Sunbridge
home health care

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

Health Insurance Portability and Accountability Act (HIPAA) Inservice Handout

1. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as "Kennedy-Kassebaum", passed congress rapidly and with great bipartisan support in 1996. Many aspects of the legislation have been implemented in the ensuing years; the deadline for full implementation of the privacy and confidentiality requirements was April 14, 2003. Health care providers and organizations have strict guidelines that must be followed to remain within the law. While this module and most of our attention now is focused on the provisions of the legislation that deal with privacy, confidentiality, and security of patient records, HIPAA also contains other requirements that have an impact on employers, insurance companies, and purchasers of health insurance coverage.

HIPAA was designed to address public concerns about managed care, insurance availability, and insurance affordability. For example, HIPAA prohibits insurance companies from denying coverage because of:

1. preexisting conditions,
2. a family member's health status, or
3. whether or not an individual has been covered under a group policy and is seeking a personal health insurance policy.

Further, HIPAA ensures immediate coverage without regard to pre-existing conditions for individuals who change jobs and insurance carriers. HIPAA also established a pilot program for medical savings accounts (MSAs) that allows individuals to create a "health insurance individual account" to purchase health services and retain unspent funds rather than paying monthly premiums. Further, to encourage the purchase of long-term care insurance, HIPAA allows employers to deduct premiums and most benefits are tax-free to the beneficiary. Additionally, to facilitate purchase of health insurance by self- employed persons, the law allows 80% of the annual premiums to be tax-deductible by 2006. While many health policy analysts agree that these provisions have little impact on reducing the number of uninsured, they do, however, think these efforts are worthwhile. At this time, however, attention to HIPAA is riveted on implementing and paying for the privacy, confidentiality, and security aspects of the legislation (DiBenedetto, 2003).

In 1996, HIPAA was viewed as a way to reduce administrative costs, provide better access to health information, reduce fraud, and guaranty privacy of health information. However, the American Hospital Association estimates that it may cost

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

between $4 billion and $22 billion to implement the tenets of the law. A search of the literature failed to produce specifics regarding cost; however, according to Gue and Upham (2004), the majority of costs are associated with developing and implementing software that integrates providers, payers, and governmental agencies.

As part of the HIPAA rule promulgation, the Centers for Medicare and Medicaid Services CMS mandated standardization of transaction and code sets (TSC) to reduce duplication, confusion, and non-compliance. CMS standards rely on use of ICD-9 codes for discase classification, CPT codes for procedures, and national drug codes (NDC) for medications. CMS admits that problems with these coding sets exist; new ICD-10-CM and ICD-10-PCS are thought to reduce the ambiguity and facilitate full implementation of electronic processing. The industry is working toward integrating HIPAA fully, it is just taking longer than they hoped to get the electronic interfaces coordinated (Gue and Upham 2004).

HIPAA is just the beginning of the ultimate conversion of healthcare information into an electronic health record (EHR). The Bush administration projects it will cost $100 million a year for 10 years primarily to fund demonstration projects and trial programs aimed at achieving four major goals:

1. establish routine use of EHRs in clinical practice,
2. connect health care workers in information exchange for clinical decision making,
3. enhance patients' ability to choose providers based on quality, and to integrate public health surveillance systems into an interoperable network to support new research and better care (Scott 2004, p. 34).

2. The Basics

HIPAA contains provisions for both privacy and security. Privacy rules have been promulgated and compliance was required by most health plans by April 14, 2003; plans with less than $5 million in annual receipts had until April 14, 2004 to fully comply. These rules have gone through several iterations, some as recently as March 2003 and refinements continue. Security rules that detail further requirements for the health care industry and patients were issued in October 2004.

A key factor for all health care providers and organizations to keep in mind is that, while HIPAA rules are strict, if state law covering the same topic is more stringent, the state law must be followed (Herrin, 2003). Health providers are well advised not to overlook state law as they accommodate HIPAA, Providers and organizations must remain up-to-date with both HIPAA and state law changes.

The intent of HIPAA is to protect patients from unauthorized or inappropriate use and access to their health information. Further, the rules protect patients by giving them access to their health information so they know what has been documented about their health status. Proposed by- products of HIPAA are to improve quality of care,

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

restore trust in the health care system, and improve the efficiency and effectiveness of information dissemination by building on existing legal frameworks. HIPAA also contains an administrative simplification section designed to improve the efficiency of health information coding to facilitate digital transfer of information between and among health care providers, payers, and health plans.

HIPAA creates safeguards so that only those people or entities having a real need to know health information will be able to access it (Calloway and Venegas 2002). The HIPAA rules complement other standards that protect patients' rights. Compliance with privacy rules promises to be a cornerstone of future JCAHO and Medicare/Medicaid surveys. Remember, compliance is mandatory, not voluntary.

3. Why is HIPAA Needed?

Health care professionals have long realized the need to protect patients from unauthorized use of their health information; at the same time, they want to have access to needed information when treating a patient. Widespread use of electronic data is facilitating the rapid transfer of information and the Institute of Medicine has urged the creation of standards so electronic records can be available (Follansbee, 2002).

Similarly, the public is greatly concerned about the privacy of their medical records. Prior to the electronic medical record, patient information was maintained in paper form and neatly locked away, accessible only to those who had authorized access. With computerized records information can be accessed, changed, distributed, and copied with far less regard for appropriate authorization (Follansbee, 2002).

Serious breaches of record confidentiality have occurred. An employee of the Hillsborough county health department was able to carry home a disk with the names of 4000 HIV positive patients. People have purchased used computers that contained prescription records of patients; Eli Lilly recently sent out an email with the names of patients taking Prozac; the University of Montana inadvertently placed the medical records of some 62 people on the internet. Consequently, patients, health care providers, and other health care entities are very concerned about confidentiality, restoring the public trust, and protecting themselves from lawsuits.

Yet, the ability of multiple providers to access a patient's record can significantly improve the overall quality of care. Think about the chronically ill individual who receives care from more than one or two specialist providers. If each provider has access to the most recent treatment plan, it stands to reason that care will be more coordinated, efficient, and effective.

4. Understanding HIPAA

HIPAA describes those affected by the law as "covered entities". Included under this

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

umbrella are health care providers, health plans, health care clearinghouses, and business associates.

Health care providers are defined as anyone who is paid for health care services or bills for services provided. The list is all inclusive: physicians, licensed health care providers, hospitals, outpatient physical therapists, social workers, certified nurse midwives, technicians administering X-rays done at home, home health agencies, pharmacists, providers of home dialysis supplies and equipment, nursing homes, nurses, and nurse administrators. This list means that any hospital or health facility worker who may see confidential patient information is included.

A health plan is any individual or group that pays for health care services. Included are health maintenance organizations (HMOs), insurance companies, Medicare/Medicaid, self-insured plans, employee group plans, federal plans such as CHAMPUS, military, veteran's administration, and Indian health services.

Clearinghouses are those entities that receive health information from providers and health plans. They typically are responsible for standardizing the information to improve claims processing. Included in this group are third-party administrators, billing services, and re-pricing agencies.

The *business associate's* category covers a broad range of professionals and services. Included are attorneys, consultants, auditors, accountants, billing firms, data processing companies, and practice management firms. Nurses working as independent contractors, i.e., case managers, legal nurse consultants, and educators are included and subject to compliance with HIPAA law. A contract between the business associate and hiring agent must be in place before the associate can see any patient information.

5. What Health Information is Protected

HIPAA created two new phrases to describe information protected by the legislation. The medical record is now referred to as protected health information (PHI). This includes all information that is created by any covered entity. All forms of the information are part of protected health information, i.e., paper, electronic, video tapes, photos, audiotapes, and any information that has been duplicated, discussed, read from a computer screen, or shared over the internet.

The other new HIPAA phrase is individually identifiable health information (IIHI). Included in this category is any information that could reasonably be linked to a specific patient, such as a photo, name, address, date of birth, next of kin or responsible relative, medical record identifier, social security number, driver's license number, health beneficiary, account number, employer, finger, or voice prints.

The law specifics that some information that is not individually identifiable can

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

remain. Age that is reported as 60+ if the patient is older than 60, zip code if the patient lives within a zip code with greater than 20,000 people in it, race, gender, ethnicity, marital status, and the year only of the health care occurrence are not considered individually identifiable information and these data may be used in the aggregate.

All facilities must limit access to information only to those who have a need to know. A nurse who seeks information about a patient not under her care is violating the HIPAA rules. Similarly, health information can only be used for health purposes. Employers cannot use the information to screen candidates for hire or promotion. Financial institutions may not use it to determine lending practice. Only the patient can explicitly authorize employers, banks, and individuals to have access to his/her medical information.

HIPAA also established the "minimum necessary rule" which stipulates that only the minimum necessary information may be shared, even with the patient authorization. A classic example would involve treatment for a case of child or domestic abuse; the provider would, rather than providing an entire medical record, furnish the pertinent data furnished in the form of an abstract outlining the information that is necessary to provide treatment and protect the victim(s). The abstracted information could be provided to legal and law enforcement entities. Health providers involved in the treatment of patients are not subject to the minimum necessary rule and can have full access to all information that is needed to provide patient care. Health information that has implications for the public health and safety can be shared without consent. There are several situations where medical information can be shared: In Emergency 911 situations, when communicable diseases are involved, when law enforcement agencies participate, or if national defense or security is a factor.

The public health department is deemed a legitimate recipient of certain personal health information and providers may, in fact in some instances, must report some findings to the proper public health agency. Included are:

1. cause of death even when the patient dies at home
2. reportable communicable diseases
3. child abuse
4. reporting an adverse drug reaction to the Federal Drug Administration
5. occurrence of cancer in a state with a cancer registry
6. meningitis, and
7. immunizations for children.

These examples are thought to be important to the health of the public (Campos-Outcalt 2004).

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

6. Patient Consent and Authorization

HIPAA makes a distinction between informed consent and patient authorization. Patients are entitled to know exactly how an entity plans to use the information.

Informed consent is signed at the first encounter the patient has with the provider/health care facility; the consent covers treatment, payment, and other health care information. The meaning and use of the patient's consent must be carefully explained to the patient. Facilities must explicate their disclosure process in a document called Information Practices. The American Hospital Association published a sample consent and explanation document that was 10 pages long. The document explains patient rights, as well as a description of how patient information is collected and used. Facilities must decide how and when the information concerning consent is presented to patients and how patients can use their right to revoke consent. Patients must also be advised about the agency's policy that covers conditions for admission that are related to consent.

Patients may also sign authorizations. These are required when information is used by the agency for purposes outside of treatment. Agencies must assess their policies and procedures to assure that they are always using an authorization when it is needed; some agencies may not realize that information sharing policies violate the patient's right to restrict release of data (Cichon, 2002). Patients must be fully informed about the way agencies use a signed authorization and are entitled to receive a free accounting every twelve months describing how their health information has been used.

HIPAA privacy regulations also mandate specific patient rights that include the following:

1. Right to privacy notice requires disclosure and reasonable effort to assure that the patient understands the agency's policy concerning privacy of information.
2. Right to request restrictions means that patients may specify health information that cannot be released and/or, they may restrict to whom information can be released. 3. Right to access of PHI means that patients must be allowed to inspect and copy information contained in the agency's record.
4. Right to know what disclosures have been made means the agency must track all information released and be able to provide documentation to the patient.
5. Right to amend the PHI means that while patients may request amendments to the PHI and the agency must allow amendments, the agency may deny some requests.

All covered entities are required to comply with certain procedural rules. Most have had to develop new policies and procedures to address the many aspects covered under these rules. The following are some of the rules:

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

1. Agencies must appoint a privacy officer who will monitor and audit compliance.
2. Agencies must develop an internal compliance process that will assure no patient rights are violated, complaints are addressed and investigated, and that a process for remediation is in place.
3. Training must be provided to employees to assure that they are informed about patient rights and disclosure of information.
4. HIPAA requires that agencies document any and all violations and that sanctions parallel other disciplinary policies.
5. Agencies must have a process for mitigating any harmful effect of disclosure.
6. All forms of communication must be addressed in administrative safeguards.
7. Agencies must agree and have policies that specify no retaliation for an employee or consumer who files a complaint.

7. Practical Implication

Questions about the implications HIPAA rules have been numerous. Can an office or laboratory have a patient sign in sheet? Can you use a patient's name to call him into a treatment room? Can the patient's name be posted outside the hospital door? At this point, there is some agreement about some of these. As long as personal information regarding the patient's care or procedures to be done remain confidential, names can be outside hospital room doors, patients can be verbally called to treatment rooms, etc. New questions will undoubtedly arise in the future. Staying informed about the rules and regulations concerning HIPAA will be every health care worker's obligation.

Sign-in sheets, once disallowed, can now be used along with bedside charts as long as reasonable precautions are taken to safeguard patient information. Sign in sheets can only have the name and time; no information about the nature of the appointment can be included. The patient can give consent or may decline to have information given to family members; facility staff is not obligated to verify the identity of relatives.

HIPAA retains the rights of parents as the personal representative for minor children. There are exceptions, however. Parents may decide that the child and provider have a confidential relationship that excludes the parent from receiving information. A provider may choose to exclude the parent when abuse is suspected or when including the parent would endanger the child.

Patients have the right to restrict clergy visits and religious information. If the patient does want the clergy to visit, health care individuals should provide only the name and location of the patient. They should not provide any information about the patient's medical condition. Further, patients have the right to restrict informing callers or visitors that they are in the hospital. Most patients are asked on admission to the facility if they want such restrictions and, if they do, hospital workers may not acknowledge that a patient is in the hospital even including visitors, florists delivering flowers, etc.

1313 13th Avenue Decatur, AL 35601
Office: 256-580-5800
Fax: 256-580-5801

Some information can be provided to law enforcement without patient consent. Emergency technicians can contact the police at a crime scene and convey nature and location of the crime. Information about a suspicious death may also be reported to the police. HIPAA has a one call rule that permits contacting an organ procurement agency following a death.

Repositories that store human tissue and fluids for future scientific analysis, i.e., genotyping, cell lines, other biotechnologies, express concern that HIPAA will fundamentally change how those commercial repositories function. At question is whether property rights continue to apply to human tissue after removal from the body. Prior to HIPAA, the Supreme Court in California ruled on the side of future research and determined that property rights end when tissue is removed from the body (Allen 2004). However, depending on how HIPAA rules are interpreted, informed consent may be required in order for research to be conducted on removed tissue.

8. HIPAA and Research

Patients must sign an authorization to allow their information to be included in research projects. Information can only be disclosed in accordance with a research protocol approved by an institutional review board. All identifying individual information must be removed. One difficulty researchers may experience is the lack of specific guidance from HIPAA regarding construction of compliant, de-identified data sets, at this point researchers are developing strategies that they believe comply with the intent of privacy under HIPAA. Ongoing analysis of medical information is critical for developing strategies to improve patient outcomes and reduce medical errors (Clause, S.L.; Triller, D.M.; Bornhorst, C.P.; Hamilton, R.A.; Cosler, L.E. 2004). Information that can be used in compliance with HIPAA includes: gender, race, ethnicity marital status, dates of treatment if reported in years, age (for individuals older than 60, one must use 60+), and zip code if more than 20,000 reside in that zip code (Erlen, J.A. 2004).

9. Conclusion

HIPAA regulations require new behavior from health care professional and health care facilities. Close coordination with other partners in health care delivery and reimbursement is mandatory to assure a continuous process of patient privacy.

Restrictions and the ability to amend IIHI give patients new control over their health information. Health care professionals may be challenged. Involving patients as active participants in their care will dispel and avoid potential problems.

Administrators are advised to be sure staff is well-trained and knowledgeable about the requirements of HIPAA. Similarly, they many want to scrutinize day-to-day practices to evaluate whether violations of patient rights are occurring.