Health Insurance Portability and Accountability Act
Privacy and Security Rules
Hamilton Health Care System

2019

Course Objective

- After completing this topic, you should be able to define client confidentiality, describe protected health information (PHI) and client rights regarding it, and describe the Health Insurance Portability and Accountability Act (HIPAA) compliance practices.
- You will be aware of common mistakes made by healthcare workers and will be able to apply your knowledge to real life scenarios following HIPAA guidelines.

Workforce Responsibilities Under HIPAA:

- As you move through this CBL keep in mind these Workforce Responsibilities and think about how you can use the Responsibilities in your day to day activities.
  - Maintain patient privacy by safeguarding PHI
  - Become familiar with Hamilton Health Care System's (HHCS) Privacy Policies and Procedures
  - Recognize common privacy mistakes and how to avoid them
  - Ask a Supervisor before using or disclosing PHI in a way not allowed by the Notice so a patient can sign an Authorization, if needed
  - Report possible Privacy Policy violations to Supervisor, Privacy Officer or Corporate Compliance Officer

Why do we need Confidentiality regulations?

Why do we need Confidentiality regulations?

HHCS has committed itself to ensure that patients receive the best possible care and that their rights are protected.

We want patients to be confident that their information will be protected so that they will be comfortable disclosing complete and accurate information such as medical history, condition and symptoms.

Patient care could be compromised if the patient does not fully disclose their information due to mistrust in our facility.

Today, standards are present to protect confidentiality and to alleviate patient concerns in this area.

HIPAA: Privacy and Security

Privacy and Security regulations have been put into place to protect the confidentiality and privacy of our patients.

- The HIPAA Privacy Rule is part of a larger federal rule called the Health Insurance Portability and Accountability Act (HIPAA). This act was created in 1996 and is designed to protect the privacy of health information.
- Each health care facility must comply with the HIPAA Privacy Standards. Health care facilities must inform clients of their privacy policies and provide training to all staff and volunteers regarding HIPAA regulations. Noncompliance with HIPAA regulations is a federal offense.

The HITECH Act

- The HITECH Act is a federal law which amends HIPAA and contains a breach notification obligation.
- If a Security Incident or other unauthorized access, use or disclosure of PHI occurs, immediately report it to the Privacy Officer.
- The Privacy Officer will assess whether the incident falls within the definition of a “breach” under the HITECH Act.
- Not all incidents are breaches under the HITECH Act, and legal analysis can be helpful.
- If an incident is determined by HHCS to be a HITECH Act breach, then HHCS must notify the individual patients involved, the media and HHS, depending on how many patients were involved.
- The report to HHS is posted publicly on the HHS website.

The HITECH Act

- Under the HITECH Act, the Georgia Attorney General can file a lawsuit on behalf of Georgia citizens involved in a breach of their PHI
  - These lawsuits can seek money damages of up to $100 per violation with a maximum of $25,000.
- Also, money penalties can be imposed by HHS for violations of the HITECH Act
  - These penalties can range from $100 up to $50,000 per violation.

Examples of Potential HITECH Breach

- Laptop containing PHI is stolen from a car.
- Medical records faxed or emailed to the wrong person.
- Office is broken into and records or computers containing PHI are stolen.
- Medical records are left at restaurant.
- Mobile device containing PHI is stolen or lost.

If you believe a potential breach has occurred, contact the Privacy Officer immediately.

Important Terms

PHI – Protected Health Information

- Any patient identifiable medical and billing information
- This term used under the HIPAA Privacy Rule

ePHI – Electronic Protected Health Information

- Any PHI that is transmitted or stored in Electronic Media, Email or wireless phones (e.g. Ascom phones)

HIPAA Governance

- Privacy and Security Rule – Department of Health and Human Services Office for Civil Rights ("OCR")
- OCR can audit health care facilities
- OCR can investigate complaints

Privacy Overview: HIPAA...

- Is a federal privacy law that establishes how health care workers should handle medical information
- Requires HHCS to notify patients of their rights and provides them a process in which to exercise those rights
- Defines patient identifiable medical and billing information, including genetic information, as PHI
- Outlines how HHCS can properly use and disclose PHI
- Requires that HHCS protect PHI from misuse or inappropriate disclosure

Notice of Privacy Practices

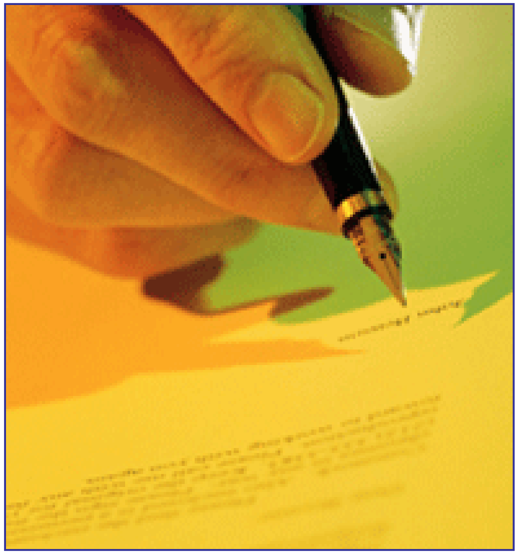
Patients will be asked to sign an Acknowledgment stating that they have been shown and offered a copy of the Notice of Privacy Practices.

- Must be given written Notice of Privacy Practices
- Must give authorization before providers can disclose PHI outside of treatment, payment and health care operations
- Has the right to request restrictions of use and disclosures of PHI
- May request to correct PHI
- May view their medical records or obtain a copy of the medical record
- May request an accounting of disclosure of their PHI

Notice of Privacy Practices

And...

- May ask if there have been non-routine uses and disclosures of PHI
- May file a complaint with any HHCS facility or the U.S. Department of Health and Human Services if they believe their PHI was mishandled or privacy rights violated



Authorizing Disclosure of PHI

A patient must authorize disclosure of PHI. If the patient is less than 18 years of age, his or her parent or guardian must give authorization. Some minors can provide their own consent; these minors may be married, have children, or be pregnant teenagers.

Other Disclosures of PHI

There are circumstances where PHI may be disclosed without the authorization of the patient. Examples of these disclosures include:

- When required by law
- For public health activities to control disease, injury, or disability
- For disaster relief
- For incidental disclosures as a by-product of lawful and permitted disclosures

Other Disclosures of PHI (continued)

- In cases of abuse or neglect
- For coroners, funeral directors, and organ donation
- For legal proceedings
- For workers' compensation
- In cases of communicable diseases, such as HIV or hepatitis

Case Study Questions

Question 1:

Mrs. Smart is a patient at HMC. She is able to make decisions about her own care. Jessica, her cousin and closest relative, lives 50 miles away has learned that Mrs. Smart is in the hospital. Jessica is requesting detailed information regarding Mrs. Smart’s care and has expressed the desire to make care decisions for her cousin. Which response is appropriate?

a) Do not allow Jessica to see her cousin.

b) Inform Jessica about Mrs. Smart’s care and allow her to make all health care decisions.

c) Inform her about HIPAA. She can visit Mrs. Smart and discuss her care.

Case Study Questions

Question 2:

According to HIPAA, Mrs. Smart is entitled to which of the following?

a) privacy and confidentiality

b) opportunity to make decisions regarding her care

c) the right to act in any manner she desires

d) file a complaint if she feels her PHI was mishandled

Case Study Answers

Survey Question Answers

Question 1: c

Question 2: a, b, d

Protected Health Information (PHI)

In order to maintain the confidentiality of client information, the HIPAA rule addresses PHI. PHI is information that can identify a patient. This information includes:

- Patient's Clinical Information
- Information that can reasonably be used to identify the patient
- Information related to past, present, and future physical or mental condition
- Information related to any health service or health treatment
- Genetic information
- The information can be in any form – paper, oral, written, faxed, or in a database

Protected Health Information (PHI)

Includes:

- Name
- Date of birth
- Address, phone number, fax number, and e-mail address
- Names of relatives
- Photographs
- Medical record numbers or health information, such as history and laboratory or radiology results

Permitted Uses of PHI

- Treatment (to treat a Patient)
- Payment (so the Facility can bill and collect for treatment of a patient)
- Health Care Operations (quality improvement, infection control, credentialing, peer review, case management, clinical training, customer service and some fundraising)
- If you want to use PHI for any other reason, you may need to get the patient's prior written authorization

Treatment

- – Treatment is providing, coordinating, or managing a patient's health care
- – Treatment includes consultations between health care providers about a specific patient
- – Treatment includes the referral of a patient from one physician or facility to another
- – Using PHI for Treatment purposes is permitted under the Privacy Rule WITHOUT the patient's authorization

Incidental Disclosures

- – The Privacy Rule is not intended to prohibit providers from talking to each other or to their Patients in a treatment setting
- – Should use reasonable safeguards to limit incidental disclosures
- – A disclosure may not be considered incidental if it was preventable

Disclosures of PHI

Upon admission to the hospital patients are given the opportunity to agree or object to the following uses/disclosures of their PHI

- Listing in the inpatient directory. Patients are asked if they will allow a listing of their name, room, general condition and religious affiliation in the inpatient directory. If the patient objects to this disclosure, any person calling about the patient will be told that there is no record of that patient.
- Notification of family members and persons assisting in the patient's care.
- Disaster relief purposes.

Case Study Question

Patient PHI includes all of the following EXCEPT:

a) Medical information and patient’s medical record number.

b) Patient’s date of birth.

c) Social Security number.

d) Patient’s address.

e) Patient’s hair color.

Case Study Answer

Survey Question Answer: e

Business Associates

- Business Associates are also covered by HIPAA.
- Business Associates are persons and companies which provide a service to HHCS and, in doing so, have access to patient PHI.
- Example of Business Associates include consultants, billing and collection companies, vendors, accountants, and lawyers.
- Business Associates are required by HIPAA to sign a written Business Associate Agreement which contains certain protections for PHI.
- If you are not sure whether a person or company is a Business Associate or whether a Business Associate agreement is required, contact the Privacy Officer.

Telephone Security

Telephone Security

- Clinicians frequently use telephones to communicate with each other about patient care, whether they are on the patient floor or elsewhere.
  - Telephone communication is a useful tool to facilitate patient care, but it opens up the possibility for patients or visitors to overhear PHI.
- Use the tips on the next slide to help you abide by HIPAA guidelines.

Telephone Security Steps

- Do not place the caller on speaker phone without letting that person know you are placing them on speaker and confirming the speaker’s agreement that the call be place on speaker phone.
- Keep your volume level where you can hear adequately, but do not disturb others.
- Do not leave confidential information as a voicemail message.
- Do not initiate a confidential conversation before asking the speaker if he or she is in a private area to converse. Do not discuss PHI about a patient over the telephone in the presence of another patient or another person who is not authorized to receive that PHI.

Who Needs to Know?

The "Need To Know" Rule

When sharing PHI remember to disclose information only to associates that are involved in the direct care of the patient.

- Confidentiality is essential because many different people may have access to client records. Examples of Associates with access to inpatient records include:
  - Those who work in Administration
  - Dietitians
  - Those who are directly involved in the client's care
  - Those who work in Medical Records, Infection Control, Quality Management, or Social Services
  - Client educators
  - Pharmacists
  - Risk manager and planners
  - Physicians

The "Need To Know" Rule

Access is on a need-to-know basis.

Computer systems that contain PHI have automatic logging of every patient record access. Routine audits of patient record access are conducted to assure that our patients' right to privacy are protected, and that YOU are following the Need To Know rule.

Confidentiality

To safeguard client confidentiality, these health care workers must be aware of:

- Where PHI can be discussed
- Limitations on access to and discussion of PHI (including disclosure to family)
- Safeguards for electronic records and the transmission of electronic records

Locations for Discussions of Patient Care Information

Health care staff will discuss patient care information, share information, and the treatment plans of patients. Every effort should be made to protect the privacy of the patient by minimizing the risk that others will overhear the conversation.

***The discussion of PHI should never be done in public areas such as the cafeteria or elevators.

Discussions of PHI can take place in any of the following locations:

- At the nursing station
- With a patient in a treatment area, such as the emergency department
- In an outpatient setting, such as the laboratory or radiology
- Offices with doors closed
- Anywhere you are out of earshot of those who have no need to know

Limitations on Access to and Discussion of PHI

There are certain limitations on access to and discussion of PHI:

- The health care worker should never access PHI for any patient who is NOT under his or her care at a HHCS facility.
- If your friend is in the facility, you are not to discuss the friend's care with the provider.

These rules apply to your family members, friends, and neighbors. You are not permitted to access these patients' records just because you know or care for them outside of an HHCS facility.

Disclosing PHI to Family Members by Phone

Before disclosing PHI to a patient’s family member by phone, you must obtain the patient’s permission to release the information. Additionally, the identity of the individual on the phone must be verified.

Privacy Review: Common Mistakes

Review

- Avoid discussing patient’s medical information with friends, family or in public places.
- Avoid leaving clipboards with medical information and medical records in places where they could be looked at, altered or stolen.
- Be careful to fax information to the proper address.
- Avoid leaving information on fax machines and printers. Make sure you get the original and any copies.
- Avoid leaving computers on with information that can be seen or accessed by unauthorized people.
- Follow HHCS's policies for retaining and discarding PHI.
- Do not recycle PHI (i.e. discard physical PHI in Shred Bins).

Case Study Questions

Staff members are discussing Mrs. Smart’s plan of care. Which locations are not acceptable?

a) Cafeteria

b) Nursing station

c) Elevator

d) With a patient in a treatment area

e) An empty hallway in hushed voices

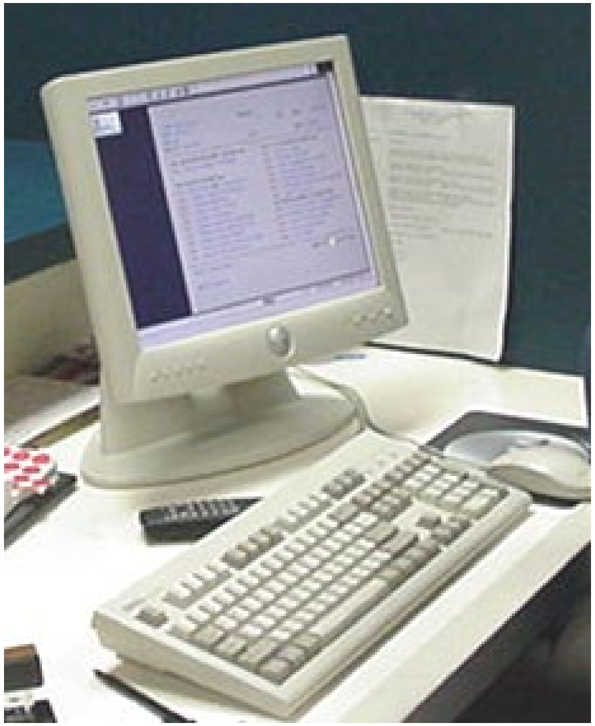
Case Study Answers

- Survey Question Answers: a, c

Security Rule

Security Rule

- The Security Rule covers PHI that is stored in an electronic form.
- PHI stored in electronic form is called ePHI.



Security Rule Requirements

- **Ensure everyone accessing PHI has an individual password - no generic passwords.**
  - PHI is available only to those that need to know. Track associate access of PHI.
- **Audit computer user's access to patient electronic records.**
  - To ensure workforce compliance with the Security Rule HHCS conducts Scheduled Audits, Random Audits, Suspected Security Incident Audits
- **Provide a secured network.**
  - Ensure that PHI is held in private from non-authorized associates as well as outside parties.
- **Assure the availability of all ePHI.**
  - Ensure that patient PHI is available when needed.
    - – Help Desk: Extension 6140
    - – 24 / 7 / 365

Security Rule Requirements Continued

- – Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI
- – Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the Privacy Rule
- – Ensure compliance with the Security Rule by the workforce

Hospital ePHI Security Policies

Password Policy

- Disclosure of your password is prohibited
- Do not share your password
- Posting passwords on computers is prohibited
- The Security Rule requires that all access to ePHI be audited
- Generic User access to ePHI is not allowed
- Password use is audited

Hospital ePHI Security Policies

Access Control Policies

- HHCS has implemented auditing, logging and monitoring tools.
- Examination of system activity will be routinely conducted.
- Scheduled Audit
- Random Audit
- Suspected Security Incident Audit

Your access to PHI and ePHI will be audited

Can you view your own Medical Records or Test Results?

- No, do not access your own medical records on the computer.
- Yes, you are allowed to view your records in the Medical Records Department after your access has been properly recorded. You can also receive the test results from your physician.

What does Auditing Mean?

Electronic patient records access will be audited at times:

- Various system access log files will be inspected.
- Each user that accessed the patient's electronic record will be examined to see if the access was appropriate and for job related reasons.

Your access to PHI and ePHI will be audited

Do you have a friend, relative or co-worker in the hospital?

- – Do not access their patient records on the computer.
- – If you were told by your co-worker or friend that they were going to be in the hospital, visit them in their room. They will enjoy the visit, and they will tell you what they want you to know.

Hospital Fax Policy

Faxes are vulnerable to unauthorized access

- Verify fax number
- Confirm receipt by authorized person
- Use cover page with preprinted disclaimer
- *Follow the Minimum Necessary Rule*

Email Policy

- Associates of HHCS should not transmit ePHI by email, either internally or externally.
- Email transmissions are vulnerable to interception or receipt by unauthorized persons.
- There is currently no universally accessible and accepted secure email technology in the healthcare industry.
- Emails are audited for inappropriate ePHI disclosures.
- Internet and Electronic Mail (Email) policy outlines appropriate use of the HHCS email system.
- All laptops must have McAfee encryption software installed by Information Services. A password will be required to access the laptop. Call the helpdesk for assistance.
- All outgoing emails are scanned for sensitive content and automatically encrypted if the search criteria are met. Users may manually encrypt an email by putting the word [encrypt] in the subject line. The word [encrypt] **MUST** be enclosed in square brackets [ ]. **Do not use** parentheses ( ) or braces { }.

Email Policy

- You **CAN** send **NON-IDENTIFYING** information about a patient in emails. The patient number is allowed.

Do not send any patient's name in an email.

Example of INAPPROPRIATE email containing ePHI:

- Patient Jane Doe in OB room 3 will have a C-Section.

Example of ALLOWABLE non-identifying email:

- Patient 7234321 in OB room 3 will have a C-Section.

Security Incidents

A Security Incident is defined as unauthorized access, use, disclosure, modification or destruction of ePHI.

- Interference with the Health Information System.
- Improper network activity.
- Misuse of outside data.

Security Incident Examples

- Service Disruption – Natural Disaster
- Virus or Worm
- Theft of ePHI
- Hacking
- Unauthorized use of system for processing, transmitting or storage of data
- Business Associate Security Incident

Security Review: Common Mistakes

Security Review: Common Mistakes

- Using or disclosing ePHI without prior, written patient authorization for a purpose other than Treatment, Payment or Operations (TPO)
- Not securing ePHI by:
  - Logging off or securing computer screens when not in use or unattended.
  - Keeping files closed when not being used.
- Conducting inappropriate and unintentional actions and disclosures of PHI through e-mail, internet and facsimile such as sending a fax without verifying the fax number
- Posting passwords on the computer
- Sharing passwords with others
- Failing to follow the Need to Know Rule
- Failing to follow the Minimum Necessary Rule

Special Precautions

- Don't disclose password
- Verify recipient of faxes
- Don't view ePHI in public areas
- Don't send ePHI via Internet unless encrypted
- Don't view ePHI inappropriate to your job
- Don't email ePHI to anyone internal or external to HHCS

Case Study Question

When you are reviewing a patient's PHI on the computer, which of the following actions will NOT promote confidentiality?

a) Leaving the computer screen open while you answer a call light

b) Keeping the computer in a secure location

c) Keeping your password confidential

d) Not accessing the information if you are not directly involved in his care

Case Study Answer

Survey Question Answers: a

Enforcement and Consequences

Government Enforcement

Consequences of Violation by Workforce

- Compromise patient care because patients keep information from their caregivers (such as medical history, condition and symptoms).
- Could be the basis for disciplinary action, ranging from counseling to a warning to termination.
- Could subject an individual to civil and criminal penalties, including fines and imprisonment.
- Is inconsistent with HHCS's mission.

Penalties

- Against health care workers and against the Facility
- Civil fines
- Criminal penalties
- Professional licensure could be affected

Example

- An Emergency Department physician in Rhode Island was fired from a hospital and penalized by the state medical board for posting comments on Facebook about a patient. Despite not revealing the name of the patient, the physician disclosed other details that were sufficient to cause community members to know who the patient was.

  (www.boston.com 04/20/2011)
- Hospitals and Health Care Agencies across the country continue to terminate employees for similar disclosures of protected health information through social media.

Example

- An employee of a Texas based health care system was sentenced to 10 years in federal prison for the theft of protected health information, including names, social security numbers, dates of birth, etc., over a 4 year period and the subsequently selling of that information to two other individuals.

  (www.ktre.com – 07/23/2012)

Example

- Six employees were terminated from an L.A. health care provider after it was confirmed that they inappropriately accessed the medical records of North West, child of Kim Kardashian and Kanye West. Five of the employees used the logins of physicians to access the information and the sixth had access for billing purposes.

  (www.emrandhipaa.com – 01/16/14)

Review: How can I protect PHI?

Limit physical access to PHI

- Do not leave files open and unattended.
- Lock cabinets and drawers.
- Turn computer screens so that unauthorized persons cannot view the screen.
- Prevent disclosures from copies/originals in the copy machine or unattended facsimile printouts.
- Dispose of confidential information in the proper container (Shred-it bins).

Limit oral communication of PHI

- Discuss PHI so that it cannot be overheard.
- Discuss PHI only with individuals involved with the patient's treatment.
- Disclose only the minimum amount of information necessary.

Limit electronic communication of PHI

- Log off computers when not in use
- Keep your password private
- Do not view ePHI in public places
- Do not email ePHI to anyone
- Be careful with laptops and mobile devices which contain PHI. Do not leave them unattended in cars or in public places.

Do not send any patient's name in an email.

Limit oral communication of PHI

If you overhear or come across PHI that does not concern you…

Please,

KEEP IT TO YOURSELF

And

Report possible Privacy Policy violations to your Supervisor, Privacy Officer or Corporate Compliance Officer

Limit oral communication of PHI

HIPAA Privacy and Security Policies and Procedures are available on the HHCS Intranet.

Contact one of the following when answers are not available in our Policies and Procedures.

- Your supervisor
- HIPAA Privacy Officer x 6625 (Tera Lusk)
- HIPAA Security Officer x 6121 (John Forrester)
- Corporate Compliance Officer x 6622 (Janet Morton)
- Compliance and Privacy Hotline: 706-278-1910

Confidentiality and Non-Disclosure Statement

The following pages contain HHCS's Confidentiality and Non-Disclosure Statement.

Read the Statement carefully. You will be asked to acknowledge that you have reviewed this CBL. Answering the question regarding the Statement will stand as your electronic signature.

Confidentiality and Non-Disclosure Statement

- As an associate, volunteer or other member of the workforce of HHCS, I acknowledge that I have completed training on the privacy and security policies and the privacy and security regulations issued under the Health Insurance Portability and Accountability Act of 1996 (also known as HIPAA).
- I understand that all patient information, including billing and financial data, is confidential and should not be removed from Hamilton.
- I agree to keep patient information confidential.
- I agree to comply with all Privacy and Security Policies and Procedures including those implementing the HIPAA.
- I understand that if I violate patient confidentiality by using or disclosing patient information improperly, I may be subject to disciplinary action up to and including termination of my employment.
- I understand that if I have any questions or concerns about the Privacy Rules, Security Rules and/or the proper use or disclosure of patient information, I should ask my Supervisor, the Privacy Officer, the Security Officer or the Corporate Compliance Officer.
- I understand and agree that the Privacy and Security Policies and Procedures will apply to any patient information I have access to even after I terminate my employment or other relationship with the HHCS.

Please Remember...

Maintaining patient confidentiality means keeping information about a patient’s health care private. Only people who need to know information should receive it and only to the extent needed to perform duties for the patient. Maintaining patient confidentiality requires that any information about a patient cannot be repeated to anyone who is not directly involved with the care of that patient.

Bibliography

- Badzek, L., & Gross, L. (June 1999). Confidentiality and privacy: At the forefront for nurses. *Nursing World, American Journal of Nursing*. Retrieved November 15, 2005, from http://www.nursingworld.org/ajn/1999/june/issu069c.htm
- Buppert, C. (2002). Safeguarding patient privacy. *Nursing Management*, *33*(12), 31–35.
- Centers for Medicare and Medicaid Services. (2005). *HIPAA administrative simplification glossary*. Retrieved November 15, 2005, from http://www.cms.hhs.gov/glossary/default.asp?Letter=ALL&Audience=7
- McLeod Health. (2005). *Patient bill of rights.* Retrieved November 15, 2005, from http://www.mcleodhealth.org/Home/PatientBillofRights.cfm

Bibliography

- Providence Health System. (1997–2005). *Confidentiality of patient information*. Retrieved November 15, 2005, from http://www.providence.org/everett/Patient_Resources/HIPAA.htm
- The Joint Commission. (2010). *2010 hospital accreditation standards*. Oakbrook Terrace, IL: Author.
- The patient care partnership: Understanding expectations, rights and responsibilities. (2003). Chicago: American Hospital Association.