 - * Ask for a business card
- * Provide only the minimum necessary 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 this information
- Routine requests from employees you know in HSMSO who have business related reason to obtain information are authorized to do so
- Unusual requests from individuals you don't know can be risky, so before sharing PHI:
 - Ask your supervisor
 - And/or check HSMSO's HIPAA Privacy Policies and Procedures



*Release of Information

Minimum Necessary

- * HIPAA requires reasonable steps to limit the use and disclosures of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose.
- * The standard does not apply to the following:
 - * Disclosures to or requests by a health care provider for treatment purposes
 - * Disclosures to the individual subject of the information
 - * Uses or disclosures made pursuant to the individual's authorization
 - * Use or disclosures required for compliance with Health Insurance HIPAA administrative Simplification Rules
 - * Disclosures to the Dept. of Health and Human Services (HHS) when disclosure is required under the Privacy Rule for enforcement purposes
 - * Uses or disclosures that are required by other laws

*Release of Information



Documentation (cont'd)



- * Why do we have to document when we release PHI (when required by law)?
 - * Patients have the right to request a record of what PHI was released and to whom (Accounting of Disclosures)
- * Documentation of releases of information applies to both verbal and written disclosures

*Release of Information Process

- * If you don't know for sure if information can be released:
 - * Don't guess!
 - * Contact HSMSO Privacy Officer



Next, we'll move on to some release of information examples...

*Release of Information



Faxing PHI

- * May PHI Be Transmitted via Fax Machine?
 - * Yes, but only when in best interest of patient care or payment of claims.
 - * Faxing sensitive PHI, such as HIV, mental health, AODA, and STD's is strongly discouraged.
 - * It is best practice to test a fax number prior to transmitting information. If this is not possible:
 - * Restate the fax number to the individual providing it.
 - * Obtain telephone number to contact the recipient with any questions.
 - * Do not include PHI on the cover sheet.
 - * Verify you are including only correct patient's information (i.e. check the top and bottom pages).
 - * Double check the fax number prior to transmission

*Release of Information

E-Mail (cont'd)

- * We may communicate with patients through e-mail only if the patient has signed the organization's privacy and security E-Mail Agreement.
- * When sending ePHI to anyone for treatment, payment or healthcare operations, encrypt the e-mail per HSMSO's procedures, and verify the organization's confidentiality disclaimer is included.



Section IX

HIPAA Security Rule



*HIPAA Security Rule

- *In general, the HIPAA Security Rule requires covered entities and business associates to do the following:
 - *Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is created, received, maintained or transmitted.
 - *Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
 - *Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule.
 - *Ensure compliance with security by its workforce.

*How We Apply the Security Rule

Administrative Safeguards

Policies and procedures are REQUIRED and must be followed by employees to maintain security (i.e. disaster, internet and e-mail use)

Technical Safeguards

Technical devices needed to maintain security.

- * Assignment of different levels of access
- * Screen savers
- * Devices to scan ID badges
- * Audit trails

Physical Safeguards

Must have physical barriers and devices:

- o Lock doors
- o Monitor visitors
- o Secure unattended computers



*How We Apply the Security Rule

Policies and Procedures

*Internet Use

- * Access only trusted, approved sites
- * Don't download programs to your workstation

*E-Mail

- * Keep e-mail content professional
- * Use work e-mail for work purposes only
- * Don't open e-mails or attachments if you are suspicious of or don't know the sender
- * Don't forward jokes
- * Follow HSMSO's policy for sending secure E-mails

* How We Apply the Security Rule

ePHI Access

* How Do We Control ePHI Access?

- * User names and passwords
- * Biometrics
- * Screen savers
- * Automatic logoff



* Access to ePHI

Information Access Management

- HSMSO must implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the HIPAA Security Rule.



* Access to ePHI

User Names

- HSMSO must assign a unique name and/or number for identifying and tracking user identity. It enables an entity to hold users accountable for functions performed on information systems with ePHI when logged into those systems.



* Access to ePHI

Passwords

- The Security Rule requires HSMSO to implement procedures regarding access controls, which can include the creation and use of passwords, to verify that a person or entity seeking access to ePHI is the one claimed.
- The use of a strong password to protect access to ePHI is an appropriate and expected risk management strategy.



Access to ePHI

User Names and Passwords

What Makes a Strong Password?


- * To do so, here are 5 tips: make use of your entire keyboard - too many passwords are overly reliant on lower-case letters which makes them weak and easily cracked. Instead, mix in numbers, symbols (!"£\$%^&*) and capitals
- * change your password on a regular basis - with a password manager in place this won't be too much of a chore and, unless you keep up with data breach news, will add some degree of extra security should your login credentials be compromised via an incident with a third party
- * as previously mentioned, always, always, use a different password for every account - doing otherwise is just asking for trouble
- * make your password as long as possible - the shorter it is, the easier it will be cracked by automated password-guessing tools. Aim for an absolute minimum of 8 characters and a whole lot more if possible, especially when using a password manager which will negate the need to remember even the most complex of passwords
- * if you are not entirely comfortable using a password manager, try stringing several memorable words together - but change letters for numbers where possible, i.e. 'e' becomes '3', 'a' becomes '4', and throw in some punctuation and other symbols for a degree of extra complexity
- * Use a "pass-phrase" such as MbcFi2yo (My brown cat Fluffy is two years old)
- * Do not use passwords that others may be able to guess:
 - * Spouse's Name, Pet or Child's Name
 - * Significant Dates
 - * Favorite sports teams

User Names and Passwords are required by the HIPAA Security Rule



What Can I Do to Help Protect Our Computer Systems and Equipment?



- * Workstation use
 - * Restrict viewing access to others
 - * Follow appropriate log-on and log-off procedures
 - * Lock your workstation, press Ctrl-Alt-Del or Windows key  “L”
 - * Use automatic screen savers that lock your computer when not in use
- * Do not add your own software and do not change or delete ours
- * Know and follow organizational policies
- * If devices are lost, stolen or compromised, notify your supervisor immediately!
- * Do not store PHI on mobile devices unless you are authorized to do so and appropriate security safeguards have been implemented by your organization

E-Mail Security



Appropriate use of e-mail can prevent the accidental disclosure of ePHI. Some tips or best practices include:

- * Use email in accordance with policies and procedures defined by the HSMSO.
- * If an email containing PHI is sent **outside** HSMSO's domain then Message Encryption **MUST** be used.
- * If an email containing PHI is being sent **within** HSMSO domain then Message Encryption does not need to be used.
- * Subject lines are not encrypted. **DO NOT PUT HIPAA INFO IN SUBJECT LINES!**
- * Use e-mail for business purposes and do not use e-mail in a way that is disruptive, offensive, or harmful.
- * Verify email address before sending.
- * Include a confidentiality disclaimer statement.
- * Don't open e-mail containing attachments when you don't know the sender.

Audit Controls

- * The Security Rule requires organizations to implement hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems that contain or use ePHI.
- * Organizations should define the reasons for establishing audit trail mechanisms and procedures for its electronic information systems that contain ePHI.
- * Reasons may include, but are not limited to,
 - * System troubleshooting
 - * Policy enforcement
 - * Compliance with the Security Rule
 - * Mitigating risk of security incidents
 - * Monitoring workforce member activities and actions



Section X

PHI Safeguarding Tips



What else can I do to protect our patients' PHI?

*Safeguarding PHI

Confidentiality

- * Securing information from improper disclosure also includes
 - * Sharing PHI with only those that need to know (direct care workers, staff) in a discreet manner
 - * Refraining from discussing patient visits, conditions, progress, etc. with family, friends, neighbors, and co-workers that do not have a need to know
- * Ensuring the disclosure of information reaches the intended person:
 - * Validating fax numbers prior to faxing PHI
 - * Verification of identity prior to releasing information without the patient present
 - * Requesting verbal authorization from the patient to discuss their health, conditions, etc. with those that may be present.



*Safeguarding PHI

Availability

- * Ensuring that those who require information for proper treatment, payment or health care operations have access to the information they need to fulfill their job obligations.
- * Limiting the access of information to those who do not require access to perform the obligations of their job.
- * Secure workstations by logging off, using strong passwords and keeping passwords confidential.



*Safeguarding PHI

Integrity

- * Ensuring the electronic transmission of data is secured in a manner to protect the integrity of the data. Protecting data integrity may include using:
 - * Secure e-mail; or
 - * Organization communication portals that transfer files within or external to the organization for treatment, payment or operation purposes.



*Safeguarding PHI

Family, Friends, You and PHI



- * Do not share with family, friends, or anyone else a patient's name, or any other information that may identify him/her, for instance:
 - * It would not be a good idea to tell your friend that a patient came in to be seen after a severe car accident.
 - * Why? Your friend may hear about the car accident on the news and know the person involved
- * Do not inform anyone that you know a famous person, or their family members, were seen at this organization

*Safeguarding PHI

Media and PHI

- *If I am contacted by the media, may I release PHI to them?
- *If I am contacted by an individual offering to pay me for PHI, may I release it to them?
 - *No! You may not release PHI under either of these circumstances. Both are grounds for disciplinary action.
 - *Refer the requestor to the Privacy Officer.



* Safeguarding PHI

Delivery of PHI



* I need to transport paper records/PHI to another department. Is this okay?

* Yes, you may transport documents to another department.

* Secure so you don't drop them:

* Carry them close to your person.

* Carry them in a facility designated bag, box, or container.

* Ensure no names are visible.

* Ensure no records are left unattended.

*Safeguarding PHI

Inter Office Mail and PHI

- * Send all PHI in sealed Inter-Office envelopes
 - * Verify all PHI was removed from the envelope before stuffing it
 - * Address to correct individual and department
 - * Mark the envelope “confidential”
 - * Confirm you are sending correct PHI



*Safeguarding PHI

Paper

- * Turn over/cover PHI when you leave your desk/cubicle so others cannot read it.
 - If you have an office, you have the option of closing your door instead.
- * Turn over/cover PHI when a coworker approaches you to discuss something other than that PHI.
- * Don't leave documents containing PHI unattended in fax machines, printers, or copiers.
- * Check your fax machine frequently so documents are not left on the machine.

*Safeguarding PHI

Disposal

- * How should I dispose of confidential paper?
 - * Shred or place all confidential paper in the designated confidential paper bins.

- * How should I dispose of electronic media (floppy disk, CD, USB Drive, etc.)?
 - * Provide electronic media to the IS Department for proper disposal.



*Facility Security

Protecting Our Patient's Physical Security

How can I help protect our facilities?

- * Only employees may enter through employee entrances with you. Direct visitors, vendors, deliveries to front lobby
- * Keep hallway doors that lead to file areas closed.
- * Request vendors and contracted individuals to sign-in and obtain Vendor ID Badges when visiting a restricted area.



* What are Restricted Areas?

* Restricted areas are those areas within our facilities where PHI and/or organizationally sensitive information is stored or utilized

* Receptionist stations

* Business office windows

* Hallways/cubicles

* Offices

* Storage closets and cabinets

* Accounting, Human Resources, Administration Offices, IS Department, etc.

* Employee meeting/rooms/kitchens in the departments



If you see someone in a restricted area not wearing a badge, kindly ask "May I help you?" Then escort the individual out of the restricted area and to the area he/she is visiting.

Section XI

Business Associate Agreements



* Business Associate Agreements

- * If you initiate negotiations to contract with a company to perform, or assist in the performance of a function or activity involving the use or disclosure of PHI, please contact your direct supervisor to obtain a Business Associate Agreement (BAA).
- * Examples of when to obtain a BAA with a company include:
 - * Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; and
 - * Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.



*Business Associates Include

- * Companies that “maintain” PHI on behalf of a Covered Entity (CE)
 - Data storage company
 - Patient safety organizations
 - Companies that transmit PHI to a Covered Entity



*Business Associates (cont'd)

*Business Associates Also Include:

- *Personal Health Record vendors
- *Subcontractors to Business Associates that create, receive, maintain or transmit PHI on behalf of the Business Associate.



*Business Associates (cont'd)

Requirements

- * Limit uses and disclosures of PHI to minimum necessary
- * Enter into a BAA with their subcontractors
- * Comply with the BAA and the same HIPAA; administrative, physical and technical safeguard rules as covered entities (CEs)
- * Report to CE Breach of Unsecured PHI
- * Comply with Privacy Rule to extent it must carry out a CE's obligation under Privacy Rule



* **Section XII**
SECTION XII

HIPAA Violations and Complaints



* HIPAA and Your Role

- * Remember, it is your responsibility, as a HSMSO employee or provider, to comply with all privacy and security laws, regulations, and HSMSO's policies pertaining to them.
- * Violations of any law, regulation, and/or HSMSO policy may result in disciplinary action, up to and including termination, according to policy.



*HIPAA Violations

*Three types of violations:

*Incidental

*Accidental

*Intentional

The Rules

How much is enough?



How much is too much?

*Incidental Violations

- * If reasonable steps are taken to safeguard a patient's information and a visitor happens to overhear or see PHI that you are using, you will not be liable for that disclosure.
- * Incidental disclosures are going to happen (even in the best of circumstances).



An incidental disclosure is not a privacy incident and does not require documentation

* **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, you must**

- * 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 supervisor 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 your Privacy Officer immediately!
Documentation of Accidental Disclosures is required.**

*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 of Intentional Violations of Privacy Include:

- *Accessing PHI for purposes other than assigned job responsibilities

- *Attempting to learn or use another person's access information



If you're not sure about a use or disclosure, check with your Supervisor or the Privacy Officer

*Reporting HIPAA Violations

- * If you are aware or **suspicious** of an accidental or intentional HIPAA violation, it is your responsibility to report it.
- * HSMSO may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone who in good faith reports a violation (whistleblowing).



*** It's Important!**



You Must Report HIPAA Violations

- * So they can be investigated, managed, and documented
- * 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, management may have to notify affected parties of lost, stolen, or compromised data

Incidental disclosures need not be reported, but if you're not sure, report them anyway

* Cool Stuff to Personalize My Computer Are These Good Ideas?

That screen saver with the bubbles? I love it and I want it!

Maroon 5's newest song is amazing---I could listen to it all day long!

I'm a gamer addicted to "Wild Robots of the World V2." There's no reason I can't load it onto my work computer so I can play during breaks and lunch.

My sister's wedding last weekend was just gorgeous and the pictures prove it. I was able to load all the pictures from the ceremony and the reception on my work computer. One's even my home screen. So, my computer crashed when I was loading them. I booted and now they seem just fine.



We Must Respect Each Other's Jobs

As your employer, we appreciate that you want to personalize your workstation. We value your individuality. It's one of the things that makes you a great employee!

You can feel free to bring framed pictures of your family and friends, posters and desk items to create a pleasant work environment.

However, your computer is a different story



- Loading music, screen savers, game and photos can slow down our systems, including the effectiveness and quality of medical records and financial data
- Unapproved tools such as software, downloads, CDs, or flash drives may damage or increase likelihood of unauthorized events such as hacking, viruses and TrojanHorses
- Just as you don't want another department to come into your office and start changing things around, the Information Services Department doesn't want you to compromise the things they do to keep electronic systems effective and safe
- Organizational policy is clear. You may not add such tools without written permission from the Information Services Department

Calling All Privacy & Security Professionals!

Some Facts:

- Emerging electronic technology impacting privacy and security is a reality
- It's getting smarter and smarter & faster and faster
- It's not just desktops and laptops—today we have tablets, iPads, iPhones, Androids, remote monitoring of health conditions, HIE's, eVisits, Work-at-Home, Apps, GPS, and cameras recording us shopping, driving, walking, banking, and grocery shopping

Privacy & Security Professionals Must Keep the Pace:

- Stay tuned in, ensure understanding and be heard!
- Anticipate how privacy and security protections must change to accommodate technology
- How will audit trails work?



Thank you for your attention to the annual HIPAA training.

Please make sure that you signed the attendance sheet.

Please make sure that you have signed all of the attestations and have passed them to me!