HIPAA Privacy: How it Affects Mended Hearts
Goals of the Presentation

- To increase your knowledge and understanding of Protected Health Information (PHI) and Treatment, Payment and Operations (TPO)
- Enhance your awareness of your role in helping Mended Hearts follow HIPAA rules
- Alert you to the possible penalties for violation of HIPAA law for you and MHI
- Understand this law protects you as a consumer of health care
Privacy Regulations April 14, 2003
Implementation Date
What is HIPAA

- Health Insurance Portability and Accountability Act of 1996 – a Federal Law
HIPAA Key Terms

- **Privacy** - the right of an individual to keep his/her individual health information from being disclosed
- **Use** – how covered entities share, employ, utilize, examine, PHI within their facility
- **Disclose** – release or divulgence of information by an entity to persons or organizations outside the entity
- **Authorization** – mechanism for obtaining consent from a patient for the use of health information for a purpose that is not treatment, payment, or health care operations
HIPAA Key Terms – cont.

- PHI – all Individually Identifiable Health Information and other information on treatment and care that is transmitted or maintained in any form
- Minimum Necessary – This means don't ask or look for more PHI than you need to do a visit. The OCR states that this is not an "absolute standard," but a "reasonableness standard" and the covered entity has "substantial discretion" as to implementation. Providers will have to balance protection of PHI with the timely delivery of quality health care
HIPAA Key Terms – cont.

- TPO - Treatment, payment, and health care operations
- Office for Civil Rights - The HHS entity responsible for enforcing HIPAA privacy rules
- Health and Human Services - U.S. Dept. of The federal agency responsible for implementing HIPAA
Patient consent or authorization is not required for release of PHI for treatment, payment, and operations (TPO). A signed authorization will be necessary for release other than for TPO such as research, fund-raising, or to a third party specified by the patient.

- While HIPAA lays a floor of privacy protection, entities are free to retain or adopt more protective policies.
- Some organizations are taking a tough line on release of information thereby slowing down information exchange.
- The OCR suggests negotiating with the entity to reach a solution.
The recent clarification by the OCR should lay many fears to rest by stating that a covered entity can not guarantee the privacy of PHI from all potential risks, but should use reasonable safeguards depending on the size and need of the organization.

The following activities meet the reasonable safeguard test:

- Open treatment areas in many covered entities
- Calling out a patient's name in a waiting room
- Talking in a hallway
- Using sign-in sheets
- Sending appointment reminders
Privacy: Why the Concern?

- CIVIL Penalties for failure to comply
  - $100 fine per person per violation
  - $25,000 fine per year for multiple violations
  - $25,000 fine cap per year per requirement
  - YOU can be personally liable!!!
Privacy Why the Concern – cont.

- CRIMINAL Penalties for failure to comply
  - Knowingly or wrongfully disclosing or receiving PHI:
  - Commit offense under false pretenses: $100,000 fine and/or five years prison time
  - $250,000 fine and/or ten years prison time
Key Things to Remember about Privacy

- You as a MHI visitor must safeguard patient health information
- Share only information necessary to do a visit or follow-up visit
- Know the policies on HIPAA where your chapter visits and follow them
- If you are ever in doubt have your Visiting Chairperson contact your hospital’s Privacy Officer
Who is Affected?

- Hospital employees who handle/use/know individuals’ Protected Health Information (PHI)
- Health Care Providers (Health departments, hospitals, doctors’ offices, any agency that transmits PHI electrically)
- Business Associates – Performing services on the covered entities behalf
- Mended Hearts Visiting Programs and Visitors
HIPAA Requires Hospitals to...

- **Identify PHI Uses and Disclosures**
  - **WHO**
    - People who routinely use or disclose PHI in their institution
  - **WHAT**
    - Individually identifiable health information is used or disclosed
  - **HOW**
    - Written, oral, electronic communication
  - **HOW MUCH**
    - Minimum necessary to accomplish purpose
Examples of PHI

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code
- All elements of dates directly related to an individual, including birth date, admission date, discharge date, date of death
- Telephone numbers
- Fax numbers
- Medical record numbers
- Health plan beneficiary number
- Account numbers
- Full face photographic images and any comparable images
- ANY other unique identifying number, characteristic
- Social Security Numbers
Where is PHI Found?

- Medical records
- Insurance/benefits enrollment and payment
- Claims adjudication
- Case and medical management records
Things to Know and Do

- Know your hospital’s HIPAA policies and follow them
- Know that the patient is King/Queen over their health information
- Know that there are NO cookie cutter solutions
- Know Nationals’ HIPAA Guidelines and if applicable offer suggestions and recommendations to National
Questions & Answers