HIPAA and Network Security

Curriculum

This curriculum consists of an overview/syllabus and 11 lesson plans

Week 1

Developed by
NORTH SEATTLE COMMUNITY COLLEGE
for the IT for Healthcare Short Certificate Program

Funded by the Seattle Community-Based Health Care Partnership Project

Seattle CENTRAL Community College
NORTH Seattle Community College
SOUTH Seattle Community College
SVI Seattle Vocational Institute

This product was funded by a grant awarded under the President’s Community-Based Job Training Grants as implemented by the U.S. Department of Labor’s Employment & Training Administration. The information contained in this product was created by a grantee organization and does not necessarily reflect the official position of the U.S. Department of Labor. All references to non-governmental companies or organizations, their services, products, or resources are offered for informational purposes and should not be construed as an endorsement by the Department of Labor. This product is copyrighted by the institution that created it and is intended for individual organizational, non-commercial use only.
Week 1: HIPAA Definition, History, and Standards

Note: I have set up the entire curriculum for this class with weekly lesson plans. This will allow the Instructor to determine how to incorporate the information into lesson plans whether it is a daily class, a twice weekly class, a three times a week’s class, or even a one class per week calendar.

HIPAA – Health Insurance Portability and Accountability Act is a federal law that passed in 1996 seeking to make health insurance more efficient and portable. HIPAA has administrative simplification (billing and other transactions) that will save the healthcare industry billions of dollars. Due to public concerns about confidentiality, HIPAA also addresses information protection, such a protecting the privacy of the patient’s personal and health information. It provides for electronic and physical security of personal and health information. HIPAA objectives are:

- To ensure the portability of health insurance
- To prevent health care fraud and abuse
- To ensure the security and privacy of health information
- To enforce health information standards that improve the efficiency of health care deliver, simplify the exchange of data between health care entities, and reduce cost
- To reduce the paperwork associated with processing healthcare transactions

History:

HIPAA was also known as the Kennedy-Kassebaum Bill, it was the first federal legislation to protect automated client records and to provide uniform protection nationwide. There were previous attempt to legislate medical records, which includes the Individual Privacy Act, the Fair Health Information Practices Act of 1995, and the Medical Records Confidentiality Act of 1995 – none of these bills passed.

The Privacy Act of 1974 protected federally managed records (Medicare and Medicaid) and mandated that federal agencies develop, implement, and disclose their plans for maintaining the security of stored data. Because there was no similar federal mandate for private institutions or providers, European Agencies refused to transmit medical information to the United States. Remember, this was before the widespread computer use. Medical records were protected differently from state to state, which necessitated practitioners to be familiar with regulations in the state they practiced in.
Standards:

Legislative, regulatory, and accreditation issues and quality initiatives place excess demands on health care providers to safeguard, track, provide, and manage information. Examples of some of the organizations that perform accreditation and establish standards for health care delivery:

- Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
- Commission for Accreditation of Rehabilitation Facilities (CARF)
- National Committee for Quality Assurance (NCQA)
- American Medical Accreditation Program (AMAP)
- Accreditation Association for Ambulatory Healthcare (AAAHC)
- American Association for Accreditation of Ambulatory Surgical Facilities (AAAASF)

Information systems can and must facilitate a process for the demands placed on healthcare providers. HIPAA compliance requires a broad approach that incorporates administrative and technical procedures. Education, the development and enforcement of policies, and process changes are key factors.

HIPAA had such broad scope and complex nature that it resulted in an extensive definition of its’ rules. This was accomplished in steps since its enactment in 1996.

- Privacy Standards: April 2003; protect an individual’s health information and provide patients with certain rights. Compliance was to be April 14, 2003, but for some small health plans they were given until April 14, 2004 to achieve compliance (Final Privacy Rule 2002)

- Security Standards: Final Rule Published February 20, 2003 – Physical, technical and administrative safeguards of patient information that is stored electronically. Became effective in 2005

- Codes and Transaction Standards: October 2003 – Standardization for electronic billing and claims management.

The **HIPAA Privacy Rule Compliance** mandates for both administrative and technical procedures to protect privacy.

Administrative procedure include information access controls, contingency plans, formal mechanisms for processing records, security configuration and management, security incident procedures, security management processes, security training, certification of compliance, chain of trust partner agreements, and termination procedures.
Technical procedures include audit controls, authorization controls, data authentication, communication and network controls, encryption, and various types of authentication for event reporting, integrity controls, message authentication, message integrity, and user authentication. (Give examples of signing on to the computer or signing into an Application – this User Authentication. Ask class what is message integrity? What is message authentication? Why would we need this – good place for class discussion.)

Each healthcare facility must designate a chief privacy officer who is assigned the accountability for HIPAA compliance. The privacy officer also is able to give more HIPAA Privacy training to employees (or direct the employee to the correct person/department), written information that describes how HIPAA affect the individual job of the employee, and is available to answer questions from employees.

One very visible requirement of the privacy rule is the requirement that all health care consumers must receive a privacy notice. These notices include the following content:

- Responsibility of providers to protect privacy, provide a notice of privacy practices, and abide by the terms of the notice
- Description of individuals’ rights, including the right to complain to the provider in the event that the individual believes that his or her rights have been violated
- Point of contract for further information and complaints

**The HIPAA Privacy Rule Compliance** includes requirements for electronic signature standards. Electronic signatures include an encrypted digital tag added to an electronic document. This allows for the following features:

- User authentication that guarantees the user’s identity
- Provides evidence that supports the validity of the signature
- Ensures the integrity of the message

Why would this be important? Who would use this feature? (Class discussion on importance of understanding that logging onto a Clinical Software Application may be the user’s electronic footprints/signature – what does this mean for a Healthcare Professional?)

**The HIPAA Security Rule Compliance** mandates safeguards for the physical storage, maintenance, transmission, and access to patient’s health information to ensure its confidentiality, data integrity, and availability when require for treatment. The date for compliance was identified as April 2005. This rule also requires the appointment of a security office, just as the privacy rule required.
HIPAA Electronic Data Interchange (EDI) and Transaction Rule

The Centers for Medicare & Medicaid Services (CMS) published regulations in August 2000 mandating all providers, insurers, and middlemen involved in health care claims submission, referrals, eligibility verification, and the transmission of other client related information to use a common format to send and receive electronic information by October 2002 – and act of Congress extended that to October 2003. Paper claims are exempt from this requirement.

In other words, electronic claims submission now must meet standards set forth by HIPAA. The standards were established to streamline the claims submission process. Providers have the option to buy and maintain a HIPAA compliant practice management system (PMS) or to use a claims clearing house to meet this standard. (Hand out attached article clarifying clearing houses, and have discussion with class of how hard was it for health care providers to comply with HIPAA)

HIPAA legislation includes descriptions of the various penalties for noncompliance, which can be severe. For example, the penalty for violating transaction standards is up to $100 per person per violation and up to $25,000 per person per violation of a single standard per calendar year. Penalties for wrongful disclosure of client information include large fines as well as possible imprisonment. How easy would it be to share information? Give example (You are working in Medical Records, or at the Helpdesk, or are a MA or LPN and have access to the Clinical Software Application in your daily work. A close friend’s sister is in the hospital where you work at, and they are anxiously awaiting some lab results. They ask you to look in the Clinical Software Application and see if the lab results are there. You look it up and give them the results. What could be the consequences of this action? Per HIPAA? Personal – i.e., the lab results are incorrectly understood to the bad – resulting in unnecessary stress and pain, or the lab results are incorrectly understood to the good – and the patient checks out Against Medical Advice (AMA)

Information systems and the design of automated documentation (i.e., clinical application software) must incorporate safeguards for the information privacy as well as standards for quality of care imposed by accrediting agencies.

Accrediting agencies such as JCAHO and CARF, Medicare and Medicaid regulations, third-party payors demands, state and feral laws and ambulatory payment classifications dictate documentation requirements in clinical applications.

Commission on Accreditation of Rehabilitation Facilities (CARF) is an accrediting body, with a focus on the improvement of rehabilitative service to people with disabilities. CARF provides accreditation in the following service areas: adult day services, assisted living, behavioral health services for the visually handicapped, employment and community services. CARF is a private, nonprofit organization that uses input from consumers, rehabilitation professional, state and national organizations.
Joint Commission for Accreditation of Healthcare Organization (JCAHO) mission is to “improve the safety and quality of care delivered to the public through the provision of health care accreditation and related services that support performance improvement in health care organizations.” JCAHO standards shape organization practice and documentation, thereby affecting information system documentation design. When accreditation standards change, documentation must reflect the new/revised requirements.
Week 1 – Assignment 1
LAB – Week 1

Assignment: JCAHO introduced information management standards for health care organizations in 1994. Please give me a brief description of 3 standards. (Answer sheet to follow lesson plan)

LAB: This will be when to introduce the class to the lab portion. In the first lab the students should be familiarized with the computer, computer lab rules, and hours. A brief discussion should occur on Internet Research – what are search engines? How does one search? Does everyone know how to print? Save favorites/bookmarks?
Assignment #1
JCAHO Standards
Lesson Plan 1 –

Assignment: JCAHO introduced information management standards for health care organizations in 1994. Please give me a brief description of 3 standards.

Standards:

1. Measures that protect information confidentiality, security, and integrity, inclusive of:
   • Determining user need for information access and level of security
   • Easy, timely retrieval of information without compromising security or confidentiality
   • Written and enforced policies restricting removal of client records for legal reasons
   • Guarding records and information against loss, destruction, tampering, and/or unauthorized use

2. Uniform definitions and methods for data capture as a means to facilitate data comparison within and among health care institutions

3. Education on the principles of information management and training for system use. This may include education about the transformation of data into information for subsequent use in decision support and statistical analysis.

4. Accurate, timely transmission of information as evidenced by the following characteristics:
   • Twenty-hour availability in a form that meets user needs
   • Minimal delay of order implementation
   • Quick turnaround of test results
   • Pharmacy system designed to minimize errors
   • Efficient communication system

5. Integration of clinical systems (i.e., pharmacy, nursing, laboratory, and radiology systems) and nonclinical systems for ready availability of information

6. Client specific data/information – the system collects, analyzes, transmits, and reports individual client-specific data and information related to client outcomes that can be used to facilitate care, provide a financial and legal record, aid research, and support decision making.

7. Aggregate data/information – the system generates reports that support operations and research and improve performance and care. For example, information may be provided by practitioner, client outcomes, diagnosis, or drug effectiveness.

8. Knowledge-based information- Literature is available in print or electronic form

9. Comparative data- the system can extract information useful to compare the institution against other agencies. Deviations from expected patterns, trends, length of stay, or number of procedures performed may be noted.
On Finance: Examining the Claims Clearinghouse Market

Feb 1, 2003
By: Charlotte A. Martin
Managed Healthcare Executive

For those healthcare providers and payers who still believe large claims clearinghouses are the only way to reduce administrative costs, it may be time to think again. This widely held industry myth is being dispelled today by new savvy players who are proving that big national clearinghouses can be expensive and are not the only way to go.

At one time large clearinghouses could in fact leverage their market power to reduce the price of processing claims and other electronic transactions. Providers and payers, receiving these discounts through exclusive arrangements with the large claims clearinghouses, believed they had the best deal around.

HIPAA regulations took effect and stiff business competition abruptly changed the industry’s trust in a "big clearinghouse" concept as the only available option. Once stung with increasing administrative costs, confusion, and lost claims, many providers challenged the status quo. Larger providers, who had the technical expertise and financial wherewithal, found they could send their claims directly to many payers to avoid the cost and hassle of the large middleman clearinghouses. Meanwhile, some larger providers eventually discovered the value in clearinghouse services. They quickly began to appreciate the economies of scale inherent in a clearinghouse, those advantages allowed them to offer services that large practices needed, but couldn’t afford, such as converting reports, telecommunication costs, data abstraction, reporting, formatting different transactions, and implementing multiple transactions with multiple payers, among others.

Concurrently, smaller stealth clearinghouses began to gain momentum by luring away the small providers with better service at a time when HIPAA shook the marketplace. And to survive in this otherwise shaky market, the clearinghouses that could not rely on the large reimbursement from payers began to increase their efficiency, and hence market power.

Then, for the first time in years, providers and payers cut their relationships with large players and learned how to get better service at reduced prices through small, nimble regional clearinghouses, which could offer parallel services with lower prices and higher quality. This powerful transition is still in play. Yet, as the marketplace continues to change, there is still a lot of confusion and a few myths remain.

Myth: Clearinghouses are not paid by payers.

Truth: Clearinghouses are in fact paid by payers, with industry transaction fees ranging from $0.07 to $3.55 per transaction. This payer support of electronic claims is critical to offsetting the cost to providers.

Myth: Large clearinghouses are bad for the industry.

Truth: Exclusive relationships by payers with one single clearinghouse present new challenges in the industry. Exclusive relationships are believed to inhibit provider’s freedom to work with many
clearinghouses, which then reduces their ability to send all of their claims electronically. After all, no single clearinghouse has connections to every payer. Exclusive relationships can also add another layer of administrative inefficiency, and ultimately may reduce payer bargaining power. In today’s free marketplace, price and service matter most to customers. Moreover, when there are barriers to electronic exchange of data, choice is limited and lack of competition begins to affect the quality of service.

Myth: Providers pay additional money to send their claims through a clearinghouse but receive no financial benefit for claims transactions.

Truth: Efficient claims transactions, especially electronic transactions, can offset the cost of claims transmission and speed up payment by as much as two weeks.

Myth: Transaction fees will increase because of HIPAA.

Truth: The cost of transaction fees remains in the control of each clearinghouse. As part of its commitment to its valued customers, however, many clearinghouses, especially the smaller ones, have made the commitment not to raise prices during the HIPAA crisis, but, given this environment, find they can increase service offerings through access to additional transactions and provide other value-added services.

Myth: All clearinghouses can accept and send all formats from all providers and all payers.

Truth: Not all clearinghouses have the flexibility to accept non-compliant formats from providers and accurately translate them into fully HIPAA compliant formats to payers. In addition, not all clearinghouses have been able to process HIPAA compliant formats and get them to payers who are still only able to take in non-compliant formats.

Myth: Real-time transactions are today’s only industry focus.

Truth: HIPAA is in general continuous to be the prime industry focus.

Myth: The need for clearinghouses will go away once HIPAA is implemented.

Truth: Most small provider offices do not have the resources to connect to hundreds of payers. They need the convenience and technology that a good clearinghouse will provide. In addition, most offices cannot afford the costly upgrade that many software companies charge them to be able to produce HIPAA compliant transactions. They will need to rely on a clearinghouse to translate their transactions. Like the consumer-centric model taking hold of the health insurance market, the onus is now on payers and providers to consider the most value-added proposition when considering claims clearinghouses. Clearinghouses that focus on maintaining high-quality customer service and offer immediate resolution to outstanding or otherwise dead claims will most likely survive.

Charlotte A. Martin is president and chief operating officer of Gateway EDI.
IM.7.9 The hospital can quickly assemble and have access to all relevant information from components of a patient's record, when the patient is admitted or is seen for ambulatory or emergency care.

IM.7.10 Medical records are reviewed on an ongoing basis for completeness and timeliness of information, and action is taken to improve the quality and timeliness of documentation that impacts patient care.

IM.7.10.1 A representative sample of records is included in the review process.

IM.8 The hospital collects and analyzes aggregate data to support patient care and operations.

IM.9 Knowledge-based information systems, resources, and services meet the hospital's needs.

IM.9.1 The hospital's knowledge-based information resources are available, and authoritative.

IM.10 Comparative performance data and information are defined, collected, analyzed, transmitted, reported, and used.

WRAMC Information Management Plan

You are Visitor No. 00177480 since 12/05/2001
This page was last updated on 20 SEP 4