

Welcome to the

**Privacy and Security
Training Session!**

Disclaimer

- Document modified from HIPAA COW

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

Privacy and Security Training Presenters

Privacy and Security Officer:
Hareesh Ganesan

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 used and disclosed.
- Gives patients privacy rights and more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).



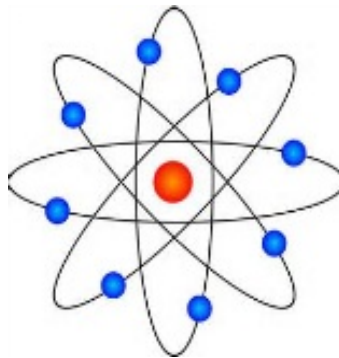
Security Rule

- 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?

- 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.
- You could be put at risk, including
- personal**
- sanctions penalties and
- You could put TVH at risk, including financial and reputational harm
- You could put TVH 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, Lab and X-Ray)
- **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?

thing!

- Makes PHI secure with minimal impact to staff and
 - Shows our commitment to managing electronic
 - **It's not just about HIPAA – it's about doing the right** protected health information (ePHI) with the same care and respect as we expect of our own private information
- 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.
- It is everyone's responsibility to take the confidentiality of patient information that is written, spoken or electronically stored, seriously.
- Anytime you come in contact with patient information or any PHI involved with some facet of the privacy and security regulations.

YOU

become

involved with some facet of the privacy and



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 to an individual
 - 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 TVH:
 - 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 TVH:
 - 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?

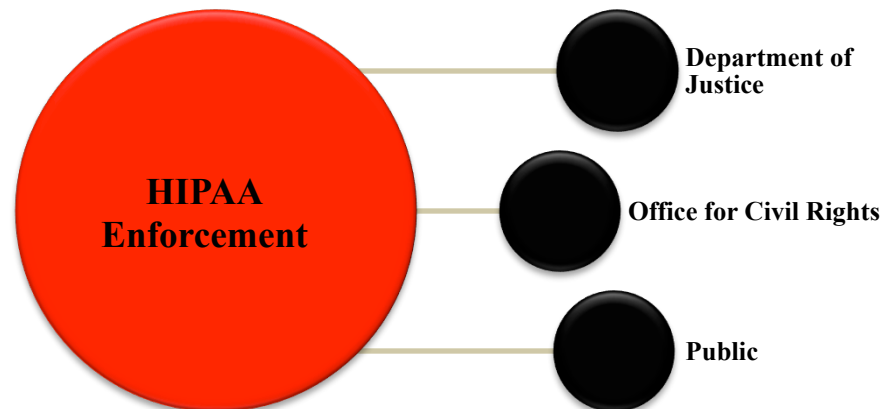
- **Federal Government** protects PHI through HIPAA regulations
 - Civil penalties up to \$1,500,000/year for identical types of violations.
 - Willful neglect violations are mandatory!
 - Criminal penalties:
 - \$50,000 fine and 1 year prison for knowingly obtaining and wrongfully sharing information.
 - \$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 the Notice of Privacy Practices (NPP).
- **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

Notice of Privacy Practices (NPP)

- What is the purpose of the NPP?
 - Summarizes how TVH uses and discloses patient's PHI.
 - Details patient's rights with respect to their PHI
- The Organization must request that new patients sign the NPP acknowledgment form at the time of their first visit.
 - Patients sign the Acknowledgment of Receipt to confirm that they have been offered and/or received the NPP.
 - If unable to obtain a signed Acknowledgement, the Organization must document its good faith efforts to obtain such acknowledgement and the reason why it could not obtain it.



Patient Rights

Access and Inspect PHI

- Patient's have the right to inspect and copy their PHI.
- However, there are some 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 prohibited by law.
 - 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 Special Access Request



Example: If a patient requests that we always call a family member instead of her directly, what are some options:

- Your organization may have specific form to complete
- Your organization may have a policy to refer such requests to Patient Relations or another customer service department
- Usually, organization will have a process in place to document the patient's wishes in his/her medical record

Patient Rights

Request Amendment

- Patient has the right to request an amendment or correction to PHI
- However, may be a situation when request may be denied, including:
 - ✓ TVH did not create the information.
 - ✓ Record accurate according to health care professional that wrote it.
 - ✓ Information is not part of the TVH's record.
- If a patient indicates there is an error in his/her record, what are some options:
 - ✓ Your organization may have a specific form to be completed
 - ✓ Your organization may have process in place to direct requests to Member Relations or another customer service department
 - ✓ Usually, an approved amendment will be directed to the Health Information Management Department or 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.
 - Organization 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, organization must make reasonable effort to honor request, but approval is not required
 - Organization typically has a form to complete to request the restriction
 - 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.
 - Organization typically has a form to complete to request the accounting
 - 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.
- As part of a limited data set (see 45 CFR s. 164.514).



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 TVH's Privacy Official regarding health information privacy violations or TVH'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 TVH's policies and procedures.
- Document sanctions that are applied.
 - NOTE: “Sanctions” can be referred to as discipline or corrective action.





Mitigation

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

Refraining From Intimidating or Retaliatory Acts

- TVH 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 with the Secretary;
 - 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

- TVH 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

- TVH must implement policies and procedures designed to comply with the Breach and Privacy Rules.
- TVH must change policies and procedures as necessary and appropriate to comply with changes in the law and maintain consistency between policies, procedures and the Notice of Privacy Practices.
- TVH must document all changes made to policies and procedures and maintain all policies for 6 years.
- TVH must train employees on changes made to policies and procedures.



Documentation

- TVH must maintain all documentation for 6 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 PHI Misuse

- ▶ 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 Policy.

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 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 TVH 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. TVH (or a TVH 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 TVH'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 TVH, a statement outlining this
10. If the authorization relates to Wisconsin Statute Chapter 51 treatment records, the authorization must include a statement that the individual has a right to inspect and receive a copy of the material to be disclosed
11. Expiration date or event
12. Time period during which the authorization is effective
13. Signature and date signed and
 - A. If signed by a personal representative, a description of his/her authority to sign and relationship to individual must be provided
14. 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 TVH 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 TVH have to respond to the request?
- What fees can/should be applied?

Note: If you are uncertain about any of these steps, ask TVH'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:

- Use or disclosure of psychotherapy notes
- Except in limited circumstances, use and disclosure of PHI for marketing purposes
- When selling PHI

When Authorization IS NOT Required:

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

Release of Information

Another Regulation to Consider

Statute	Summary
42 CFR, Part 2	Federal Alcohol and Drug Regulations which covers use and release of a patient's drug and alcohol abuse records in a federally assisted program



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 TVH 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 TVH's HIPAA Privacy Policies and Procedures



Release of Information

Individual Needs to Find Patient In Any Setting

- If an individual would like to find out if a patient is in our facility, but he or she is not in our Facility Directory:
 - Do not confirm or deny the patient is here until you:
 - Obtain the names of the patient and individual making the request
 - Inform the requesting individual that if the patient is in our facility, and agrees for us to notify them of this, you will...
- ▶ Privately call the department in which the patient is located
 - That department should ask the patient if their location and/or condition may be released to this individual
 - If the patient agrees, provide information to requesting individual
 - If patient not in facility, or does not agree to notify the requesting individual he/she is here, inform the requesting individual that you are unable to confirm or deny whether or not the patient is in the facility

Release of Information

Hospital Facility Directory

- Use the following protected health information to maintain a directory of individuals in its facility:
 - (A) Individual's name
 - (B) The individual's location in the health care provider's facility
 - (C) Individual's general condition, no specific information
 - (D) The individual's religious affiliation
 - (E) Use of disclosure for directory purposes of such information
 - (F) To members of the clergy; or except religious affiliation, to others who ask for individual by name

Release of Information

Hospital Facility Directory (cont'd)

- Patients have the right to opt out of having their information disclosed from a facility directory. There may be State laws that also apply as to what qualifies as directory information.
- The patient must be provided an opportunity to express his or her preference about how, or if, facility directory information may be disclosed. Disclosure of directory information may still occur if doing so is in the individual's best interest as determined in the professional judgment of the provider and would not be inconsistent with any known preference previously expressed by the individual.



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

- Document the release, when required by law, or TVH's policies
- HIPAA law does not require documentation of disclosures for purposes relating to treatment (providing and coordinating care); payment (billing for services rendered); and health care operations (internal business)
- HIPAA requires documentation of breaches and other releases of information



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 TVH Privacy Officer at 3019436475



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

Release of Information

Family and Friends

- Verbal disclosure of information permissible when:
 - Patient present and alert – patient decides
 - Patient incapable to make wishes known – inferred permission to discuss current care
 - Needed for care or payment
 - Information needed for patient's care
 - Family member/friend must clearly be involved in payment for care (involvement is obvious, patient stated so)
- Notify family or friend(s) who are involved in patient's care of:
 - Patient's general condition
 - Patient's location
 - Patient being ready for discharge
 - Patient's death



Disclosures of this nature exclude paper copies

Release of Information

Divorced Parents

- A divorced parent calls to get information on their child. Can you release it?
 - If the parents are divorced, either parent may get access to the records with a proper release. Assume that they can get records unless told otherwise.
- When parental rights are in question:
 - Obtain the court documents for the child's file from one of the parents.
 - If parental rights for physical placement have been terminated, Wisconsin law allows only the parent with sole physical placement to access records.



Release of Information

Legal Guardians

An individual calls to discuss appointment information with you for a patient and states he is the patient's legal guardian. May I discuss with the individual?

- Yes, after obtaining the court documents appointing the individual as the patient's Legal Guardian.
- Make a copy of the court documents for the patient's file.
- Confirm that the information being provided is appropriate and necessary.
- If unable to obtain court documents verifying legal guardianship, do not discuss PHI with the individual.



Release of Information

Step-Parents

A step parent calls to discuss her stepchild's care. May you discuss this with her?

- No, unless the step-parent is a legal guardian and TVH has the guardianship papers on file, or a legal guardian has provided authorization.
- Step-parents may call to schedule appointments, but do not have access to their stepchildren's PHI without authorization by a legal guardian.



Release of Information

Foster Parents

What are the release of information rules for foster parents?

- A foster parent must provide a copy of their WI driver's license or state ID and one or more of the following:
 - Foster Parent ID Card (state-issued)
 - Foster Parent Authorization Form (signed by biological parent or another individual of the proper authority). This form will describe the foster parent's rights in health care situations. (Note: this may be limited)

If the foster parent cannot produce these documents, are there other options?

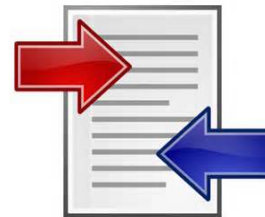
- Provide TVH with name and phone number of their [Insert County]Social Worker
- TVH may call the Foster Parent Intake Line at [Insert phone number] to confirm
- TVH may call either biological parent, if information available, to confirm status.
- Give foster parent the TVH authorization form, if available, indicating that it must be signed by a biological parent and returned to TVH.



Release of Information

Power of Attorney

- The Designated Agent on patient's power of attorney (POA) for health care contacted me to discuss the patient's care. May I discuss?
 - It depends. The Designated Agent's rights to access care, treatment and payment information are not effective until the patient is declared incapacitated by two physicians or one physician and one therapist (with few exceptions)
 - The POA must be reviewed in detail to ensure the requested information is consistent with the rights outlined in the document.
 - A Declaration of Incapacity Form should be submitted prior to honoring a request from the designated agent.



Release of Information

Disclosure of Workers' Compensation PHI to Employer

- What information can be disclosed in response to a Workers' Compensation request?
 - We may disclose only those records reasonably related to the Workers' Compensation claim/condition without an authorization
 - Patient's written authorization is required to release any PHI unrelated to the Workers' Compensation claim



Release of Information

To Another Facility

- Can I release a patient's address and/or insurance information to a nursing home?
 - Yes, if you know the requesting individual and the request is legitimate
 - If you are unfamiliar with the individual requesting the information, ask for the following in writing:
 - Patient's name, date of birth, and address
 - Why the information is needed
 - Specific reason (e.g. treatment or payment)
 - The requestor's name, name of the nursing home, and a direct telephone to the nursing home (switchboard)
 - If uncertain, obtain patient authorization



Release of Information

Leaving Messages

- A spouse answers the phone, or voice mail picks up. What information may I provide?
 - State your first name and that you are calling from TVH (include the site).
 - Ask the patient to return your call, and provide your direct phone number.
 - Do not provide lab results, or other detailed information, other than an appointment reminder.
 - Example: “This is Sally from TVH calling for Johnny Doe. Please call me back at your earliest convenience at [number]. Thank you.”
 - Ensure call is disconnected.



Release of Information

Item Pick Up

- An individual arrives requesting to pick up a prescription for his neighbor. Now what?
 - Request he provide you with the patient's name, date of birth, address, and relationship to the patient.
 - Confirm the patient's and requestor's information matches what the patient provided when informing TVH this individual was picking up the prescription.
 - If information is consistent, we can be assured that the patient requested prescription pick-up by this individual (according to Item Pick Up Policy).
 - Request that the individual sign the Item Pick Up Form and provide him with the prescription.



Release of Information

Faxing PHI

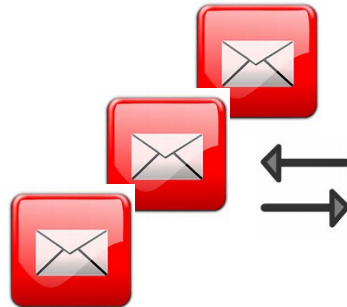


- May PHI Be Transmitted via Fax Machine?
 - Yes, but only when in best interest of patient care or payment of claims.
 - Faxing sensitive PHI, such as HIV, mental health, AODA, and STD's is strongly discouraged.
 - It is best practice to test a fax number prior to transmitting information. If this is 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

- We may **not** communicate with patients through e-mail at this time.
 - The patient portal will provide the opportunity to electronically communicate with our patients.
- When sending ePHI to other organizations for required business functions (i.e. treatment, payment or healthcare operations), encrypt the email per TVH's procedures.



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 TVH'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:

- Lock doors
- Monitor visitors
- 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 TVH'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

- TVH 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

- TVH 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 TVH 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?

- Use at least 6-8 characters.
- Use a minimum of 2 letters and 1 number, and capital and lower case letters
- 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 TVH.
- 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 those that 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 to information to those that 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

Transporting PHI Offsite

- When necessary to transport PHI externally:
 - Place in a locked briefcase, closed container, sealed, self-addressed interoffice envelope;
 - Place PHI in the trunk of your vehicle, if available, or on the floor behind the front seat;
 - Lock vehicles when PHI is 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?

- Wear your ID Badge at all times (helps identify you as an TVH employee/provider).
- Only let employees enter through employee entrances with you.
- Keep hallway doors that lead to patient care 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
 - Main office

If you see someone in a restricted area not wearing a badge, kindly ask “May I help you?”
restricted area and to the area he/she is visiting.



l out of the

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 the Hareesh Ganesan 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



Other Confidentiality Agreements

- When initiating a contract with a company to perform work for TVH which will ***not*** have direct access to PHI, request a Confidentiality Agreement be signed and forwarded to Hareesh Ganesan.



Section XII

HIPAA Violations and Complaints



HIPAA and Your Role

- Remember, it is your responsibility, as a TVH employee or provider, to comply with all privacy and security laws, regulations, and TVH's policies pertaining to them.
- Employees and providers suspected of violating a privacy or security law, regulation, or TVH policy are provided reasonable opportunity to explain their actions.
- Violations of any law, regulation, and/or TVH policy will result in disciplinary action, up to and including termination, according to TVH HR 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 leader 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.
 - TVH 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

Patient Complaints

We Must Respond to Privacy and Security Complaints

All Privacy Complaints Must Be Reported



How Do I Report

HIPAA Privacy Violations?

- Directly to your Supervisor, who in turn reports it to the TVH's Privacy Officer
- Call or email the Privacy Officer
- Complete a HIPAA Incident Report form which is located on the Google Drive under Security



How Do I Report HIPAA Security Violations?

- Same as for Privacy Violations, except instead of reporting to the Privacy Officer, report to the TVH's HIPAA Security Officer
- You may also call or email the TVH's Technical Security Officer, Information Services Help Desk, or Director of Information Services

