HIPAA and PHI

Harmony Healthcare International (HHI)

We **C.A.R.E.** About Care

Version 8.13.17

Harmony Healthcare INTERNATIONAL

HIPAA

Health Insurance Portability and Accountability Act

Harmony Healthcare INTERNATIONAL

PHI

Protected Health Information

Harmony Healthcare INTERNATIONAL

HIPAA

- HIPAA Act passed in 1996 with the intent to reduce administrative costs of healthcare
- Now most commonly associated with the **Privacy and Security Rules**

Harmony Healthcare INTERNATIONAL

HIPAA: Background

- To improve the **efficiency** and **effectiveness** of the health care system the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** of 1996, Public Law 104-191 was created
- To improve standardization by establishing a common "language" for the transmission of electronic claims, payment and administrative information

Harmony Healthcare INTERNATIONAL

HIPAA: Background

- Required the Department of Health and Human Services (HHS) to adopt national standards for:
  - Electronic Health Care Transactions
  - Code Sets
  - Unique Health Identifiers
  - Security

Harmony Healthcare INTERNATIONAL

HIPAA: Background

- At same time **Congress** recognized that **advances in electronic technology** could **erode the privacy of health information**
- Congress incorporated into HIPAA provisions that mandated the adoption of **Federal privacy protection** for **identifiable health information**

Harmony Healthcare INTERNATIONAL

Administrative Simplification Section of Title II

- Section of HIPAA that required the development of standardized transaction standards for content and transmission of:
  - Data
  - Single National Provider Identification number for all healthcare providers
  - The Privacy and Security Rules to protect health information

Harmony Healthcare INTERNATIONAL

Common Abbreviations

- PHI – Protected Health Information
- OCR – Office of Civil Rights
- CMS – Centers for Medicare & Medicaid Services
- DOJ – Department of Justice
- HITECH – Health Information Technology for Economic and Clinical Health
- TPO – Treatment Payment and Operations
- BA – Business Associate

Harmony Healthcare INTERNATIONAL

Which Law Governs

- A patient who resides in MA, is at a subacute facility in NH. The facility maintains medical records in NH. Which laws govern (NH or MA) the disclosure of PHI in the patient's medical records?
  - Step 1: Rely on the standard where the records are maintained
  - Step 2: Between HIPAA and the operative state law (NH), follow the stricter standard.

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule

- The HIPAA Privacy Rule (effective April 15, 2003) establishes federal protections for **individually identifiable health information held by covered entities and their business associates (called "protected health information")** and gives **patients important rights with respect to their health information.** At the same time, the Privacy Rule is balanced to permit the use and disclosure of health information needed for patient care and other important purposes.

Harmony Healthcare INTERNATIONAL

Use & Disclosure of PHI

- A **covered entity**
- May not **use or disclose**
- **Protected health information**
- Except as **permitted** or **required** by the Privacy Rule

Harmony Healthcare INTERNATIONAL

Covered Entities

- **Health Plans:** A plan that provides or pays the cost of medical care (e.g., Medicare, Medicaid, HMO, Managed Medicare etc). Does NOT include group health plans with less than 50 participants administered by the employer.
- **Health Care Providers:** A provider of medical or health services (such as SNFs, home health, hospitals, physician clinics, etc.) that transmits any health information in electronic form.

Harmony Healthcare INTERNATIONAL

Covered Entities

- **Clearinghouses:** Process health information from a non standard content into standard data elements or to a standard transaction (e.g., billing services, health information systems). NOT third party administrators.

Harmony Healthcare INTERNATIONAL

Covered Entities

- To determine if a facility is a covered entity ask the two questions:
  - Does the facility **provide health care**?
  - Does the facility **engage in a standard transaction**?
- If yes to both then it is a covered entity

Harmony Healthcare INTERNATIONAL

Covered Entities

- Examples of **Covered Entities**:
  - SNFs
  - Hospitals
  - Assisted Living
  - CCRC organized as a single legal entity

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule

- Two approaches to protecting privacy of health information:
  1. **Assigns rights** to individual patients to provide them with some control over their own health information
  2. **Provides standards** for the ways that healthcare provider, health plans, and health clearinghouses are permitted to access, use and disclose health information

Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

- **The Security Rule** (effective April 20, 2005) specifies a series of **administrative, physical, and technical safeguards** that covered entities and their business associates must implement to assure the **confidentiality, integrity, and availability of electronic protected health information**

Harmony Healthcare INTERNATIONAL

HIPAA Rules

- HIPAA Rules apply to **Covered Entities and Business Associates:**
  - Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information

Harmony Healthcare INTERNATIONAL

HIPAA Rules

- HIPAA Rules apply to Covered Entities and Business Associates:
  - If a covered entity engages a business associate to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes the uses and disclosures of protected health information that the business associate is permitted to make and requires the business associate to safeguard the information

Harmony Healthcare INTERNATIONAL

HIPAA Rules

- HIPAA Rules apply to Covered Entities and Business Associates:
  - In addition to these contractual obligations, business associates are directly liable under the HIPAA Rules for making uses and disclosures that are not authorized by its contract or required by law and for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule

Harmony Healthcare INTERNATIONAL

HIPAA Laws and Regulations

- Divided into **Five Rules**:
  - Privacy Rule
  - Security Rule
  - Transaction Rule
  - Identifiers Rule
  - Enforcement Rule (HITECH Act)

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule

- The Privacy Rule **establishes national standards to protect individual's medical records** and **other personal health** information
- The Privacy Rule **applies to:**
  - **Health plans**
  - **Health care clearinghouses**
  - **Health care providers that conduct health care transactions electronically**

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
What is PHI?

- Definition: Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
What is PHI?

- HIPAA regulations **allow researchers** to access and use PHI when necessary to conduct research
- However, HIPAA only affects research that uses, creates, or discloses PHI that will be entered in to the medical record or will be used for healthcare services, such as treatment, payment or operations

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule

- The HIPAA Privacy Rule **requires** appropriate **safeguards to protect the privacy of Personal Health Information**, and **sets limits and conditions** on the **uses and disclosures** that may be made of such information without patient authorization

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
What is PHI?

- Data are "individually identifiable" if they include any of the 18 types of identifiers for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual.
- These identifiers are as follows…

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule PHI 18 Identifiers

PHI 18 Identifiers:

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code) and their equivalent geocodes, except for the three digits of a zip code, if according to the current publicly available data from the Bureau of the Census:
   - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   - The initial three digits of zip code for all such geographic units containing 20,000 or fewer people is changed to 000

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule PHI 18 Identifiers

3. **Dates of all elements (except year)** for dates directly related to an individual,
   - Including **birth date,**
   - Admission date,
   - Discharge date,
   - Date of death,
   - All ages **over 89** and all elements of dates **(including year)** indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
PHI 18 Identifiers

4. Telephone numbers
5. FAX numbers
6. Email address
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
PHI 18 Identifiers

11. **Certificate/license numbers**
12. **Vehicle identifiers** and serial numbers, including license plate numbers
13. **Device identifiers** and serial numbers
14. **Web URLs**
15. Internet Protocol **(IP) address numbers**

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule
PHI 18 Identifiers

16. Biometric identifiers, including **finger and voice prints**
17. **Full face photographic images** and any comparable images
18. **Any other unique identifying number, characteristic, or code** (note this does not mean the unique code assigned by the investigator to code the data)

Harmony Healthcare INTERNATIONAL

Individual Privacy Rights

- Right to access and obtain a copy of their PHI
- Right to amend their PHI
- Right to obtain an accounting or listing of disclosures of their PHI
- Right to receive a Notice of Privacy Practices
- Right to have communication about their PHI conducted in a confidential manner
- Right to restrict disclosure on certain uses and disclosures of their PHI
- Right to file a complaint about a covered entity's privacy practices to the covered entity as well as to the Office of Civil Rights

Harmony Healthcare INTERNATIONAL

Notice of Privacy Practices

- Healthcare providers and health plans are required to provide the patient with a copy of their notice of privacy practice that describes in easily understood terms how the covered entity uses and discloses individual PHI and examples on how their health information may be used or disclosed
- Explains covered entity legal obligations are, what the individual rights are and whom to contact with complaints and questions

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule: Privacy Practices for PHI

- The Notice of Privacy Practices (NOPP) allows PHI to be used and disclosed for purposes of TPO
- Treatment (T), Payment (P), Operations (O):
  - TPO includes teaching, medical staff/peer review, legal auditing, customer service, business management and releases mandated by law

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule: Privacy Practices for PHI

- Examples of TPO:
  - The patient's referring physician calls and asks for a copy of the patient's recent exam:
    - Treatment
  - A patient's insurance company calls and request a copy of the patient's medical record for a specific services date
    - Payment
  - The Quality Improvement office calls and asks for a copy of an operative report
    - Health Care Operations
- For these TPO purposes, patient information may be provided

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule: Privacy Practices for PHI

- Except for **Treatment,** the **Minimum Necessary** Standard Applies:
  - For patient care and treatment, HIPAA does not impose restrictions on use and disclosure of PHI by health care providers:
    - **Exception:** Psychotherapy information, HIV test results, and substance abuse information
  - For anything else, HIPAA requires users to access the minimum amount of information necessary to perform their duties:
    - Example: A billing clerk may need to know what laboratory test was done, but not the result

Harmony Healthcare INTERNATIONAL

HIPAA Privacy Rule: Privacy Practices for PHI

- When Should You:
  - View PHI
  - Use PHI
  - Share PHI

Remember

  - Use information **only when necessary** to perform your job duties
  - Use only the **minimum necessary** to perform your job duties

Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

- **Security Rule:**
  - 45 CFR § 164.3xx
  - Enforceable since 2005
  - Applies to all Electronic PHI
  - Flexible, customizable approach to health information security
  - Uses Risk Analysis to identify and plan mitigation of security risks
  - Calls for Policies and Procedures
- Now being enforced more, including identity theft cases

Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

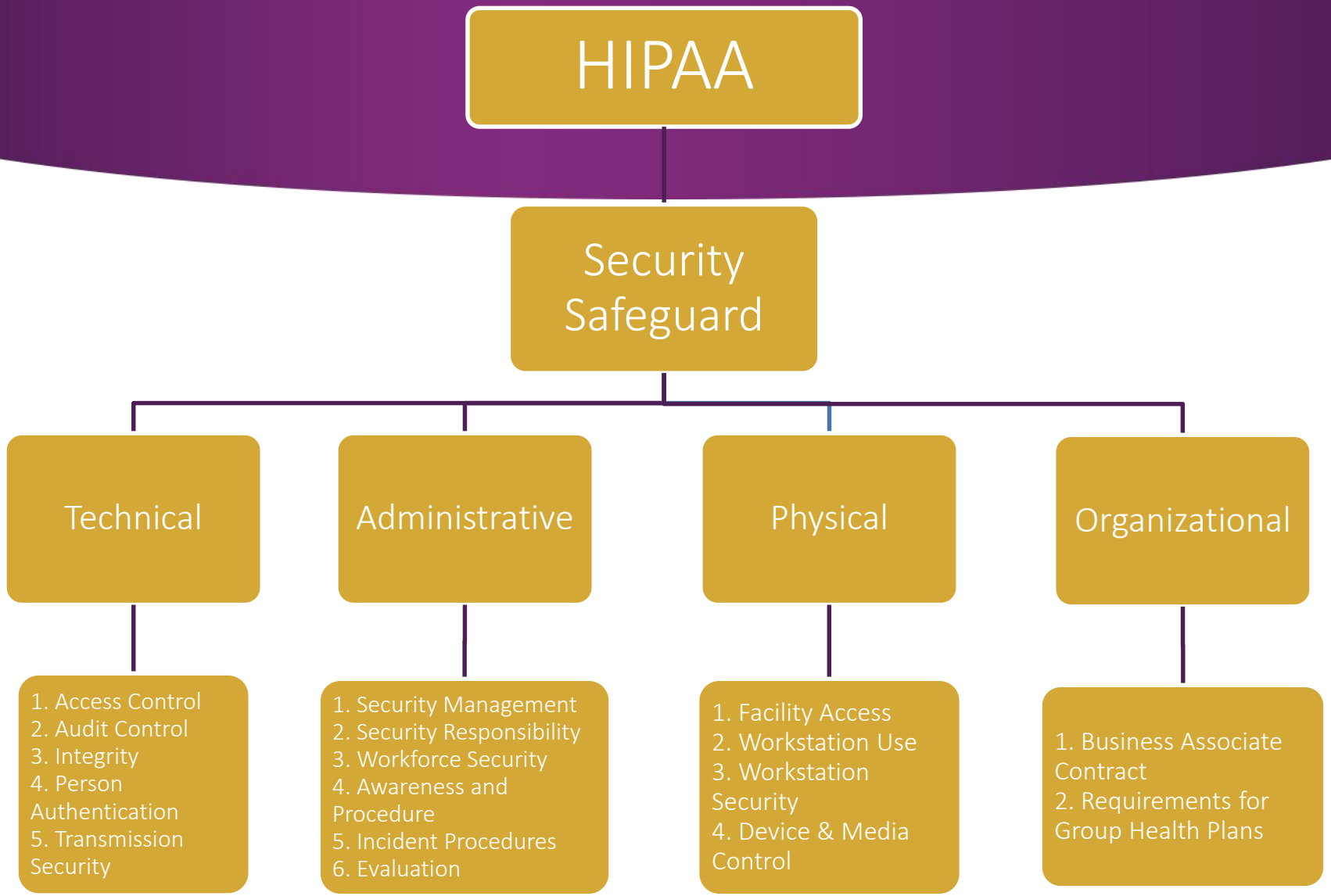
- The HIPAA Security Rule addresses the privacy protection of electronic protected health information (PHI)
- Similar to the Privacy Rule, the Security Rule also deals with identifiable health information as defined by 18 HIPAA identifiers
- The Security Rule defines standards, procedures and methods for protecting electronic PHI with attention to how PHI is stored, accessed, transmitted, and audited

Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

- The HIPAA Security Rule addresses **three** aspects of **security:**
  - **Administrative Safeguards** - Assignment of a HIPAA security compliance team
  - **Physical Safeguards** - Protection of electronic systems, equipment and data
  - **Technical Safeguards** - Authentication and encryption used to control data access

Harmony Healthcare INTERNATIONAL



Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

- Covered entities need to **perform a Risk Analysis and utilize Risk Management methodologies** so vulnerabilities and possible risks can be reduced
- Organizations should assign a **security analyst or officer** who is **responsible or maintaining and enforcing the HIPAA standards within the organization**

Harmony Healthcare INTERNATIONAL

HIPAA Security Rule

- **Hardware, software and transmission security:**
  - Organizations should have a **hardware firewall in place**
  - Transmission of personal information should be **encrypted** and **comply with HIPAA rulings**
  - Operating Systems should be hardened and up to date
  - **Policies** should cover the updating of hardware, firmware, operating systems and applications

Harmony Healthcare INTERNATIONAL

HIPAA Transaction & Code Set Rule

- Per HIPAA regulations, a **Code Set** is any set of codes used for **encoding data elements**, such as:
  - Medical terms
  - Medical concepts
  - Medical diagnosis codes
  - Medical procedure codes
- Code sets for medical data are required for administrative transactions under HIPAA for **diagnoses, procedures, and drugs**

Harmony Healthcare INTERNATIONAL

HIPAA Transaction & Code Set Rule

- Medical data code sets used in the health care industry under HIPAA include:
  - Coding systems for health-related problems and their manifestations;
  - Causes of injury, disease or impairment;
  - Actions taken to prevent, diagnose, treat, or manage diseases, injuries, and impairments;
  - And any substances, equipment, supplies, or other items used to perform these actions

Harmony Healthcare INTERNATIONAL

HIPAA Transaction & Code Set Rule

- The following code sets are used in HIPAA transactions:
  - ICD-10-CM Codes
  - HCPCS Codes
  - CPT-3 Codes
  - CPT-4 Codes
  - NDC Codes

Harmony Healthcare INTERNATIONAL

Identifiers Rule

- To juxtapose HIPAA's Administrative Simplification efforts, the Centers for Medicare & Medicaid Services (CMS) introduced four **unique identifiers** which promise to standardize the identification numbers for providers, employers, and ensure future consistency and ease of use.

Harmony Healthcare INTERNATIONAL

Identifiers Rule

- The four unique identifiers are:
- The **Standard Unique Employer Identifier** - This is the standard Employer Identification Number or EIN which can be found on employee's federal Internal Revenue Service (IRS) Form W-2, Wage and Tax Statement received from their employer. With the help of using EIN, it would be easy to identify an entity acting in an employer role in standard HIPAA transactions that too without identifying the patient's health plan or insurance coverage. Moreover, EIN will not replace the group number, account number, policy number, or subscriber number.

Harmony Healthcare INTERNATIONAL

Identifiers Rule

Standards for Transactions:

- Under HIPAA, HHS adopted certain standard transactions for the electronic exchange of health care data. These transactions include:
- Claims and encounter information
- Payment and remittance advice
- Claims status
- Eligibility
- Enrollment and disenrollment
- Referrals and authorizations
- Coordination of benefits
- Premium payment

Harmony Healthcare INTERNATIONAL

Identifiers Rule

- HIPAA-covered entities who conduct any of these transactions electronically must use an adopted standard from ASC X12N or NCPDP
- The **National Provider Identifier (NPI) -** For covered health care providers, NPI is a unique identification number. For all HIPAA administrative and financial transactions, covered health care providers and all health plans and health care clearinghouses should use NPIs. As the NPI is a 10-position, intelligence-free numeric identifier (10-digit number), it does not disclose other information about health care providers.
- An NPI must be used in all HIPAA standard transactions.

Harmony Healthcare INTERNATIONAL

HIPAA Enforcement Rule

- The HIPAA Enforcement Rule stems directly from the **ARRA HITECH Act provisions** that **distinguishes between violations occurring before, and on or after the compliance date of Feb. 18, 2013** "with respect to the potential amount of **civil money penalty** and the **affirmative defense** available to covered entities", according to the rule

Harmony Healthcare INTERNATIONAL

HITECH Act

- HITECH is the **Health Information Technology for Economic and Clinical Health Act**
- Passed in **February 2009** as part of the American Recovery and Re-investment Act (ARRA)
- Includes modifications to the Privacy and Security rules
- Designed to promote widespread adoption and standardization of electronic health records

Harmony Healthcare INTERNATIONAL

HITECH Act

- Includes notification requirements:
  - Breaches of unsecured information
  - Increases the potential civil monetary penalties for violation of HIPAA
  - Strengthens certain privacy rights

Harmony Healthcare INTERNATIONAL

HITECH ACT

- As part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act updated federal HIPAA privacy and security standards
- Updates Include:
  - Breach notification requirements
  - Fine and penalty increases for privacy violations
  - Right to request copies of the electronic health care record in electronic format
  - Mandates that Business Associates are civilly and criminally liable for privacy and security violations

Harmony Healthcare INTERNATIONAL

HIPAA Breach Notification Rule

- Enforceable since February 2010
- Final Rule in effect with new changes in how to determine if a **breach must be reported**
- Works with Privacy and Security Rules
- Requires reporting of all PHI breaches to HHS and Individuals
- HHS Wall of shame: Post all large breaches 500 or more
- Extensive/expensive obligation

Harmony Healthcare INTERNATIONAL

Reportable Breach

- All breaches not meeting an exception are reportable, unless there is a “low probability of compromise” of the data, based on a risk assessment including at least:
  - What was the information, how well identified was it, and is its release “adverse to the individual”
  - To whom it was disclosed
  - Was it actually acquired or viewed
  - The extent of mitigation
- Right to notification of breaches must be listed in the Notice of Privacy Practices

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

1. Was there acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule?
   - If No, not a breach, end of process
   - If an incident, document the incident and the determination of “not a breach”
   - If yes, Go on to Step 2

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

2. Was the information secured according to HHS guidance, or destroyed?
   - If Yes, not a reportable breach, end of process; document the incident and determination of “not a reportable breach”
   - If No, may be able to use lower security encryption in the evaluation of risk later in Step 5; go to Step 3

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

3. Was the potential breach internal to your organization, and unintentional, in good faith, with no further use, or inadvertent and within job scope?
   - If Yes, not a breach, end of process; document the incident and determination of “not a breach”
   - If No, go on to step 4

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

4. Is there no way the breached information can be retained?
   - If no way the PHI was retained, not a breach, end of process; document the incident and determination of “not a breach”
   - If the breached information may be retained in some way, go to Step 5

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

5. If you've gotten here, you have a breach, and now the only way to keep from having to report is to do a risk assessment to see if there is a "low probability of compromise"
   - If there is a low probability of compromise, it is not reportable, end of process; document incident and determination of "not a reportable breach"
   - If not a low probability of compromise, **Must** report

Harmony Healthcare INTERNATIONAL

Breach Notification Decision Tree

- Breach Notification Risk Assessment: Not reportable if there is a “low probability of compromise” of the data, based on a risk assessment of:
  - What was the information and how well identified was it
  - To whom it was disclosed
  - Was it actually acquired or viewed
  - The extent of mitigation

Harmony Healthcare INTERNATIONAL

Breach Notification & Report

- If a small Breach (less than 500 individuals affected):
  - Report to the individual within 60 days
  - Report to DHHS no later than 60 days after the end of the year
- If a large Breach (500 or more affected)
  - Report to the individual within 60 days
  - Report to DHHS when you notify the individual
  - If more than 500 individuals in any jurisdiction, notify major media

Harmony Healthcare INTERNATIONAL

What are the Penalties for Violating HIPAA?
Civil Monetary Penalties

Tier	Penalty
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

Harmony Healthcare INTERNATIONAL

What are the Penalties for Violating HIPAA?

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

Harmony Healthcare INTERNATIONAL

HIPAA: What's New

- Individual rights of **access**
- Individual rights of **restriction**
- New restrictions on use of genetic information by health plans
- Change in the way to determine whether or not a **breach must be reported**
- New restrictions on disclosures for marketing, sale of PHI; changes to rules for use of PHI for fundraising
- Notices of Privacy Practices must be updated to reflect new individual rights and privacy practices
- Expansion of rules to Business Associates
- PHI not protected > 50 years after individual's death

Harmony Healthcare INTERNATIONAL

Individual Rights to Access PHI

- Must have a process for individual to request access and for a reasonable cost-based fee
- Must provide the entire record in the Designated Record Set if requested:
  - Medical and billing records used in whole or in part to make decisions related to health care
  - New- Information kept electronically must be available electronically if requested.
  - Exceptions for Psychotherapy notes, CLIA, others
  - Changes to HIPAA and CLIA proposed to allow access of lab information by individuals (not finalized yet)
- New- 30-day extension to provide records held off-site no longer allowed-must retrieve within 30 days

Harmony Healthcare INTERNATIONAL

Business Associates (BA): Expansion of Rules

- Security Rules applies
- Breach Notification Rules applies
- Privacy Rule Use (how they use the information) and Disclosure provision apply
- BA responsible for having contracts with Covered Entities and Subcontractors
- BA directly liable for compliance and violations

Harmony Healthcare INTERNATIONAL

Business Associates (BA): Expansion of Rules

- BA will need to educate their Subcontractors
- Contracts signed since January 25, 2013 must meet new standard by September 23, 2013
- Older, complaint contracts signed before January 25, 2013 have until September 23, 2014 to comply

Harmony Healthcare INTERNATIONAL

Revisions to the Notice of Privacy Practices

- HIPAA Notices of Privacy Practices must reflect individual rights and controls on uses and disclosures:
  - New right of access to electronic PHI
  - New right of restriction of disclosures
  - New right to be notified in the event of a breach
  - Changing to marketing
  - Changes to Fundraising
  - GINA notice for health plan NPPs
- Must update policies and NPP together, by deadline
- Start using (and post) new version; no requirement for providers to redistribute to all patients

Harmony Healthcare INTERNATIONAL

Nursing Home Regulation HIPAA

- **Privacy Rules:**
  - HIPAA privacy rules define the circumstances under which a **resident's electronic health care information can be disclosed to third parties.** With few exceptions, a facility must have the resident's **written authorization** to disclose specific medical information.
  - Residents **must be provided with a written notice** as to how health information is used and shared

Harmony Healthcare INTERNATIONAL

Nursing Home Regulation HIPAA

- **Security Rules:**
  - Facilities must implement **administrative**, **technical**, and **physical safeguards** to ensure that **electronic protected health care information** is not disclosed to unauthorized persons
  - Specific electronic security systems and requirements are not defined in the HIPAA security rules, allowing nursing homes to select and tailor the security systems and equipment that is appropriate to their organization and facilities

Harmony Healthcare INTERNATIONAL

Nursing Home Regulation HIPAA

- **Enforcement:**
  - The U.S. Department of Health & Human Services, Office for Civil Rights, or OCR, investigates complaints of possible violations of HIPAA security and privacy rules
  - The U.S. Department of Justice investigates Privacy criminal violations
  - The State Attorney Generals Office investigates HITECH violations
  - The OCR also conducts compliance reviews and provides outreach and educational programs

Harmony Healthcare INTERNATIONAL

How the HIPAA Laws Apply to You

- These Rules apply to you when you:
  - Look At
  - Use or
  - Share

  Protected Health Information (PHI)

Harmony Healthcare INTERNATIONAL

Who Uses PHI?

- Anyone who **works with** or may **view health, financial** or **confidential** information with HIPAA protected health identifiers
- Everyone who uses a computer or electronic device which stores and/or transmits information

Harmony Healthcare INTERNATIONAL

Case Scenario

- Florence Nightingale, a long-term care employee is retiring. At her retirement party hosted by the facility, she takes selfies with residents, whom the employee considers to be her family members, and posts selfies to the employee's FB account with captions about her "facility family"
  - Unauthorized disclosure of PHI?
  - Does it matter if the residents "consented" to taking the picture?
  - Does it matter if the employee posted nothing about the resident's health or condition(s)?
  - Does it matter that the employee was retired when she posted the pictures?

Harmony Healthcare INTERNATIONAL

Question & Answer

- **Question:** Can a skilled nursing facility (SNF) display residents' names and pictures on a plaque outside their doors?

Harmony Healthcare INTERNATIONAL

Question & Answer

- **Answer:** Residents' names and pictures can be displayed outside their doors **only** if the SNF **obtains authorization from residents.** If a resident is not capable of authorizing the display of his or her name and picture, the SNF would need to seek authorization from a personal representative of the resident.

Harmony Healthcare INTERNATIONAL

Question & Answer

- **Question:** Do I have the right as a Medicare beneficiary to **access the UB-04 form** that a hospital submits as a bill for payment to Medicare?
- May I access and receive a copy of my coding abstract? I understand that these documents are part of the electronic data that is part of my record, which is considered part of the designated record set.

Harmony Healthcare INTERNATIONAL

Question & Answer

- **Answer:** The Privacy Rule gives you the **right to access records in the designated record set. This is defined as information used by a covered entity to make decisions about individuals.** For providers, the designated record set includes medical and billing records. For health plans, the designated record set includes enrollment, payment, claims adjudication, and case management records.
- The UB-04 form is a billing record, so it is part of the designated record set to which you have access

Harmony Healthcare INTERNATIONAL

Question & Answer

- **The coding summary is an administrative record and may not be considered part of your medical record.** If the covered entity defines the medical record to exclude administrative records, such as coding summaries, the covered entity may deny your request to access your coding summary. However, codes that were submitted for billing will appear on the UB-04.

Harmony Healthcare INTERNATIONAL

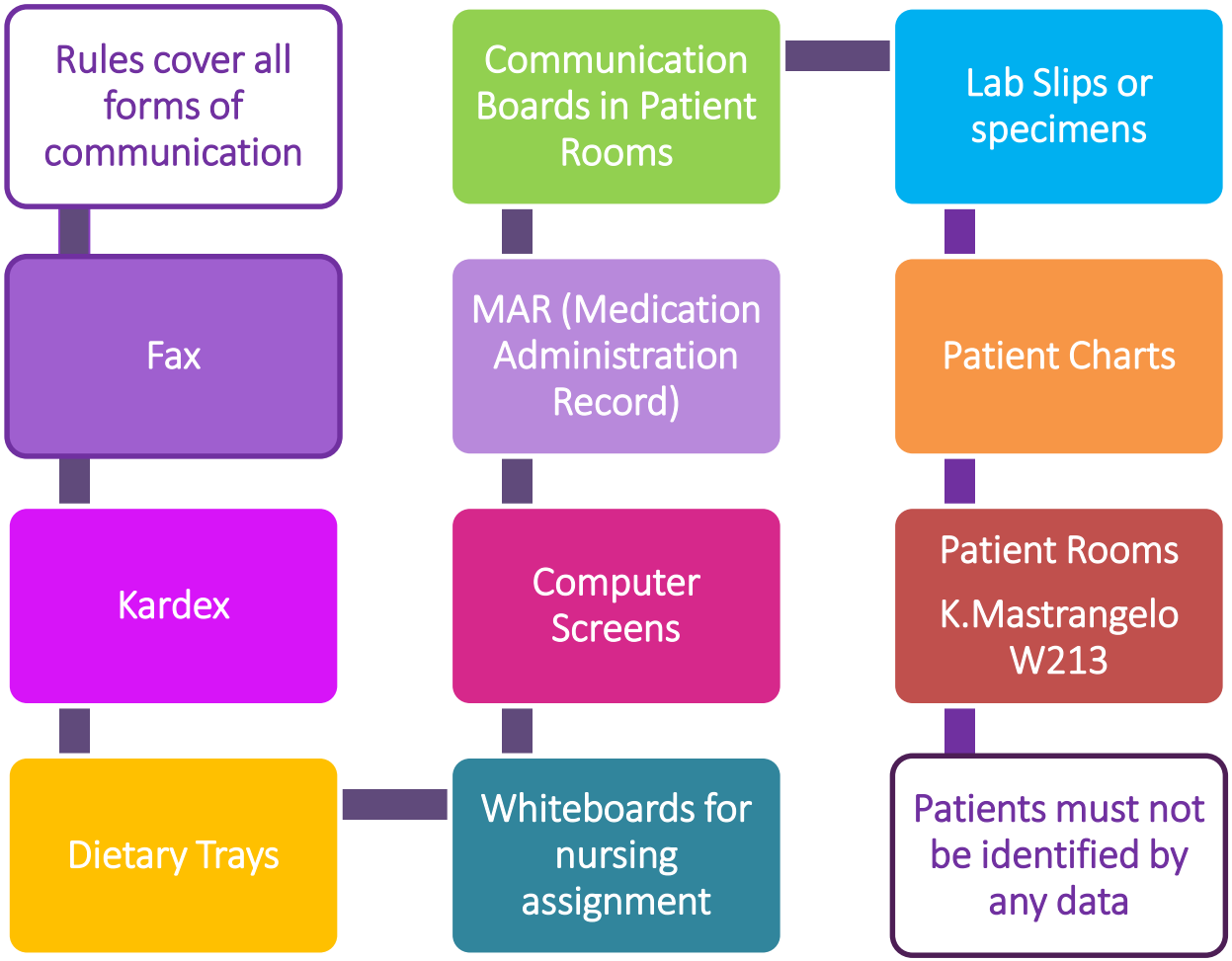
Confidentiality

" General rule is that patient authorization is required for any use or disclosure or protected information that is not directly related to treatment, payment or health operations"

This is to prevent unauthorized disclosure to anyone outside the agency or within the agency

Harmony Healthcare INTERNATIONAL

Confidentiality



Harmony Healthcare INTERNATIONAL

Protecting Privacy
Reporting Privacy Breaches

- Immediately report any known or suspected privacy breaches (such as paper, conversations, suspected unauthorized or inappropriate access or use of PHI) to the Privacy Officer

Harmony Healthcare INTERNATIONAL

Protecting Privacy
How to Report Security Incidents

- Report lost or stolen laptops, Blackberries, PDAs, cell phones and flash drives immediately to security/police
- Report any unusual or suspected information security incidents to supervisor

Harmony Healthcare INTERNATIONAL

SNF Compliance Scenario

- A not-for-profit managed care plan serving the New York metropolitan area did not erase the drives prior to returning the copiers after their lease ended
- Estimated that up to 344,579 individuals may have had their data breached
- The breach cost $1,215,780

Harmony Healthcare INTERNATIONAL

References

- OIG Compliance Program Guidance For Nursing Facilities Federal Register/Vol. 65,No 52 Thursday March 16,2000 Notices
- Compliance 101 Third Edition, Debbie Troklus & Greg Warner
- Health Care Compliance Professionals Manual

Harmony Healthcare INTERNATIONAL

Connect with Kris

- Harmony Healthcare International (HHI)
- 800.530.4413
- www.Harmony-Healthcare.com
- kmastrangelo@harmony-healthcare.com

@KrisMastrangelo @Harmonyhlthcare

facebook.com/HarmonyHealthcareInternational

linkedin.com/company/harmony-healthcare

harmonyhealthcareinternational

Harmony Healthcare INTERNATIONAL

Harmony Healthcare International (HHI)

- Would you like a…

Free Five-Star Analysis

Contact

Matt McGarvey

mmcgarvey@harmony-healthcare.com

Harmony Healthcare INTERNATIONAL

harmony17

Join us at

harmony17

6th Annual LTPAC

Interdisciplinary Symposium

November 2nd & 3rd 2017

Foxwoods Resort, Ledyard, CT

CLICK HERE TO REGISTER

Harmony Healthcare INTERNATIONAL

Thank You

Harmony Healthcare INTERNATIONAL