Information Sharing and HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) became a federal law in 1996 and it is administered by the Department of Health and Human Services (DHHS). Title II of HIPAA regulates patient information sharing by providers, hospitals, health insurance plans, and coding/billing companies. HIPAA aims to protect patient privacy while encouraging efficient access to a wide spectrum of electronic medical records. Unfortunately, because of severe penalties with HIPAA noncompliance, technologic advancements in rapid data delivery are hindered by HIPAA misinterpretation leading to unfounded fears of noncompliance. This document intends to help providers become comfortable with HIPAA and appropriate patient information sharing, an important component in the provision and assessment of emergency medicine excellence.

HIPAA defines *Protected Health Information (PHI)* as any medical information (e.g., provider notes, billing records, and test results) in any form (e.g., electronic, paper, or verbal) that can be linked to an individual. The *HIPAA Privacy Rule* establishes regulations for the use and disclosure of PHI. Once authorized by the patient (or legal guardian), providers commonly disclose PHI in order to facilitate health care treatment, conduct hospital operations, and perform billing/collecting. Providers may openly discuss joint patients unless the patient stipulates a constraint. It is the unusual patient that does not approve PHI sharing and, when unreasonable restrictions are dictated, these can be denied by a provider acting in the best

interest of the patient. As part of their mission, public health departments are allowed to access PHI without permission to ensure community wellbeing.

Obtaining consent for sharing of PHI is a customary component of front-end ED patient registration. At that point, patients are made aware that providers may disclose the minimum necessary amount of data, to the narrowest relevant group, in order to accomplish patient care objectives. Also, patients may dictate PHI sharing within specific parameters of how, what and with whom. For example, an individual can stipulate being notified only via cell phone with test results.

Patients are entitled to obtain a copy of their personal medical records and even request corrections when they find inaccuracies. While there must be a process in place to amend the medical record, providers and hospitals may refuse unreasonable requests.

PHI disclosures that are not part of medical care must be noted in the medical record of what, when, and with whom information was relayed. Hospitals must maintain privacy policies and procedures, appoint a *Privacy Official*, assign a contact person for receiving complaints, and train all staff on HIPAA. HIPAA requires the *National Provider Identifier* (*NPI*), a 10-

digit alphanumeric, to replace all other provider identifiers used by health plans (e.g., UPIN).

HIPAA does not apply and consent for PHI sharing is not needed when data is completely *de-identified*. HIPAA specifies eighteen individual identifiers. Most exactly link to a patient such as name, MRN, phone number, and home/email address. Others are more oblique such as zip code, birth date, and registration date. The birth year is exempted so that exact age can be reported, except those under 1 year old cannot be further defined and those over 90 years of age must be grouped since narrow cohorts (e.g., 9-days or 99-years-old) makes the patient more likely to be identified.

HIPAA allows a *limited data set* (less confining than de-identified data) for marketing and operations studies. Here, the patient's town/zip code may be used as well as elements of dates. Uses of this data do not need to be recorded in the patient records but may not, under any circumstances, be traced back to an individual patient. There must be a *data-use agreement* defining who receives the data recipient what it will be used for. Also, there must be provisions safely transferring files reporting any breaches back to the data provider. Also, there can be no efforts to link data to an individual (i.e., re-identify the data).

HIPAA requires that all entities involved with PHI must control data access, handle data securely, and plan for data recovery. For instance, retrieval of PHI over open networks must be prevented from unintended intercept/alteration and PHI must be removed from retired equipment before disposal. Security risk analysis and management programs are required and HIPAA compliance examines by internal audits. For instance, an auditor may recommend that workstations in high traffic have monitor screens protected from viewing by those unauthorized individuals.

The *Enforcement Rule* sets financial and criminal penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. At this point there have been few prosecutions for violations. Still, a clear understanding HIPAA allows providers and hospitals to comfortably share PHI and maintain compliance with the law. Any individual who believes that HIPAA is not being upheld can file a complaint with the DHSS Office for Civil Rights.

Key Reference

The U.S. Department of Health & Human Services (DHHS), Office for Civil Rights, lists a plethora of online resources at www.hhs.gov/ocr/hipaa.

Glossary

Data-use Agreement – This is require between the data source (e.g., hospital) to a service provider (e.g., EMEX) where is outlined what the data will be used for and that data will not be traced back to an individual patient; Unless there is a breach of data integrity no entry in the patient record is necessary

De-identified Data – This term refers to PHI that has been completely de-identified by not including eighteen specific individual identifiers and then does not require consent for data sharing

Department of Health & Human Services (DHHS) – Federal agency that administrated HIPAA and provides interpretation of gray areas

Enforcement Rule – This sets financial and criminal penalties for violating HIPAA rules and establishes procedures for investigations and hearings

Health Insurance Portability and Accountability Act (HIPAA) – Act of Congress that became law in 1996

Limited Data Set – This term refers to PHI that has been mostly de-identified by retain limited demographic and date/time so that it is useful for marketing and operations studies (such as the EMEX-Compare product)

National Provider Identifier (NPI) – This is a 10-digit alphanumeric that HIPAA uses to replace all other provider identifiers used by health plans (e.g., UPIN)

Office for Civil Rights – Division of DHSS that accepts complaints from any individual who believes that HIPAA is not being upheld

Privacy Official – Hospitals must appoint a Privacy Official to over see HIPAA compliance, review complaints, and participate in internal audits

Privacy Rule – Portion of HIPAA establishing regulations for use and disclosure of PHI

Protected Health Information (PHI) – Any medical information in any form that can be linked to an individual

Title II – Section of HIPAA that regulates patient information sharing by providers, hospitals, health insurance plans, and coding/billing companies