CRIS

Certified Release of Information Specialist

Training Guide and Certificate Instructions

Please view the following video at www.ahios.org:
Understanding the Release of Information Process: The Misconceptions Related to Processing and Delivering Electronic Health Records

Table of Contents

CRIS Overview

Introduction

Congratulations on your decision to earn a certificate as a Certified Release of Information Specialist (CRIS). This certificate will signify your professionalism and understanding in releasing protected health information (PHI). This module outlines the certificate program – what is required to take the examination and what will happen once you take the exam and pass the test.

Certification

A certificate will be awarded to individuals taking this examination and passing with a grade of 80% or greater. A certificate provides both personal validation and validation for employers and an employee's professional competence in the area of release of information. The certificate attempts to measure:

1. General medical records knowledge
2. Aptitude with regard to situations involving patient privacy
3. Understanding of all aspects of release of medical information
4. Understanding of terms related to HIPAA

Eligibility

Candidates taking this exam must have fulfilled one of the following AND must be employed by a member or client of the Association of Health Information Outsourcing Services (AHIOS):

1. Healthcare information credentialed (RHIT, RHIA or CCS)
2. Has worked previously in release of information (ROI) for at least 6 months
3. Has attended post secondary education in HIM but is not certified as an RHIT

Experience in release of information will be verified through the application that will require a resume of work experience and education.

A candidate's eligibility to take this exam will be done in writing to the candidate by the current company CRIS Test Representative.

Continued on next page

CRIS Overview, Continued

Non-Discrimination Policy	AHIOS does not discriminate against any applicant on the basis of race, color, creed, age, sex, national origin, religion, disability, marital status, parental status, ancestry, sexual orientation, military discharge status or source of income.

The Application Process

Overview

Examinations will be administered by a representative of each AHIOS member company. Test applicants, test scores and all relevant data will be maintained by the CRIS Test Representative from each member company.

To take the examination, you must complete an application and submit it to the representative of each AHIOS Company designated to administer the CRIS test. You will be sent the written test and will take the exam and mail it back to the representative of your company. Tests must be returned within 5 working days or less.

Tests must be taken in the presence of another individual who will vouch that the applicant taking the examination did not use outside sources, printed materials or online information while taking the test.

Completing the Application

An application to take the exam will be required prior to taking the test. All applications will be submitted to your company's CRIS Test Representative.

Incomplete Applications

Incomplete applications will be returned to the applicant.

Eligibility Appeals Process

Any applicant denied the opportunity to take the examination may appeal. Appeals must be made in writing to:

AHIOS CRIS Certification Application Committee
c/o Mariela Twiggs
1813 Claudius St.
Metairie, LA 70005
504-835-3453
Email: *mtt@velfile.com*

The burden of proof is borne by the applicant, to make a case as to why the applicant should be able to take this examination. Appeals must be made within 15 days of the application denial. The decision of the CRIS committee is final.

The Test Process

Preparing for the Test

The Certified Release of Information Specialist test attempts to measure a broad working knowledge of situations that affect how Protected Health Information is released to others. Because health information is private and protected under state and federal laws, the test has been designed for the applicant/tester to answer a number of multiple choice and true/false questions. There are no essay questions.

Questions chosen for the exam are not state specific. That is, it is not necessary to know a statute from a particular state in order to answer a question. Rather, many of the questions are situational where the best answer must be selected.

There are also some questions that relate to the Privacy Provisions within HIPAA. The applicant/tester must also have a working knowledge of the terms of the Privacy Provisions within HIPAA.

Taking the Test

This test is administered by paper. You will need to complete the exam and mail it in within 5 working days back to the representative of your company administering the test. Tests results will be mailed to the applicant/tester. Your test must be signed by someone willing to vouch that the test was taken without the aid of another person, printed information or information available online.

Test Results and Retesting

Test results will be mailed to the applicant/tester. If the applicant/tester did not receive a passing grade of 80%, the applicant/tester may re-take the examination only after reviewing the training materials. Test re-takes may be completed 30 days after the date of the original test. The passing grade for re-taking the test is 90%.

All test results must be sent to the CRIS Committee Chairperson. This test information will be added and maintained by the CRIS Committee Chairperson in an electronic format.

Continued on next page

The Test Process, Continued

Confidentiality of Test Results	The names of all applicant/testers will be protected by AHIOS.
Validation of Scores	The integrity of the scores is the responsibility of AHIOS. AHIOS has the right to void or withhold a score in question. Applicant/testers are expected to cooperate with any investigation necessary to determine the validation of a test score.
Issuance of Certificates	Certificates will be mailed to applicant/testers at the address on the application. Notification of those applicant/testers that pass the examination may be posted on the AHIOS website. (*www.AHIOS.org*)
Complaint and Appeals	Complaints may be made in writing within 30 days of the mailing of the test results. Complaints may be made to: AHIOS CRIS Certification Application Committee c/o Mariela Twiggs 1813 Claudius St. Metairie, LA 70005 504-835-3453 Email: *mtt@velfile.com*
Release of Test Results	Test results will be mailed to the applicant/tester. The results will be mailed within seven days of the receipt of the test.
Use of Certificate	The CRIS Certificate will be issued only to those applicants who have received a test score of 80% or higher. The CRIS Certificate gives the applicant the distinction of having applied knowledge about the privacy and security of health information. The test and certificate should also validate an individual's understanding of release of health information (ROI).

Continued on next page

The Test Process, Continued

Revocation of Certificate

Once the certificate has been issued, it may be revoked if it has been determined that the individual supplied false information on the application, had another person take the examination or engaged in inappropriate conduct during the examination. If the person who possesses the certificate engages in unethical behaviors during the course of employment where the applicant/tester is terminated from employment while working for an organization engaged in release of information services, the CRIS Committee and AHIOS has the right to revoke the certificate. Certificates are issued to individuals who not only pass the examination, but who have also proven they are honest and ethical in all dealings with Protected Health Information.

Certified Release of Information Specialist

Test Application & Work Experience

Personal Information

Name:_____

Address:_____

City, State, Zip:_____

Phone Number:_____

Email: _____

Employer

Current Employer:_____

Years with this employer: _____

Is your current employer a member or a client of AHIOS? Yes _____ No _____

Work Experience related to ROI

Where have you worked previously in release of information? (Additional information can be added on a separate sheet).

Name:_____

Address:_____

Phone Number: _____

How long did you work in this position?_____

List duties you performed for ROI that would qualify you to take the CRIS test?

_____

_____

Education

College (name): _____ Degree Received: _____

Post Secondary (name): _____ Degree Received: _____

Designations received: RHIT ____ RHIA ____ CCS ___ Other (name) _____

Signature: _____ **Date:** _____

Thank you for your application. Please submit it to your company's CRIS representative. They will notify you of your eligibility. Please retain a copy of the application and handbook materials for your reference.

CRIS Subcommittee for Association of Health Information Outsourcing Services (AHIOS)

The Medical Record

Contents

This chapter contains the following topics:

The Medical Record

Definition

The medical record is often referred to as the “who, what, when, where, and how” of patient care. It is a compilation of documents containing patient information, diagnosis and treatment during an episode of care or admission. Documentation may be handwritten; computer generated or appears in the form of films, graphs, and other images.

Uses of the Medical Record

The medical record serves the following purposes in healthcare:

1. To provide a communication tool between all healthcare providers. A physician, nurse, and any healthcare professional that treats the patient will complete documentation within the medical record.
2. To provide documentation regarding diagnosis, treatment, and care of the patient while confined or receiving services from a health care facility.
3. To provide information needed for medical billing of services rendered to the patient and hospital financial management.
4. To provide a medium for analysis, study, and evaluation of the quality of care given to a patient.
5. To assist in protecting the legal rights of the patient, the health care facility, and other healthcare providers.

Medical Data

Overview

The medical record consists of three (3) types of data:

1. Personal Data (Demographics): such as patient's name, address, telephone number, sex, race, religion, next of kin, etc.
2. Financial Data: this is comprised of the patient's insurance information.
3. Medical Data: includes physical examinations, medical history, progress notes, doctor's orders, laboratory reports and other studies, consultations, signed consent forms, etc.

The medical data makes up the largest portion of a patient's medical record and is the data most often requested from the chart. There are many medical forms and reports within the chart that the ROI Representative must be able to identify. Frequently encountered reports and their descriptions are outlined below.

Tool Gathered To Obtain The Complete Medical Record

A master patient index (MPI) is an electronic medical database that holds information on every patient registered at a health care organization.

The MPI stores information like patient name, date of birth, gender, race, social security number and place of residence alongside the patient's medical history. This provides a clear and complete view of an individual patient and also a large-scale view of the demographics. MPIs ensure that every patient should be represented only once.

Frequently Encountered Reports

Report	Description
Face Sheet (FS)	Usually the first page which contains the patient's name, address, family doctor, insurance information, diagnosis, etc.
Emergency Room (ER) Report	Record of treatment in the Emergency Department. May be part of an inpatient admission.
Discharge Summary (DS)	Summary of treatment the patient received. Includes the diagnosis of their ailment. This is usually a transcribed report.
History and Physical (H&P)	Reflects the history of the patient's disease or injury, as well as the history of treatment. Usually transcribed, but may be hand written at the beginning of the progress notes.
Consultation	Handwritten or transcribed report of examination and recommendations by the consulting physician.

Frequently Encountered Reports (continued)

Report	Description
Progress Notes	Daily notes of a physician's visit with the patient. May be multi-disciplinary and include notes from other healthcare professionals treating the patient. Some progress notes may be written using a format called "SOAP" charting. In this type of charting, the entries being made are Subjective, Objective, and also identify the Assessment and Plan of treatment.
Lab Reports	Results of specialized tests performed by the Laboratory Department and often computer generated.
Radiology (X-Ray), Scans and Nuclear Medicine	These are all specialized tests from the Radiology or Imaging Department. They are usually transcribed reports to corresponding films. Actual films or copies of films can be requested for release.
Electrocardiogram (EKG or ECG) & Electroencephalo-gram (EEG)	These are specialized tests for the heart (EKG) and the brain (EEG) that produce strips of findings that may be mounted on individual pages. These reports may also be transcribed.
Electromyogram (EMG)	Nerve conduction study used to evaluate the electrical activity produced by skeletal muscles.
Polysomnogram (PSG)	Sleep study usually found in the respiratory section.
Pulmonary Function Test (PFT)	A test designed to measure how well the lungs are working usually found in the respiratory section.
Physicians Orders	In addition to documenting in the progress notes, the physician must also document any orders for medications and/or treatments that he/she may request be given to the patient.
Operative Report (OR)	This is a summary report of the operation including a description of what was done and the findings. It is most often transcribed, but minor procedures may be hand written in the progress notes as a Procedure Note.
Operative Notes (OP)	Refers to any documentation about the actual operation such as the surgical list, anesthesia notes, recovery room notes, etc. Implant device information is often found within these documents.
Pathology Report (Path)	An analysis of anything removed from the patient during the operation (i.e., to check for cancer). This is a transcribed report completed by the Pathology Department.
Nurse's Notes	Daily notes that document the patient's progress or decline during a hospital admission. These usually include temperature, weight, blood pressure, pain measurement and general observations by the nursing staff. The notes may also be contained on large, foldout sheets for 24 hour nursing documentation in either the Intensive Care (ICU) or Cardiac Care Unit (CCU).

Medical Data, Continued

Frequently Encountered Reports (continued)

Report	Description
Graphic Charts	These are various reports that may graph intake and output of fluids, temperature, pulse, & respiration (TPR), etc.
Medication Reconciliation (MAR)	This report is a listing of all medications ordered for and dispensed to the patient. These reports can be either handwritten or computer generated
Immunization Records	Listing of all vaccinations given. This report is often comprehensive, with past immunizations as well.
Continuity of Care Document (CCD)	The CCD is generated from an electronic health record (EHR). It is a summary data set with demographic & clinical information about a patient's healthcare covering one or more encounters.

Admission Types

Type of Admission	Description
Inpatient (IP)	A patient is admitted to the hospital and occupies a bed for a period of at least 48 hours or more. An admission may last for days, weeks, or months.
Outpatient (OP)	A patient receives treatment or testing at the hospital but never occupies a bed. The episode of care is usually less than 24 hours at a time and can be spread out over days, weeks even months.
Observation	A patient is admitted to evaluate the need for inpatient care and generally doesn't exceed 24 hrs.
Ambulatory or Same Day Surgery (SDS)	A patient is admitted into the hospital for treatment and occupies a bed for 24-48 hours. This section may be filed in either the outpatient record or inpatient record, depending on the site.
Emergency Room (ER) or Emergency Department (ED)	A patient enters the hospital by way of the Emergency Room or Emergency Department, receives treatment and is released usually within a matter of hours. This visit to the ER is usually unplanned and is usually of an urgent nature. (Note: A patient may enter the hospital through the ER and receive treatment but due to the nature of the illness and required treatment, be admitted into the hospital. This admission is then classified as Inpatient rather than ER and the original ER Record becomes part of the Inpatient Record).

Various Types of Records and Documentation

Overview

Medical records can be maintained in several different formats including paper, microfilm, microfiche, and electronic (computerized) medium. They may be filed separately in different departments or in a centralized location. A “unit” record is one that contains all inpatient, outpatient and emergency department records of an individual patient in one specific file.

Unit Record

In some facilities, all admission types are filed together in one folder (called a unit record). In other hospitals, the different admission types may be filed in separate folders or even in separate locations or departments. Some or all of these records may be stored electronically. It is a requirement of the Joint Commission of Accreditation of Healthcare Organizations (JCAHO) that the facility (hospital, clinic, etc.) be able to assemble a “unit record” each and every time a patient receives treatment.

Who Owns the Medical Record

Every health care facility (includes hospital, clinic, physician office, etc.) is required to maintain the medical records of patients that receive care and must safeguard it from loss, damage, alteration and unauthorized use. The medical record is considered a legal document and may not be removed from the facility premises without a court order. Therefore, the actual medical record is the property of the facility in which it was created.

The content of the medical record belongs to the patient or an authorized patient representative. Copies of the medical record must be made available to the patient within a reasonable period of time, once the facility is in receipt of a valid request and authorization. A patient’s physician may prohibit release of the record to the patient if doing so may adversely affect the treatment and care of the patient. The physician is required to clearly document this restriction within the medical record.

Continued on next page

Various Types of Records and Documentation, Continued

Correction to the Medical Record

Because the medical record is a legal document, any correction to it must be done carefully and without obliterating the information being corrected. For instance, if an entry has been made by mistake, it should be corrected in the following way:

A single line is drawn through the incorrect words, phrase, or sentence(s). The word “error” is written above the lined sentence. The entry is signed and dated by the person making the correction.

In the instance of a transcribed medical report that needs correction, the physician may choose to dictate an amendment/correction to the report. This document is signed and placed with the original document.

Confidentiality and Security

Contents

This chapter contains the following topics:

Confidentiality and Security

Confidentiality

Confidentiality is an individual's right, within the law, to personal and informational privacy that includes the protection of patient health records. Confidentiality must be maintained by all health care workers, including physicians, and any contract employee working in a facility with access to patient information.

Security

Security of patient records involves protection from unauthorized disclosure, modification, or destruction. Security most often involves the physical safeguarding of patient information and records. Security extends to medical records, appointment scheduling, computer systems, financial data, management reports, and any other information that can be used to identify a patient. Passwords should never be shared or written down in an area where others can view them.

Destruction of Documents

When destroying protected health information that is no longer needed, the documents should be shredded such that the PHI cannot be read or otherwise reconstructed and electronic media have been cleared, purged, or destroyed at a secure location.

Breach of Confidentiality

Breach of Confidentiality & Security

Confidentiality is considered a contract that ensures that a patient's privacy is protected. Any time that contract is broken it is considered a "breach of confidentiality" and is a violation of the law. Both state and federal laws are in place to safeguard medical information. If state law is in conflict with federal law, whichever is the stricter of the two with more privacy protection will prevail.

Examples of a Breach of Confidentiality

- Disclosing the wrong patient's health information or wrong type of information or dates.
- Releasing records without a valid authorization
- Elevator, cafeteria, or hallway talk about private patient information
- Faxing records to an incorrect fax number
- Tossing discarded copies of patient records without shredding or placement in a recycle bin
- Taking records or copies of records home for personal use
- Leaving records open on counters, desks and any unauthorized area
- Discussing patient information with friends or family members
- Incorrect writing of mailing addresses on envelopes
- Releasing any sensitive records without the special authorizations that may be required (drug, alcohol, HIV, mental health, genetic, etc.)
- Unauthorized access or viewing of computer terminals
- Speaking loudly on the telephone or in the work area where someone may overhear patient health information

Continued on next page

Breach of Breach of Confidentiality Continued

Determining a Breach

According to the HITECH Act, a disclosure is considered a breach when unsecured protected health information is accessed, acquired or disclosed by an unauthorized entity and is not secured by a technology standard that renders protected health information unusable, unreadable or indecipherable to unauthorized individuals.

The HIPAA Omnibus Rule, passed in 2013, amended the Breach Notification Rule's "harm" threshold. Prior to Omnibus, when an improper disclosure was made, organizations were required to assess whether harm was likely in order to qualify as a breach. The Omnibus Rule now states that an improper disclosure is presumed to be a breach unless it is determined that a low probability exists that protected health information has been compromised. A risk assessment must be conducted regarding the following factors: 1) nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification, 2) the unauthorized person who used the PHI or to whom disclosure was made, 3) whether the PHI was actually acquired or viewed, and 4) the extent to which the PHI has been mitigated.

Some additional exceptions to a breach would include if the entity accessed the information in good faith, by unintentional acquisition, or if PHI was accessed or used by an employee or workforce; inadvertently disclosed to another authorized person within the entity or organized health care arrangement; if the recipient could not reasonably have retained the data; or the data is limited to a limited data set that does not include dates of birth or zip codes. If the risk assessment determines that the risk of harm to the individual is of low risk for disclosing the unsecured health information, then the disclosure would not have to be reported to the patient or the Department of Health and Human Services.

If the risk assessment is unable to demonstrate a low probability that the protected health information has been compromised, then HIPAA requires covered entities to provide notification to affected individuals and to the

Secretary of HHS. In the case of a breach of unsecured protected health information (PHI) at or by a business associate of a covered entity, the business associate is required to notify the covered entity of the breach immediately. The covered entity is required to report the notice of the breach electronically to the HHS Secretary without reasonable delay and no later than 60 days from the discovery of the breach for breaches affecting 500 or more individuals. For breaches affecting fewer than 500 individuals, the covered entity must provide a report of all breaches to the HHS Secretary annually within 60 days of the end of the calendar year in which the breaches occurred. Finally, it is required that the Secretary post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Notice to the individual shall be provided according to state guidelines, but no later than 60 days of the discovery of the breach. The notice must be given by either first-class mail at the last known address of the individual or the next of kin or by electronic mail. If there are 10 or more individuals to contact and there is insufficient or out-of-date contact information, a conspicuous posting can be done on the home page of the covered entity's website or notice in major print or broadcast media. If the information is listed on the website or in the media, a toll free number where an individual can learn whether or not the individual's information is possibly included in the breach must be listed.

Continued on next page

Breach of Breach of Confidentiality Continued

Content of Breach Notification

Regardless of the method by which notice is provided to individuals, notice of a breach shall include, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

3. The steps individuals should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, Web site, or postal address.

Identity Theft

Overview	Identity theft has become a huge problem and there is not a lot of data on what to do if this happens to you. Here are a couple of typical scenarios of what happens: A patient receives a bill from the hospital. The patient disputes the bill because they were never seen on that date at that hospital. The billing department argues that the patient was seen at the hospital and they have the patient's signature on the conditions of service. The patient goes to the hospital to compare the signatures and the signatures do not match. At this point a red flag should be sent to medical records department or a system flag that this account may be an identity theft situation and medical records may not be released.
What Happens	What typically happens is the patient goes directly to the medical records department and completes an authorization form to receive a copy of his/her medical records. One mistake after another happens and a copy of the medical records in question end up in the hands of an incorrect patient. The medical records do have that patient's name on the record, but the medical information does not belong to that patient. Therefore you may NOT release a copy of that specific account/encounter of medical records.
Additional Scenario	Another scenario is that the patient will come in to fill out an authorization before they go to the billing department. They will tell you their story and at that point it is necessary to call either the Privacy Officer, the Director of HIM or Patient Relations. Hospitals should have a policy and procedure for identity theft in place, but this is new to them and often times they do not.

HIPAA Privacy Rule

Contents

This chapter contains the following topics:

HIPAA

Overview

HIPAA stands for Health Insurance Portability and Accountability Act of 1996. It provides federal standards to ensure the privacy and security of every individual's medical and financial data. A portion of the Act, known as the Privacy Rule, provides protections against the misuse and disclosure of the individual's health records. Most organizations covered under HIPAA regulations had until April 14, 2003 to comply with the Privacy Rule. Health providers who violate HIPAA guidelines are subject to civil penalties for each offense. Anyone who deliberately violates individual privacy is subject to federal criminal penalties. The Office of Civil Rights (OCR) enforces HIPAA guidelines. Follow whichever law is the most stringent.

Patient's Rights

HIPAA provides for some basic patient rights, including:

1. The right of access to their protected health information; The Omnibus Rule also added the right to request information in the form and format desired such as an electronic copy.
2. The right to request correction or amendment of their record;
3. The right to an accounting of disclosures of most releases of information from their Protected Health Information (PHI).
4. The right to restrict the use and disclosure of their PHI. The Omnibus Rule added the right to restrict information from being released to their health insurance payer if the patient pays for treatment in full.
5. The right to file a formal complaint with the facility and to the Dept. of Health & Human Services, if they suspect a violation of the Privacy Rule and/or the policies and procedures of the facility.
6. The right to receive the provider's Notice of Privacy Practices.
7. The right to receive notification if their confidentiality has been breached.
8. The right to control the sale, marketing & research of their PHI.

Releasing Records (Disclosure) under HIPAA

HIPAA defines protected health information as information in any form or medium that is created or received by a healthcare facility and relates to the past, present or future condition of a patient and identifies or could be used to identify an individual. Under HIPAA, disclosures of patient information should be limited to the minimum amount necessary to satisfy the request. Minimum necessary rules do not apply to disclosures for treatment, to patients, pursuant to an authorization, and any requirements made by State or Federal law.

Continued on next page

HIPAA Authorization Requirements

The HIPAA rule (Section 164.508) pertaining to the release of protected health information states that an authorization for the release of medical records must be in plain language and contain the following elements in order to be valid:

√	Requirement
1	Identification of the persons or class of persons (i.e. physician practice; hospital) authorized to make the disclosure.
2	Identification of the persons or class of persons (i.e. attorneys; insurance companies) to whom the physician practice or hospital is authorized to make the disclosure to (recipients).
3	A description of the protected health information to be disclosed.
4	A description of each purpose for the use or disclosure of the protected health information; It is sufficient to put “at the request of the individual” on the authorization form, if the authorization was initiated by the patient.
5	An expiration date or event.
6	The individual's (patient) signature and date. If signed by a patient's personal representative (i.e. legal guardian), the relationship of the representative's authority to act on behalf of the patient must be documented.
7	A statement that protected health information used or disclosed pursuant to the authorization may or may not be subject to re-disclosure by the recipient and thus no longer protected by the Privacy Rule.
8	A statement that the patient may revoke the authorization in writing, with instructions for revoking the authorization.
9	A statement containing the inability / ability to condition treatment, payment or health plan enrollment or eligibility of benefits on whether the patient signs the authorization.

Continued on next page

HIPAA, Continued

Invalid Authorization

The authorization for release of information is not valid, according to the HIPAA statute, if the authorization has any of the following defects:

- The expiration date or event has passed.
- The authorization has not been filled out completely with respect to the required content listed above.
- The authorization is known by the physician practice or hospital to have been revoked.
- Any material information in the authorization is known by the physician practice or hospital to be false.

Request Without Authorization

Here are some requestors that are not required to provide an individual's authorization, provided that individual state law does not further prohibit disclosure without authorization:

- Coroners/funeral directors
- Organ procurement facilities
- Health agencies
- Correctional institutions
- Law enforcement (in limited situations)
- State Workers' Compensation programs.

Compound Authorization

HIPAA does not permit an authorization to be combined with any other document to create a compound authorization. For example, a consent to treat form cannot be combined with a release of information form. The authorization form can include all the elements of HIPAA, chemical dependence, HIV, genetic testing and other compliance issues all on one form.

Permitted Disclosures

There are several permitted disclosures outlined in the Privacy Rule. All disclosures that are specifically authorized by the patient are permitted. Disclosures for treatment purposes, payment purposes or health care operations purposes such as case management are all permitted without requiring the patient's authorization. Disclosures for research purposes are also permitted under certain conditions.

Continued on next page

HIPAA, Continued

HIPAA Exceptions

Another aspect of release of information is exceptions. These are permitted disclosures in which authorization is not required as long as state law allows these exceptions. For example, many states require reporting of conditions that affect public health to the Center for Disease Control. Some of these conditions include cancer, trauma and infectious diseases. In these cases, patient consent is not required to report to governmental agencies. Some examples are disclosures to abuse agencies, coroners, law enforcement officials, health licensing agencies, organ transplant activities, for certain research, to avoid a bio-terrorism threat and other specific government functions and workers compensation activities. Subpoenas are also generally exempt if it is requesting non-sensitive information, but they must comply with state law if it is more restrictive and requires authorization or court order.

Incidental Uses and Disclosures

Due to the nature of communications and practices that allow for individuals to receive prompt and effective healthcare, the potential exists for an Individual's Identifiable Health Information (IIHI) information to be disclosed incidentally. The HIPAA rule was not intended to put up roadblocks to these communications and practices, but covered entities must put into place reasonable safeguards to ensure protection of an individual's privacy. These reasonable safeguards should be evaluated by the covered entity to take into account the potential effects of patient care while considering the financial and administrative burdens of implementation.

Required Disclosures

There are two types of required disclosures under HIPAA- to the patient and to the Secretary of Health and Human Services (HHS) for compliance purposes. Disclosures to the patient, however, can be denied by the physician in certain situations where it may be harmful to the patient.

Individual (Patient) Access and Copy Charges

Overview & Designated Record Set

Patients are given the right to access their designated record set. The designated record set is more than the legal health record. It includes the medical records, billing records & any other records in which a decision is made about a patient, i.e. records from other facilities used in treatment. Patients also have a right to receive a copy of their health information in the form and format requested if the information is readily producible and maintained electronically. (For example, a patient requests a pdf file of their PHI from the EHR). If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

1. Copying, including labor and the cost of supplies (such as a CD); NOT to include retrieval or handling fees.
2. Preparing an explanation or summary of the protected health information, if agreed to by the individual.
3. Postage, when the individual has requested mail delivery.

Definition of Individual

An individual is defined as the actual patient or the personal representative. The personal representative is someone who stands in the shoes of the individual and has the ability to act for the individual and exercise the individual's rights.

<u>Examples of a personal representative are</u>:

- Anyone with healthcare power of attorney
- Court appointed legal guardian
- Parents of a minor (exceptions may apply)
- Executor of the estate or administrator of the will of a deceased patient
- Next of kin of a deceased patient

A personal representative does not typically include the patient's attorney or other parties not mentioned above. An attorney must provide a HIPAA compliant authorization or hold healthcare POA.

Access

Refers to the ability to learn the contents of a health record by reading it or obtaining a copy. The patient is generally required to sign an authorization form or a request for access form to obtain or read copies of his or her health information.

Patient Request for Accounting of Disclosures

Accounting of Disclosures

As mentioned above, HIPAA allows a patient to request a list or "accounting of disclosures" of some disclosures that are not specifically authorized by the patient/patient representative.

The HIM department must provide one free copy of this accounting in a twelve (12) month period. If the patient requests a second list during the same twelve month timeframe, the HIM department may "reasonably" charge for the preparation of this list.

Beginning April 14, 2003, and forward, a patient may receive an accounting of disclosures for records in paper format up to a six year period and any records in electronic format for a three year period from the date of the written request.

Covered entities have the choice of including information about electronic disclosures by their business associates, or providing a list of their business associates, which they then would be required to provide the accounting directly to individuals.

Amending the Medical Record

If a patient does not agree with something documented within the medical record, he or she cannot alter, change or require the facility to alter or change the medical record. According to HIPAA, the patient can request an amendment to the medical record, however, a covered entity may deny the request if it is found that the document was not created by the covered entity; the document is not a part of the designated record set; if the document would not be available for patient access or if it was deemed accurate and complete. If the amendment is allowed, this documentation will be placed within the medical record and must be included in any subsequent releases of that record. In either case, the patient is also to be informed.

Restriction of PHI

Patients may submit a written request to restrict the release of their medical records from certain individuals. They can also request that certain portions of their medical record be restricted from release. The healthcare facility has the right to either allow or deny the patient's request for restriction. It must, however, respond in writing either way and place this document into the medical record.

The Omnibus Rule added the requirement that facilities must restrict information from being disclosed to a patient's health insurance payer if the patient pays for the service in full and requests such restriction.

HIPAA Glossary of Terms

Glossary	The following is a glossary of terms that may assist you in further understanding of the HIPAA language.
Amendment	An amendment to a record indicates that the data is in dispute or in need of further clarification while retaining the original information.
Authorization	Upon receipt of a request for records not related to treatment, payment, or healthcare operations (TPO), the Covered Entity must obtain the patient's written authorization for the use or disclosure of protected health information (PHI).
Breach of Confidentiality	Violating the law by releasing privileged and private information to the public or to an individual without a valid authorization.
Business Associate (BA)	A person or organization that performs a function or activity on behalf of a covered entity, but is not part of the covered entity's workforce. A Business Associate must comply with HIPAA Privacy & Security rules and is liable and subject to fines for non-compliance.
Clinical Laboratory Improvement Act (CLIA)	States that clinical laboratories may provide clinical laboratory test records and reports only to "authorized persons" as defined primarily by state law. When, according to state law, an individual is not an authorized person, this restriction effectively prohibits the clinical laboratory from providing an individual direct access to this information.
Consent	A general document that may be required for treatment, payment or healthcare operations related uses.
Correction	Altering or replacing the original documentation.
Covered Entities	Includes health plans, health care clearinghouses, and health care providers (hospitals) that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transaction Rule.

Continued on next page

HIPAA Glossary of Terms, Continued

Glossary (continued)

Designated Record Set	Defined as a group of records maintained by or for a covered entity that includes the medical and billing records and any other record that documents decisions made about individuals such as enrollment, payment, claims adjudication, case management records for a health plan, pre-procedure questionnaires or records from other facilities used in the treatment of a patient.
Disclosure	The release, transfer, or access to information outside the entity holding the information.
HIPAA	Health Insurance Portability and Accountability Act of 1996
Individually Identifiable Health Information (IIHI)	Information that is a subset of health information, including demographic information collected from an individual, in the past, present and future where there is reasonable belief that the information can be used to identify the individual (telephone number, zip code, etc.).
Minimum Necessary Standard	Requires covered entities to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Non-Routine Disclosure	A disclosure for any purpose other than treatment, payment or healthcare operations (TPO).
Notice of Privacy Practices	This is a document that explains the following: How the covered entity may use and disclose protected health information about an individual. The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity. The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information. Whom individuals can contact for further information about the covered entity's privacy policies. The Notice of Privacy Practices must also include a description of the types of uses and disclosures that require patient authorization, must be displayed or posted on a healthcare facility's website and must be signed by patients upon their first visit to a physician.
OCR	Office of Civil Rights is the Health and Human Services entity responsible for enforcing the HIPAA Privacy Rule.
Protected Health Information (PHI)	Means individually identifiable health information. Examples: Names, addresses, zip codes, admission & discharge dates, birth date, telephone and fax numbers, e-mail addresses, Social Security number, Medical Record Number, Health Plan numbers, Account numbers, finger or voice prints, full face photographs, etc.
Psychotherapy Notes	Notes of a mental health professional about counseling sessions that are maintained separate and apart from the regular health record. These notes are protected under HIPAA and can't be disclosed without special authorization.

Continued on next page

HIPAA Glossary of Terms, Continued

Glossary (continued)

Qualified Protective Order	Prohibits uses or disclosure for other purposes and requires return or destruction of medical records.
Request	Written notice from the patient asking for records to be released.
Restriction	Right of an individual (patient) to request restriction of uses and disclosures of either certain components of his/her protected health information or to certain individuals.
Subpoena by Satisfactory Assurance	Upon request by a health oversight committee or law enforcement agency/official, a covered entity must temporarily suspend a patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official. The agency or official must provide a written statement indicating that such accounting to the patient would impede the agency's activities and must also specify the time for which the suspension is required.
Treatment, Payment, and Operations (TPO)	**"Treatment"** generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
Payment	Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.
Health Care Operations	Are certain administrative, financial, legal and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

HIM Department

Contents

This chapter contains the following topics:

HIM Department

Introduction

The Health Information Management/Services (HIM) Department or Medical Record Department is where all of the medical records are housed. The HIM Department consists of persons very well trained in all aspects of medical record analysis, completion, filing, reimbursement and release. Some of the staff may have earned a degree in medical records and may be credentialed through the American Health Information Management Association (AHIMA). A Registered Health Information Administrator (RHIA) designates completion of a four-year degree (BA or BS), while a Registered Health Information Technician (RHIT) usually indicates completion of a two-year degree (AAS) in health information management.

Medical Record Flow within the HIM Department

The medical record goes through several channels in the HIM Department. The names of the departmental areas may vary from one hospital/facility to another, but the areas are basically the same. The typical flow of the medical record in the department is as follows:

Step	Action
Upon Patient Admission for Treatment	The medical record is created by the documents first completed by the Admitting Department and then all documentation and reporting that transpire in the nursing unit or other “patient care area.” It resides in this area until the patient is discharged from the facility.
Chart is Received in the HIM Department	Someone from the Patient Care Area or nursing unit, such as the Unit Assistant, or an employee of the HIM Department will retrieve the discharged record(s) from the nursing unit and bring it down to the HIM Department. The chart is usually not in final order at this point.

Continued on next page

Medical Record Flow within the HIM Department (continued)

Step	Action
Chart Assembly Desk	A member of the HIM Department assembles the health information documents into universal chart order and creates a folder labeled with a color-coded medical record number.
Chart Analysis Desk	A member of the HIM Department proceeds to analyze the medical record. This is the process of checking for completeness of the reports such as the History and Physical and dictated reports are present and signed. Summaries, as well as checking for signatures and dates on required entries. A colored tab is usually used to indicate the area in need of a signature or date. This information is often logged into a computerized deficiency tracking system for monitoring purposes.
Coding Shelves	After being analyzed, the medical record goes to the Coders, who then assign the appropriate ICD-9-CM diagnosis and procedure codes needed for reimbursement to the hospital for the care provided.

Continued on next page

Medical Record Flow within the HIM Department (continued)

Step	Action
Incomplete/Doctors' Area	If the medical record is still missing certain reports, signatures/dates, follow up, etc. it is considered, "incomplete". At this time, it is taken to the "Chart Incomplete Area", where the record is kept until the physician(s) completes the deficiencies documented on the "Deficiency Sheet" or in the computerized chart deficiency system. Some facilities have many components of the medical record computerized and are able to provide "electronic signature" capabilities to its medical staff. This eliminates the need to visit the HIM department in person to complete deficient charts.
Permanent File Area/Complete File	Once the chart is coded and the identified chart deficiencies are completed, the medical record is taken into the permanent/Complete File Area where it remains for a time determined by both space and the facility's record retention policy. You must check with your facility for exact time frames and retention policies since they can vary from facility to facility and state to state. If the patient is re-admitted, most often the chart is "re-activated" and the above process continues. Some medical records are maintained in off-site storage facilities; others may be sent for microfilming or may be electronically scanned.

Medical Records Filing System

Medical Record Filing System

The medical record may be filed in the HIM Department in several different ways, according to the rules of the department. The most common filing system is Terminal Digit Order (TDO or TD). This filing system requires the medical record number to be read from right to left in groupings of digits (usually two digits).

For example, 123456 would break down into groupings of 2-digits such as 12-34-56. When filing by TDO, you do not read the number from left to right, instead, you read from right to left. For example, according to the filing rules of the facility, 12-34-56 may be read/filed as:

12 – 34 – 56 (most common)
3rd 2nd 1st

Or in some cases:
12 – 34 – 56
2nd 3rd 1st

Filing can also be done as straight-numeric, which is simply read from left to right or in some cases middle-digit filing, where the middle set of numbers is read first. It is necessary to check with the Manager to determine which filing system is used in the HIM department.

Authorization and Request

Contents

This chapter contains the following topics:

Authorization

Definition

An authorization must have certain components for it to be considered valid for disclosure under HIPAA:

- It must be written in plain language and identify:
- The name of the patient
- Person authorized to disclose the information
- The purpose for the disclosure
- The specific information to be released
- The party to whom the information may be released to
- The individual's right to revoke the authorization and how to revoke it
- An expiration date or event
- The signature of the patient or person authorizing the release
- The date the authorization was signed
- A statement about the inability / ability to condition treatment, payment, or health care decisions on whether the patient signs the releases
- A statement that the information may be redisclosed and is no longer protected by HIPAA
- A statement that the patient has a right to receive a copy of the authorization form.

Timeframes

According to HIPAA, a HIM department must respond to patient requests within 30 days unless the patient requests an electronic copy from an EHR for which the facility is participating in the CMS "Meaningful Use" program. In that scenario, turnaround time would be 3 business days. Also, stricter state laws often require a response time of less than 30 days.

Deceased Patients

The executor or administrator of the estate of a deceased patient and next of kin generally have full access to a patient's designated record set in their role as patient representative. In addition, any relevant state laws will apply when determining next of kin. Next of kin may be noted on the Death Certificate.

Continued on next page

Authorization, Continued

Conservators

A conservator is appointed by the courts to act on behalf of the patient. Sometimes the powers of a conservator are automatically terminated upon the patient's death. Therefore, a conservator who had access to the patient's medical record while the patient was alive has no right to access the patient's medical records after their death. The patient is allowed to access their records as well if such authority is granted.

Power of Attorney

Power of attorney may be assigned to an individual to act for the patient. This patient allows the appointed individual to conduct certain acts with respect to the patient's real and personal property or with respect to matters, which affect the patient's real or personal property. Laws in different states will affect the powers assigned to this person. Often, Power of Attorney is referred to as POA. In some cases, there is a distinction between POA for business transactions versus Durable Health Care POA for medical decision-making. Note that power of attorney is only relevant while the patient is living. At the time of death, authority would flow to the personal representative.

Birth and Death Certificate Records

Most facilities have personnel responsible for the preparation of birth certificates. While these documents, along with death certificates, may often be found within a patient's health information records, this information must never be reproduced and released. The requestor should be directed to contact the local Bureau of Vital Statistics to obtain a copy of these documents.

Substance Abuse, HIV, Psychiatric Records, Genetic Testing

Special authorization is needed for records that contain sensitive information. This may not be an official ruling in some states, nor under federal regulations, such as HIPAA, however, most facilities have special policies in place to protect this information. If any sensitive information is in the medical record, you should take extra care to check the authorization. Sensitive information includes:

- Psychological
- Psychiatric
- Substance Abuse (drug or alcohol)
- Social Work
- AIDS (HIV
- STD (sexually transmitted disease)
- Genetic Testing

Continued on next page

Authorization, Continued

Consent and Authorization of Minor Records

A minor patient (an individual under the majority age of 18 years) may authorize ROI under the following circumstances:

- When seeking services for venereal diseases, pregnancy, or drug, alcohol, or emotional abuse
- When in a mental health facility and consenting release to minor's own attorney
- When emancipated by marriage
- When a minor patient (not emancipated) has a child, the minor can sign for her child. However, the consent for ROI for the same minor must be signed by the minor's legally responsible person

Otherwise one of the following signatures must be present for release:

- Parent or legal guardian for a minor
- Person holding Durable Healthcare Power of Attorney
- Custodian (person or agency) granted custody of a minor

Peer Review / QIO

Definition

PRO (Peer Review Organization)/QIO (Quality Improvement Organization)-These type of requestors are for government programs that assist and audit the hospital department in assuring that quality care is being provided to Medical Assistance program participants and that charges billed are accurate. They are very important to the hospital. They are exempt from HIPAA and do not require a signed authorization from the patient, even for sensitive records. They are date sensitive and if not done properly could cost the hospital in fines and penalties. Use extreme caution paying close detail as to what is being requested (specific date, encounter number, entire, specific report, etc.). Some organizations do not allow do-over's.

Common Organizations

Each region may have different names, but here are a few examples:

- CDAC
- Lumetra
- Buccaneer
- Cal Optima
- Clear Visions
- CMS
- Heritage
- Secure Horizons
- Triwest
- Viant
- HSAG (Health Services Advisory Group), etc.).

Types of Requests

Introduction	This section contains different types of requests and why the requester may need records.
Deposition	Sometimes attorneys will send deposition letters asking you to comply with their subpoena before they submit a subpoena. Until you actually receive the subpoena or the patient's authorization to release medical records you cannot release records.
Non Custodial Parent	Non-Custodial parents have rights to their child's medical records under certain conditions: • If the parent is the guarantor • If there are no legal proceedings against the non-custodial parent A non-custodial parent loses their rights when: • CPS has removed the child • There is a restraining order against the non-custodial parent • The non-custodial parent is under investigation for wrongdoing
Insurance	Insurance Underwriters process applications for life and health insurance while Insurance Adjusters process claims for benefits related to accidental injuries. A HIPAA compliant authorization must be obtained for disclosures to a life or disability Insurer.
Federal Alcohol & Drug Abuse Confidentiality Regulations	Federal Alcohol and Drug Abuse Confidentiality Regulations [42 C.F.R. ***§***2.1 et seq.] supersedes HIPAA laws. This regulation applies to patient records of alcohol or drug abuse programs that receive federal assistance.

Continued on next page

Types of Requests, Continued

Subpoena

An order directed to an individual commanding him/her to appear in court on a certain day to testify or produce documents in a pending lawsuit. These are normally signed by an attorney.

Subpoenas are governed by each state's jurisdiction and each state has different requirements for what is needed in order to comply with the subpoena. For example, some states require that the patient be notified that the records are being sought and other states do not.

Subpoena Categories

Subpoena	Definition
Civil Subpoena	are broken out between the following: • **Deposition subpoenas-** records are requested for a deposition. • **Subpoenas Duces Tecum** –records are to be delivered to the court.
Criminal Subpoena	Also called Investigatory Subpoena. Investigatory subpoenas under HIPAA require for reasonable attempts to provide notice to the patient or to obtain a qualified protective order.

Important exceptions to a Subpoena

Information such as HIV test results, test results from rhesus blood type, hepatitis B and HIV tests performed under certain circumstances, hospital medical staff committee records, mental health records, and any type of physician-patient privileged information and records pertaining to treatment for substance abuse may be protected from subpoenas by statute.

A subpoena with satisfactory assurance is exempt from the HIPAA valid authorization requirements and indicates the requestor made a good faith attempt to provide written notice to the patient and the notice included sufficient information to permit the patient to object(quash), the objection time elapsed and there were no objections filed or resolved.

Custodians Affidavit /

The records shall be accompanied by an affidavit or statement of facts

Certification

about the custodian and the records provided. Normally the custodian or other qualified witness completes the form.

If the business has none of the records described, or only part thereof, the custodian or other qualified witness shall state this in the affidavit and deliver the affidavit and those records that are available to the requestor.

Continued on next page

Types of Requests, Continued

Court Orders

A legal document issued by a court of law requiring a person to do something or to refrain from doing something. It is an official proclamation by a judge that defines the legal relationships between the parties to a hearing, a trial, an appeal or other court proceedings. A court order must be signed by a judge.

If a facility receives a court order signed by a judge, then the facility does not need a signed authorization from the patient in order to release the information requested.

Student Immunization Records

The Omnibus Rule clarified that if a parent requests student immunization records to be sent to a school in a state where they are required for school enrollment, a HIPAA compliant authorization is not necessary, but documentation of the request is recommended. The facility's policy must be consulted.

Worker's Compensation

No Authorization Required: The Privacy Rule permits health care providers to submit health information, without an authorization, to the Board and the carrier or employer in three situations:

- Pursuant to an order of a Workers' Compensation Law Judge (WCLJ). This exemption can be found in the Privacy Rule at 45 CFR §164.512. Thus, if a WCLJ directs the taking of medical testimony or depositions, health care providers are not restricted by HIPAA.
- In compliance with Workers' Compensation Law with reasonable assurances from the requesting party that the claimant has been notified. This exemption can be found in the Privacy Rule at 45 CFR §164.512 (e) and (l). WCL §13-a(4)(a) requires health care providers to regularly file medical reports of treatment with the Board and the carrier or employer.
- For the health care provider's own payment operations. This exemption can be found in the Privacy Rule at 45 CFR §164.502(a)(1)(ii) and §164.501 definition of "payment." WCL §13-f requires that medical records be provided to the Board and the carrier or employer before they are required to pay for any medical services. Thus, a health care provider must provide the required medical information in order to be paid.

When a Covered Entity May Release Records

Release of Records

A covered entity is permitted to disclose an individual's health information as necessary to comply with and to the full extent authorized by workers' compensation law. **45 CFR 164.512(a)**

When the individual's written authorization has been obtained and is consistent with the Privacy Rule's requirements at **45 CFR 164.508**, a covered entity may disclose protected health information about an injured workers' previous condition. A covered entity would be permitted to make the above disclosure if the individual signed such an authorization.

Individuals do not have a right under the Privacy Rule at **45 CFR 164.512(a)** to request that a covered entity restrict a disclosure of protected health information about them for workers' compensation purposes, if the disclosure is required or authorized by a workers' compensation law. **45 CFR 164.522(a)**.

Practice Questions

Overview

Introduction

In this section you will find a page of practice questions and the answers to those questions following.

Contents

This chapter contains the following topics:

Practice Questions

1. Jane's aunt passed away and Jane wants to get a copy of her aunt's death summary. She fills out an authorization form and shows legal proof that she is a beneficiary. Her aunt was married and there is a surviving spouse. Why or why not is she entitled to get a copy of the death summary?

2. John is the middle child of three siblings. His mother is the widow to his deceased father. John would like to get a copy of his father's medical record and has filled out an authorization form. Why or why not is he entitled to get a copy of his father's records?

3. A patient requests a copy of their medical records for an ER visit that transpired last month. She fills out an authorization form and shows you a picture ID. You pull the ER record and check the patient's signature on the conditions of admission (COA) only to find out that the signatures are the same name, but the handwriting does not match. Why or why not would you release the records to the patient?

4. Law enforcement request a copy of a patient's medical record and has a signed authorization from the patient. The police tell you that it is for identity theft. Why or why not can you release the records to them?

5. You receive an authorization that is signed by the patient, but it was not dated. Why or why not is this authorization valid and would you or would you not honor the authorization?

6. You receive an authorization from the mother of a 12 year old son. She is requesting a copy of his medical records where he was seen for a sexually transmitted disease in which he signed for his own care. Why or why not is she entitled to receive a copy?

7. A 17 year old girl was seen at an abortion clinic where she had an abortion. Later the next day she develops complications and goes to the emergency room to seek further care. Her mother requests copies of her medical records. Since the patient is still a minor, Mom signs the release form. Why or why not is mom entitled to these records?

8. The police request a copy of a patient's medical record who was involved in a traffic collision. The patient has given consent to the police for these records. The medical report shows that the patient had been drinking. Why or why not are these records protected?

Answers to Practice Questions

1. Being a beneficiary does not provide access to a decease patient's records. The best practice would be to have the surviving spouse sign an authorization form allowing Jane to receive copies of the medical record.

2. John is not entitled to receive copies of his father's medical record. The mother would need to provide proof of identity and sign an authorization form in order for John to receive copies of his father's medical record. Also, the scenario does not state how old John is and he may be a minor. However, if John is an adult and resides in a state whereby state law allows access to the records of a deceased patient by the children of the deceased, he would indeed be allowed access.

3. The information should not be released, since this may be a case of identity theft. The appropriate departments should be informed and a red flag should be placed on the file. The facility should then investigate the medical record further. If you have knowledge that an authorization is invalid, it should not be relied upon.

4. The records should not be disclosed to law enforcement under these circumstances. With there being identity theft involved, the records may not be those of the person that signed the authorization form. It would be best to obtain a court order before releasing the medical records.

5 The authorization should not be honored. Date is a required element of a valid authorization.

6. Depending on what state this took place in, the minor would also have to sign the authorization form in order for the mother to receive a copy of the medical record. When dealing with sensitive information such as sexually transmitted diseases, some states allow minors age 12 and older to authorize the release of records; other states start at age 13 or 14.

7. The mom is not entitled to receive copies of the medical records. Some states have specific laws that protect minors seeking abortions. The minor would need to sign the authorization form in order for the mother to be able to access the records.

8. Yes, the records may be released, since the patient gave consent to release the records to the police.