Domain IV: Legal Aspects

RHIT Exam Review Prep

Disclaimer

Please note that these presentations are designed to serve as a valuable supplement to your overall study plan to prepare for the RHIT certification examination.

Participation in these presentations does not guarantee a passing score on RHIT the examination. For more information on the testing dates and the RHIT credential go to www.ahima.org.

It is suggested that you follow the AHIMA Candidate Guide, Appendix H as a study guide for preparing for your certification exam.

Legal Aspects - 11% Knowledge Clusters

- 1. Ensure confidentiality of the health records (paper and electronic)
- 2. Adhere to disclosure standards and regulations (HIPAA privacy, HITECH Act, breach notifications, etc.) at both state and federal levels
- 3. Demonstrate and promote legal and ethical standards of practice
- 4. Maintain integrity of legal health record according to organizational bylaws, rules and regulations
- 5. Follow state mandated and/or organizational record retention and destruction policies
- 6. Serve as the custodian of the health records (paper or electronic)
- 7. Respond to Release of Information (ROI) requests from internal and external requestors
- 8. Work with risk management department to provide requested documentation
- 9. Identify potential health record related risk management issues through auditing
- 10. Respond to and process patient amendment requests to the health record
- 11. Facilitate basic education regarding the use of consents, healthcare Power of Attorney, Advanced Directives, DNRs, etc.
- 12. Represent the facility in court related matters as it applies to the health record (subpoenas, depositions, court orders, warrants)

Legal Aspect Review

- "For HIM professional, dealing with the legal aspects of health records and health information presents 3 primary concerns:
  - **Compilation** and **maintenance** of health records
  - **Ownership** and **control** of health records, including use and disclosure
  - **Use** of health records and health information in judicial proceedings." (Johns, 2012)

Chapter 9 Green Textbook

Legal Aspects textbook

Basic Terms and Concepts to Master

- ONC – Office of National Coordinator for HIT
- Privacy Rule – 2 key goals
  - To provide individuals with more rights to their health information
  - To provide greater privacy protection for one's health information (limit access)
- PHI – Protective Health Information is defined as individual's identifiable health information

Basic Terms and Concepts to Master

- Covered entity (CE) – healthcare providers, health plans, healthcare clearinghouses, etc.
- Business Associate (BA) person or organization, other than an employee of the CE, that performs activities on behalf of the CE that involves disclosure of PHI. Examples: consultants, transcription companies, accounting firms and law firms
- Designate Record Set – see previous slides

Basic Terms and Concepts to Master

- Minimum Necessary – applies to limiting access to PHI based on job responsibilities
- TPO or Treatment, Payment and Operations – no patient consent is required to release PHI in the provision of meeting TPO
- De-identified Information – PHI that does not identify an individual, all identifying information has been deleted or eliminated

Confidentiality & Release of Information

Ensure confidentiality of the health records (paper and electronic)

PHI Disclosure

- Authorization is required
  - Attorney request
  - Employer request
  - Workers Compensation request
  - Government agencies requests
  - IRS requests
  - Law enforcement (except where required by HIPAA)
  - Marketing communication such as news agency
  - Research that requires patient specific information
    - Follow the (IRB) Institutional Review Board approval
  - Third party payers except TPO
  - Health care providers
    - Those who have not rendered care to the patient
  - HIV related information
  - Mental health related information
  - Substance abuse related information

PHI Disclosure

- Authorization is NOT required
  - Medicare
  - Medicaid
  - Military and VA activities
  - Armed forces personnel
  - National security and intelligence activities
  - Protective services for the president and others
  - Medical suitability determinations
  - Correctional institutions for the provision of health care

De-identified of PHI

- De-identified PHI can be released without consent
- Identifiers that MUST be removed
  - Name
  - Addresses and other geographic identifiers
  - Relatives
  - Employers or household members
  - Zip codes
  - Add dates (except years) related to the individual
  - Numbers
    - Phone number
    - Fax number
    - SSN
    - Medical Record
    - Beneficiary numbers
    - Account numbers
    - Certificate/license numbers
    - VIN numbers
    - License plate numbers
    - Device identifiers and serial numbers
    - URLs
    - IP address
    - Biometric identifiers
    - Photographic images and any other unique identifying numbers, characteristics, or code

Patient Access

- Individuals have the right to inspect and obtain a copy, except
  - Psychotherapy notes
  - Information compiled for use in a civil, criminal or administrative action (i.e. Incident report)
  - PHI maintained by a CE that is subject to CLIA (Clinical laboratory Improvement Amendments)

ROI (pg. 288-300 Green)

- When information can be released
  - Patient authorization
  - Subpoena
  - Court order

ROI

- **HIPAA Privacy Rule** requires covered entities to track the release of PHI so patients can obtain an accounting of disclosure for the 6 years prior to the date of their request, retroactive to 4/16/2003
- **Accounting exception**
  - Releases related to TPO
  - To myself
  - Entered in the facility's directory
  - Patient's care providers
  - National security or intelligence purposes
  - Correctional institutions or law enforcement
  - Occurs prior to the compliance date
- **Track and report**
  - Date of disclosure
  - Name and address of the entity or person who received the PHI
  - Description of the PHI disclosed
  - Statement of reason for disclosure (or a copy of the written request for disclosure)

Release standard

- Must provide the patient with 1 free accounting of any select 12 month period
- Subsequent accounting may be reasonably charged
- Individual makes their request
  - CE has 60 days to comply with the request
  - CE has 1 – 30 day extension permitted after notifying the patient of the delay, the reason and the date the account will be available in writing

Maintain integrity of legal health record according to organizational bylaws, rules and regulations

Organizational Bylaws

- Medical staff create and vote on bylaws
- ***Bylaws*** are rules that delineate the responsibilities of the medical staff members
- ***Rules and regulations*** are procedures based upon federal, state and accreditation agency standards that clarify the bylaws

(Green 2012)

Legal Health Record

- A legal health record (LHR) is the documentation of patient health information that is created by a health care organization.
- The LHR is used within the organization as a business record and made available upon request from patients or legal services.
- There is no specific set of regulations for legal health records; however, ***they must meet standards set by federal and state laws***. After meeting these basic standards, it is up to the discretion of the individual healthcare organization to decide what is and is not appropriate to reveal.
- Historically, the legal health record was simply the contents of a paper chart but because more healthcare facilities are adopting electronic health records (EHR), using health apps for patient monitoring and tracking data on various forms of electronic media, defining and creating a legal health record is becoming increasingly complex.

Integrity of the health record

- Documentation integrity involves the accuracy of the complete health record. It encompasses information governance, patient identification, authorship validation, amendments and record corrections as well as auditing the record for documentation validity when submitting reimbursement claims.

- EHRs have customizable documentation applications that allow the use of templates and smart phrases to assist with documentation. Unless these tools are used appropriately, however, the integrity of the data may be questioned and the information deemed inaccurate—or possibly even perceived as fraudulent activity.

- Established policies and procedures such as audit functions must be in place to ensure compliant billing.

Integrity of the health record

- Without safeguards in place, records could reflect an inaccurate picture of the patient's condition, either at admission or as it changes over time.
- The provider must understand the necessity of reviewing and editing all defaulted data to ensure that only patient-specific data for that visit is recorded, while all other irrelevant data pulled in by the default template is removed.
- For example, the automatic generation of common negative findings within a review of systems for each body area or organ system may result in a higher level of service delivered, unless the provider documents any pertinent positive results and deletes the incorrect auto-generated entries.

- **Integrity of the Healthcare Record: Best Practices for EHR Documentation**
  http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050286.hcsp?dDocName=bok1_050286

Risk Management

- Work with risk management department to provide requested documentation
- Identify potential health record related risk management issues through auditing

Risk Management

- Risk manager is responsible for gathering information and managing general liability, incidents, liability claims and lawsuits.
- Responsible to manage and minimize risk exposure
- Any request from a legal source should be routed through risk management

Auditing as a Risk Management Tool

- Utilize abstracting and auditing as a risk management tool
  - Errors
  - Abnormal findings not addressed
  - Policy and procedure failures
  - Incomplete patient records

Respond to and process patient amendment requests to the health record

Amending the Patient Record

- Pg. 84-86 Green
- **Correcting** an error is an ***Amendment***
- Paper Record
  - Draw a single line through the incorrect information, making sure the original entry remains legible
  - Date, specify time, and sign the correct entry
  - Document a reason for the error in a location near the original entry "entry made in error" or "entry made in wrong chart"
  - Enter the correct information and sign by the note originator

Amending the Patient Record - continued

- Pg. 84-86 Green
- Correcting an error is an ***Amendment***
- Electronic Record
  - Each system will have it's mechanism to correct an error in the EHRs and should include
    - Store the original note and any changes posted
    - Date and time and the user making the edits
    - Reason for the change

HIPAA

- 2003, HIPAA Privacy Rule granted the patient the right to request correction made by the CE
- The CE may deny the patient's request if
  - Entry was not created by the CE
  - Is not part of the designated record
  - The information is accurate and complete

Addendum to the patient record

- From time to time, information has to be **added** to the patient's records that will **clarify** the patient's condition is an **Addendum**

Facilitate basic education regarding the use of consents, healthcare Power of Attorney, Advanced Directives, DNRs, etc.

(Greens, 2009)

Consents

- Required by federal, state and accrediting agencies that patient consents to treatment and that it's recorded in the patient's record
  - Informed consent
    - Process of advising the patient about treatment/surgical procedures, the benefits, the risks involved and available options
    - Evidence that the patient or the patient's legal surrogate understands and acknowledges the informed consent
      - Admission consent
      - Consent to treat
      - Surgical consent

Advanced Directives (AD) (pg. 130 Green)

- PSDA – Patient Self Determination Act of 1990 requires that all healthcare facilities and provider notify the patients 18 years and older that they have a right to an Advanced Directive

- AD is a legal document where the patient provides instructions as to how they want to be medically treated in the event they become so ill that there is no reasonable hope that they will recover and they are unable to make their own decisions

DNR

- Do Not Resuscitate (pg. 131 Green)
  - An order documented in the patient's medical record by the physician, which instructs medical and nursing staff to not try to revive the patient if breathing or heartbeat stops
  - Pre-determined decision when an AD is in effect.
  - No emergency efforts are made

Terms

- Health care proxy aka Durable Power of Attorney (pg. 133, Green)
  - Legal document in which the patient chooses another person to make treatment decisions in the event the patient becomes incapable of making these decisions

- Living Will Declaration (pg. 132, Green)
  - Legal document that outlines that directs the health care providers in the kind of health care services that patient wants under certain circumstances.

HIM Role

- Serve as the custodian of the health records (paper or electronic)
- Represent the facility in court related matters as it applies to the health record (subpoenas, depositions, court orders, warrants)

Records custodian

- HIM Manager, director or designated
  - Responsible to represent the organization in court related to the patient record maintenance
  - Testify that the patient record has been maintained in the normal course of business
    - Means following the medical staff bylaws, rules, regulations, policies and procedures based on federal, state and accrediting agencies

Follow state mandated and/or organizational record retention and destruction policies

Compilation & Maintenance

- State and federal rules and regulations developed b administrative agencies
  - State licensing agency, vital statistic reporting: Birth, death, etc.
  - Federal agency such as Medicare and CDC
- Accrediting bodies standards
  - Such as JCAHO, AOA
- Professional Organizations
  - Best practice such as AHIMA, AMA

Ownership & Control

- Use = how PHI is used internally
- Disclosure = how PHI is disseminated externally
- Patient records are the property of the provider = ownership and physical
- Patient has legal right to access documents
- Laws Involving Use & Disclosure
  - HIPAA Privacy Rule set's the minimum rights for patient
  - State laws on confidentiality and privacy
  - In most situation must have patient authorization
  - Other situations do not require ROI
    - Reporting vital statistics, communicable disease, violent crime victims and etc.

Judicial Proceedings

- Patient records are usually admissible in ***litigation*** (or judicial proceedings)
- ***Court order*** (issued by the judge) or a ***subpoena duces tecum*** (issued by other source) are used to obtain records for legal action in courts with jurisdiction
  - Subpoena duces tecum usually requires a patient's authorization
- The patient can also sign ROI
- Requirements vary from state to state

Types of records related to the Legal Health Record

- Legal health record – official business record
- Designated record set – includes billing records and not included in the LHR
- Electronic Health Records – contains metadata that are not ordinarily considered part of the LHR
- Personal Health Records – owned and maintained by patient; not part of the LHR

Comparison between designated record set and the legal health record

	Designated Record Set (DRS)	Legal Health Record (LHR)
Definition	A group of records maintained by or for a covered entity that is the medical and billing records about individuals; enrollment, payment, claims adjudications, and case or medical management record systems maintained by or for a health plan; information used in whole or in part by or for the HIPAA covered entity to make decisions about individuals	The business record generated at or for a healthcare organization. It is the record that would be released upon receipt of a request. The legal heath record is the officially declared record of healthcare services provided to an individual patient by a healthcare provider.
Purpose	Used to clarify the access and amendment standards in HIP AA Privacy Rule, which provide that individuals generally have the right to inspect and obtain a copy of PHI in the DRS	The official business record of healthcare services delivered by the entity for regulatory and disclosure purposes.

Comparison between designated record set and the legal health record (Johns, 2012)

	Designated Record Set (DRS)	Legal Health Record (LHR)
Content	Defined in organizational policy and required by the HIPAA Privacy Rule. The content of the DRS includes medical and billing records of covered providers; enrollment, payment, claims, and case information of a health plan; and information used in whole or in part by or for the covered entity to make decisions about individuals.	Defined in organizational policy and can included individually identifiable data in any medium collected and directly used in documenting healthcare services or health status. It excludes administrative, derived and aggregate data.
Uses	Supports individual HIPAA rights of access and amendment.	Provides a record of health status as well as documentation of care for reimbursement, quality management, research, and public health purposes; facilitates business decision-making and education of healthcare practitioners as well as the legal need of the healthcare organization.

Retention

- May vary from state to state
- AHIMA's Recommended Retention Standards

Health Information	Retention Period
Diagnostic images	5 years
Disease index	10 years
Fetal Heart monitor records	10 yrs.-age of majority
MPI	Permanently
Operative index	10 years
Adult patient records	10 yrs. after most recent encounter
Child patient record	Age of majority plus state's statute of limitation
Physician index	10 years
Registers of birth, death and surgical procedures	Permanently

Adhere to disclosure standards and regulations (HIPAA privacy, HITECH Act, breach notifications, etc.) at both state and federal levels

HIPAA Privacy Rule

- Key law covering the confidentiality of protected health information (PHI)
- HIPAA has 5 sections
  - Title I Health Care Access, Portability, and Renewability
  - ***Title II Preventing Health Care Fraud & Abuse***
    - ***Healthcare abuse, fraud***
    - ***Medical liability reform***
    - ***Administrative simplification contains the HIPAA security standards, NPI, transaction and code set standardization***
  - Title III Tax Related Health Provision
  - Title IV Group Health Plan Requirements
  - Title V Revenue Offsets

ARRA – *American Recovery & Reinvestment Act 2009*

- 2009 multilevel law which includes stimulus funding for health information technology and important HIPAA Privacy Rule which are located in the HITECH (Health Information Technology for Economic and Clinical Health Action) portion of ARRA

Individual Rights under HIPAA

- Right of Access
- Right to Request Amendment of PHI
- Right to Request Accounting of Disclosure
- Right to Request Restrictions of PHI
- Right to Request Confidential Communication
- Right to Complain of Privacy Rule Violation

Breach Notification

- ARRA requires all CE and BA be subject to FTC (Federal Trade Commission) regulations
  - Defined by ARRA as "unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information"
  - And must meet the "risk of harm" threshold

Go back to your textbooks and review the time lines for notification

HIPAA Privacy Rule Administrative Requirements

- Important to HIT
  - Designation of a privacy officer and contact person to receive complaints
  - Requirements for privacy training
  - Requirements for establishing privacy safeguards for handling complaints
  - Privacy safeguards
    - Includes administrative, technical and physical safety
  - Standards for related policies and procedures
  - Enforcement of federal privacy legislation and rules
    - Civil and criminal penalties

Fair and Accurate Credit Transaction Act (FACTA)

- Under FACTA, financial institutions and creditors are required to develop and implement written identity theft programs that identify, detect and respond to **"red flags"** that may indicate the possibility of identity theft.
- Many healthcare organizations meet the criteria as a "creditor" and therefore must meet the **"Red Flag Rules"**
  - Limit access
  - Require user ID
  - Implement encryption
  - Install protective hardware and software (firewall)
  - Eliminate open network jacks in unsecure areas
  - Routinely audit access to PHI through audit trails

Other areas to review

- Medical Staff Appointment and Privileging
- Labor laws
- ADA

Demonstrate and promote legal and ethical standards of practice

HIM Role

- HIM professional is responsible for maintaining and promoting legal and ethical standards as related to PHI
  - State and Federal laws
    - HIPAA
  - Regulations
    - Medicare
  - Standards
    - JCAHO
  - Codes of Ethics
    - AHIMA

Should or shouldn’t?

- The local police enters the HIM Department and request a copy of a recently discharged patient. The patient was involved in an auto accident and had left had left the sconce. The identification of the officers appears to be in order, do you release the information? Why or Why not?

Answer

- No
- HIPAA makes it illegal to allow law enforcement agency representatives to access PHI unless they produce a signed patient authorization to release information or a court document (e.g., court order or subpoena duces tecum.)

Should or shouldn't?

- You are the ROI clerk and received a authorization signed by the patient to release PHI to Rasmussen Insurance Company. The authorization was signed and dated by the patient more than a year ago. According to your records, the patient was admitted and discharge less than 6 months ago. Do you release the information? Why or Why not?

Answer

- **No** - The patient's signature on the ROI authorization was obtained prior to the patient discharge from the facility. Therefore you cannot release the information requested to the insurance company without an updated authorization.

- **More:** *The signature on the release of information authorization must be dated after treatment has concluded (e.g., after date of discharge from inpatient discharge). The patient doesn't know what will occur during treatment, and he may not want some aspect of his records released (e.g., HIV positive lab results). In this particular case, you would instruct the insurance the insurance company to obtain an updated, signed authorization to release medical record information from the patient (dated after discharge from the hospital).*

Should or shouldn’t?

- You receive a telephone call from a hospital emergency department (ED) located in another state. The ED physician states that this is an emergency situate, and he needs to obtain pertinent medical information about a patient currently under treatment. Do you release the information? Why or why not?

Answer

- **Yes -** Verify that this is an emergency situation by using the call-back method. Once the situation is verified, release the information via telephone (or fax) and request that the ED physician arrange for a signed authorization to release information be submitted once the patient's condition has stabilized.

- **More**: *Ideally, we would require a signed authorization to release information prior to releasing any patient information. Emergency situations, however are special cases and we routinely use the call-back method to comply with urgent requests for information because the patient's care could be compromised otherwise. The telephone call-back method verifies the authenticity of a health care facility/professional (e.g. ED physician) requesting medical information about a patient in an emergency situation (e.g., history of medication on a patient who is comatose). To implement the call-back method, you look up the switchboard number of the health care facility in the phone book (or by calling Information), call the switchboard, ask to be a connected to the appropriate department (e.g., ED), and then ask to speak with the health care professional responsible for the patient. This ensures that you are appropriately releasing information via telephone. You then follow up by requiring the facility to submit a release of information authorization signed by the patient or next of kin for documentation for your file.*

Sample Question & Answers

Question

- What federal legislation enacted the Medicare and Medicaid programs?

a. Public Law 92-603 1972
b. Public Law 89-97 1965
c. Public Law 98-21 1983
d. Utilization Review Act 1977

Answer

- What federal legislation enacted the Medicare and Medicaid programs?

a. Public Law 92-603 1972
b. **Public Law 89-97 1965**
c. Public Law 98-21 1983
d. Utilization Review Act 1977

Why

In 1965, healthcare saw several amendments to the Social Security Act that brought Medicare and Medicaid into existence.

Question

- Changes to health record entries are

a. Acceptable in certain circumstances
b. Indicative of negligent care
c. Permissible only in paper health records
d. Permissible only in electronic health records

Answer

- Changes to health record entries are

a. **Acceptable in certain circumstances**
b. Indicative of negligent care
c. Permissible only in paper health records
d. Permissible only in electronic health records

Why?

The basic principles of health record documentation apply to both paper and electronic patient records. Changes to the health record are acceptable as long as they are done in accordance to documentation guidelines, standards and regulations.

Question

- What is the term used most often to describe the individual within an organization who is responsible for protecting health information in conjunction with the court system?

a. Administrator of record
b. Custodian of record
c. Director of record
d. Supervisor of record

Answer

- What is the term used most often to describe the individual within an organization who is responsible for protecting health information in conjunction with the court system?

a. Administrator of record
b. Custodian of record
c. Director of record
d. Supervisor of record

Why?

- Associated with ownership of health records is the legal concept of the custodian of records. The custodian of health records is the individual who has been designated as having responsibility for the care, custody, control and proper safekeeping and disclosure of heath records.

Question

- An individual who brings a lawsuit is called the:

a. Defendant
b. Plaintiff
c. Arbitrator
d. Complainant

Answer

- An individual who brings a lawsuit is called the:

a. Defendant
b. **Plaintiff**
c. Arbitrator
d. Complainant

Why?

- It is the plaintiff who brings the lawsuit against the defendant which can be either an individual or a company.

Question

- The HIM Department receives a subpoena duces tecum for records of a former patient. When the RHIT goes to retrieve the patient's medical records, its discovered that the record being subpoenaed has been purged and destroyed with no copy remaining in accordance with the state retention laws. In this situation, how should the department respond to the subpoena?

a. Inform defense and plaintiff lawyers tat the record no longer exists
b. Submit a certification of destruction in response to the subpoena
c. Refuse the subpoena since no record exists
d. Contact the clerk of the court and explain the situation

Answer

- The HIM Department receives a *subpoena duces tecum* for records of a former patient. When the RHIT goes to retrieve the patient's medical records, its discovered that the record being subpoenaed has been purged and destroyed with no copy remaining in accordance with the state retention laws. In this situation, how should the department respond to the subpoena?

a. Inform defense and plaintiff lawyers tat the record no longer exists
b. **Submit a certification of destruction in response to the subpoena**
c. Refuse the subpoena since no record exists
d. Contact the clerk of the court and explain the situation

Why?

- If the record has been destroyed, the imaged copy of the record would be the legal health record. This may not be the case if the paper record is retained. State laws typically view the original medical record as the legal record when it is available. Those who choose to destroy the original medical record may do so within weeks, months, or years of scanning. *If the record was destroyed according to guidelines for destruction and no scanned record exists, the* ***certificate of destruction*** *should be presented* ***in lieu of the record****.*

Question

- Which of the following is a core ethical obligation of HITs?

a. Coding diseases and operations
b. Protecting patients' privacy and confidential communication
c. Transcribing medical reports
d. Performing quantitative analysis on record content

Answer

- Which of the following is a core ethical obligation of HITs?

a. Coding diseases and operations
b. **Protecting patients' privacy and confidential communication**
c. Transcribing medical reports
d. Performing quantitative analysis on record content

Why?

- The responsibility of the HIM professional includes a wide range of functions and activities. Regardless of the employer, such as healthcare facility, vendor, pharmaceutical company, or research firm, the HIM professional's core ethical obligations are to protect patient privacy and confidential information and communication and to assure security of that information.

Question

- A home health care agency plans to implement a computer system whereby its nurses documents home care services on a tablet taken to the patient's home. The tablet will connect to the agency's computer network. The agency is in the process of identifying strategies to minimize the risk associated with the practice. Which of the following would be the best practice to protect the tablet and network data from a virus introduced from an external device?

a. Session termination
b. Encryption
c. Biometrics
d. Personal firewall software

Answer

- A home health care agency plans to implement a computer system whereby its nurses documents home care services on a tablet taken to the patient's home. The tablet will connect to the agency's computer network. The agency is in the process of identifying strategies to minimize the risk associated with the practice. Which of the following would be the best practice to protect the tablet and network data from a virus introduced from an external device?

a. Session termination
b. Encryption
c. Biometrics
d. Personal firewall software

Why?

- “The most commonly accepted network protection is a barrier, a firewall between the corporate network and outside world. The term firewall can mean many things to many people but basically it is a method of placing device-a computer or a router between the network and the Internet, to control and monitor all traffic between the outside world and the local network.” (source unknown, 2013)

- The firewall will protect from the virus while encryption of the data will keep the data secure. Biometrics serves to protect access to the tablet and session termination will prevent someone from gaining access to your system.

Question

- Community Hospital is implementing a hybrid record. Some documentation will be paper-based and digitally scanned post discharge. Other parts of the record will be totally electronic. The Medical Record Committee is discussing how interim reports in the health record should be handled; some committee members feel that all interim reports should be discarded and only the final reports retained in the scanned record. Others take the opposite position. What should the HIM director recommend?

a. Maintaining only the final results provides the greatest measure of security
b. Maintaining only the final results is the best option
c. Maintaining al interim reports provides the greatest measure of security
d. Maintaining only final reports results in a high volume of duplicate reports

Answer

- Community Hospital is implementing a hybrid record. Some documentation will be paper-based and digitally scanned post discharge. Other parts of the record will be totally electronic. The Medical Record Committee is discussing how interim reports in the health record should be handled; some committee members feel that all interim reports should be discarded and only the final reports retained in the scanned record. Others take the opposite position. What should the HIM director recommend?

a. Maintaining only the final results provides the greatest measure of security
b. Maintaining only the final results is the best option
c. **Maintaining al interim reports provides the greatest measure of security**
d. Maintaining only final reports results in a high volume of duplicate reports

Why?

- Maintaining all interim reports provides the greatest measure of security. Managing health information in a hybrid record environment is challenging, but by maintaining the reports the facility will reduce some potential problems. (AHIMA e-HIM work Group on health information in a Hybrid Environment 2010)

Resources for the Student

- RHIT/Domain6 – Quizlet
  - http://quizlet.com/22036882/flashcards

Sources

- Johns, M.L. Health Information Management Technology: An Applied Approach. Third edition, AHIMA Press
- Carter, D. Registered Health Information Technician (RHIT) Exam Preparation, 3rd, AHIMA Press
- Green, M. Essentials of Health Information Management: Principles and Practices, 3rd edition, Delmar

Q&A


The moment
you're ready to
quit is usually the
moment right
before the
miracle
happens.
Don't give up.