Welcome to PMI’s Webinar Presentation

Brought to you by:
Practice Management Institute®
pmiMD.com

Meet the Presenter…

Maxine Collins, MBA, CPA,
CMC, CMIS, CMOM

On the topic:
Frequently Asked Questions: Medical Record Issues
Welcome to Practice Management Institute’s Webinar and Audio Conference Training. We hope that the information contained herein will give you valuable tips that you can use to improve your skills and performance on the job. Each year, more than 40,000 physicians and office staff are trained by Practice Management Institute. For 30 years, physicians have relied on PMI to provide up-to-date coding, reimbursement, compliance and office management training. Instructor-led classes are presented in 400 of the nation’s leading hospitals, healthcare systems, colleges and medical societies.

PMI provides a number of other training resources for your practice, including national conferences for medical office professionals, self-paced certification preparatory courses, online training, educational audio downloads, and practice reference materials. For more information, visit PMI’s web site at www.pmiMD.com

Please be advised that all information in this program is provided for informational purposes only. While PMI makes all reasonable efforts to verify the credentials of instructors and the information provided, it is not intended to serve as legal advice. The opinions expressed are those of the individual presenter and do not necessarily reflect the viewpoint of Practice Management Institute. The information provided is general in nature. Depending on the particular facts at issue, it may or may not apply to your situation. Participants requiring specific guidance should contact their legal counsel.

CPT® is a registered trademark of the American Medical Association.
FREQUENTLY ASKED QUESTIONS: MEDICAL RECORDS ISSUES

Presented by:
Maxine I. Collins
MBA, CPA, CMC, CMIS, CMOM
Faculty, Practice Management Institute
Director of Compliance, Audits and Education, CoreMD Partners, LLC

INTRODUCTION

• Fundamentals of medical record documentation
• What is “Information Governance” and how is AHIMA involved?
• Legality of the medical record
• Some of the HIPAA Requirements including Designated Record Set
• Common “pitfalls” in medical record documentation
• Other Federal and state laws and regulations
• Frequently Asked Questions
FUNDAMENTALS OF MEDICAL RECORD DOCUMENTATION

• Purpose of complete and accurate patient records?
  – Continuity of care
  – Quality of care
  – Means of communication between:
    • Physicians and other providers of services
    • Physicians/Providers and members/patients
      – For:
        » Assessment and Diagnoses
        » Treatment
        » Planning
        » Delivery of Care
        » Preventive health care and services

AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION (AHIMA)
“FUNDAMENTALS OF THE LEGAL HEALTH RECORD AND DESIGNATED RECORD SET”

• Legal Health Record Definition and Role

  – Legal Health Record:
    • “The legal health record serves to identify what information constitutes the official business record of an organization for evidentiary purposes. The legal health record is a subset of the entire patient database.”
    • “…the documentation of healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization.”
    • “An organization’s legal health record definition must explicitly identify the sources, medium, and location of the individually identifiable data that it includes (i.e., the data collected and directly used in documenting healthcare or health status.”
    • “The documentation that comprises the legal health record may physically exist in separate and multiple paper-based or electronic systems.”

Source: http://library.ahima.org/doc?oid=104008#.WbrTObkGMbA
• Functions of legal medical record document:
  – Supporting evidence of decisions made in patient’s medical care;
  – Reimbursement for insurance payers must be substantiated by documentation in the medical record;
  – Provides information that will be used for any formal requests for information in court.

Source: http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA

• What should organizations consider when defining the legal health record?
  • Important to have Policies and Procedures to review:
    – Functions available in EHR system that can generate the relevant information.
      • Clinical decision support functions?
      • Digital image import?
      • Patient portals?
    – If patient portal functions are available, will the information entered by the patient be included in the legal medical record?
    – Addressing “copying and pasting” in the medical record.
    – Timeliness of completing and closing the EHR patient record.
    – Following the General Principles of Medical Record Documentation
    – Meeting the requirements of Insurance Contracts and reimbursement guidelines.
    – Meeting HIPAA and other Federal and state guidelines.

Source: http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA
**Designated Record Set Definition and Role (AHIMA)**

- "The HIPAA privacy rule defines the designated record set:
  - As set as a group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

- The designated record set also contains:
  - Individually identifiable data stored on any medium and collected and directly used in documenting healthcare or health status. It includes clinical data such as WAVE files, images (e.g., x-rays), and billing information.

- The designated record set is generally broader than the legal health record because it addresses all protected health information. While the legal health record is generally the information used by the patient care team to make decisions about the treatment of a patient, the designated record set contains protected health information along with business information unrelated to patient care."

Source: [http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA](http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA)

---

**WHAT IS “INFORMATION GOVERNANCE”?**

- **Information governance** helps manage and control information by supporting the organization's activities and ensuring compliance with its duties.

- Patients entrust their personal information to healthcare organizations, creating distinct requirements for confidentiality, privacy, and security.

Source: [www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx](www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx)
AHIMA: Leading Information Governance for Healthcare

AHIMA Panelists
- Moderator: Margarita L. Valdez, Director, Congressional Relations, AHIMA
- Angela Kennedy, EdD, MBA, RHIA, President, AHIMA
- Meryl Bloomrosen, MBA, MBI, RHIA, FAHIMA, Vice President for Public Policy, AHIMA
- Deborah K. Green, MBA, RHIA, EVP, Operations and Chief Operating Officer, AHIMA

eHealth Summit -- Download presentation and Appendices at: https://www.cms.gov/eHealth/downloads/eHealthSummit_PanelPress_051914.pdf

Why Information Governance (IG)?
- Business and consumer life
  Create 2.5 quintillion bytes
  Of data every day
- Over 50 million Tweets
  Per day
- 2.9 million emails
  Are sent every second
- billion YouTube Videos were watched yesterday
- billion YouTube Videos were watched yesterday
- Over 20 hrs of
  YouTube Video uploaded
  Every minute
WHAT INFORMATION ARE WE PROTECTING UNDER HIPAA?

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   A. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   B. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000. (What?)
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death data, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Vehicle identifiers and serial numbers, including license plate numbers’
6. Fax numbers;
7. Device identifiers and serial numbers;
8. Email addresses;

Source: http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA
18+1 IDENTIFIERS (HIPAA)

9. Web Universal Resource Locators (URLs)
10. Social Security Numbers;
11. Internet Protocol (IP) addresses;
12. Medical Record numbers;
13. Biometric identifiers, including finger and voice prints;
14. Health plan beneficiary numbers;
15. Full-face photographs and any comparable images;
16. Account numbers;
17. Any other unique identifying number, characteristic, or code, except as permitted by paragraph © of this section; and
18. Certificate/license numbers; (and +1)
19. Any other identifier that the Secretary of Health and Human Services determines needing protection.

Source: http://library.ahima.org/doc?oid=104008#.WbrTObKGMbA

HHS.GOV-HEALTH INFORMATION PRIVACY

• YOUR MEDICAL RECORDS:
  – The Privacy Rule gives you, with few exceptions, the right to inspect, review, and receive a copy of your medical records and billing records that are held by health plans and health care providers covered by the Privacy Rule.
  – Access - Only you or your personal representative has the right to access your records.
    • A health care provider or health plan may send copies of your records to another provider or health plan only as needed for treatment or payment or with your permission.
    • The Privacy Rule does not require the health care provider or health plan to share information with other providers or plans.
  – Charges - A provider cannot deny you a copy of your records because you have not paid for the services you have received.
    • However, a provider may charge for the reasonable costs for copying and mailing the records. The provider cannot charge you a fee for searching for or retrieving your records.
INFORMATION PRIVACY

- Provider’s Psychotherapy Notes - You do not have the right to access a provider’s psychotherapy notes.
  • Psychotherapy notes are notes that a mental health professional takes during a conversation with a patient. They are kept separate from the patient’s medical and billing records. HIPAA also does not allow the provider to make most disclosures about psychotherapy notes about you without your authorization.

- Corrections - If you think the information in your medical or billing record is incorrect, you can request a change, or amendment, to your record. The health care provider or health plan must respond to your request. If it created the information, it must amend inaccurate or incomplete information.
  • If the provider or plan does not agree to your request, you have the right to submit a statement of disagreement that the provider or plan must add to your record.
  • See 45 C.F.R. §§ 164.508, 164.524 and 164.526, and OCR's Frequently Asked Questions.

THE PRIVACY ACT OF 1974

- Gives individuals the right to access and request amendments to their records.
- Defines a record as “any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.”

Court Orders and Subpoenas

Court Order

- A HIPAA-covered health care provider or health plan may share your protected health information if it has a court order. This includes the order of an administrative tribunal. However, the provider or plan may only disclose the information specifically described in the order.

Source: HHS.gov, "Health Information Privacy, Your Medical Records"; https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html

EMPLOYEES OF MEDICAL ENTITIES

- "Under HIPAA everybody is supposed to have access only to the minimal necessary to do their job," Practice Notes blogger and Illinois-based attorney Ericka L. Adler told Physicians Practice. "You’re not your own doctor obviously, so just because you work somewhere doesn’t mean you should be able to access your own medical records."

- "In addition, while every patient has a right to his or her own record, that doesn’t mean any patient (including a practice employee or physician) should bypass the HIPAA patient record-related protocols that should be in place at all practices, Steven Kabler, an attorney at Denver-based Jones & Keller told Physicians Practice."

- "What happens is under HIPAA there are a number of regulations that deal with the security of medical records," he said. For instance, covered entities must ensure the confidentiality of all health information they receive, and they must enact procedures and policies to keep that information secure."

- "To protect the integrity of the medical records and to protect the confidentiality, a healthcare provider should go through the procedures that a patient would go through in order to access their record," said Kabler."

THE CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS REGULATION

- Allows federally subsidized alcohol and drug abuse programs to give patients access to their own records, including the opportunity to inspect and copy any records that the program maintains about the patient;
- Defines records as “any information, whether recorded or not, relating to a patient that received or acquired services by a federally assisted alcohol or drug program.”

Source: HHS.gov; “Health Information Privacy, Your Medical Records”; https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html

THE OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION

- Requires employers to document certain employee illnesses and injuries, including medical care provided in relation to those injuries on the job.
- Employees and their designated representative have regulated “confidentiality requirements” for that information; and
- Generally have access to such injury reports and related health records.
STATE LAWS

- Many states also have laws or regulations that provide individuals rights to their health information.
- Some states may define health information more broadly than the federal HIPAA rules.
- Some states may not limit access and amendment to PHI in a designated record set.
- When state laws or regulations afford individuals greater rights of access, the covered entity must adhere to state law.

TECHNOLOGY AND THE GROWING IMPORTANCE OF QUALITY TO MEASURE REIMBURSEMENT

- Technology:
  - Quickly and dramatically changing world of healthcare.
  - Mobile electronics
    - Smartphones, “Apps”, Ipad, Tablet PCs, Touchscreens, Digital ink, Voice Recognition, Patient Portals, Telemedicine, Cloud computing
    - Dependence on these devices are now “a way of life”
    - What happens during and after a disaster?
  - Hacking and breaches of EHR
COMMON “PITFALLS” IN MEDICAL RECORD DOCUMENTATION

• All members of staff are involved in “Risk Management” for the medical entity.
• Electronic Medical Record:
  – Timeliness of Documentation
  – Accuracy of Documentation
  – Completeness of the Medical Record
  – “Cloning”
  – “Copying and Pasting”
  – Mobile technology
  – Interoperability (HIEs)
  – Medical malpractice cases – the medical record in the courtroom

FREQUENTLY ASKED QUESTIONS

1. Who owns the medical record? Do the records belong to the patient?
2. What is the difference between a Court Order and a Subpoena for medical records?
3. There are three types of Subpoenas. What are the requirements of each?
4. What is a HIPAA defined “breach” of Protected Health Information (PHI)?
1. WHO OWNS THE MEDICAL RECORD?

- **HIPAA – 09/04/2017 – “Health Information Privacy; Your Medical Records”:**
  - "The Privacy Rule" gives you, with few exceptions, the right to inspect, review, and receive a copy of your medical records and billing records that are held by health plans and health care providers covered by the Privacy Rule.
  
  - **Access:** “Only you or your personal representative has the right to access your records.” “HIPAA gives you important rights to access – PDF your medical record and to keep your information private.
  
  - **Charges:** “A provider cannot deny you a copy of your records because you have not paid for the services you have received.” “However, a provider may charge for the reasonable costs for copying and mailing the records. The provider cannot charge you a fee for searching for or retrieving your records.”
  
  - See 45 C.F.R. ¶¶ 164.508, 164.524 and 164.526, and OCR’s Frequently Asked Questions.

Source: https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html

WHO OWNS THE MEDICAL RECORD?

- Confusion exists in today’s health information management industry.

- Who actually owns the original medical record?
  
  - Many believe the patient owns their record.
  
  - However, does the physician who created the record and/or the facility in which the record was created actually own the record, while the information within the medical record is owned by the patient?
  
  - What about the clinical information having to be shared with several agencies for reporting in today’s focus on population health management – data being accumulated in data warehouses to be analyzed?
  
  - What about the “integrated” world of Electronic Health Records, such as those gathered and used by Accountable Care Organizations (ACOs)?
WHO OWNS THE MEDICAL RECORD?

• What concerns could develop with the advancing use of Telehealth?
  – In the article, “Patient records: The Struggle for Ownership”, published December 10, 2015 and written by Ken Terry, the author states, “Identifiable data is protected health information (PHI), and, as such, is covered by HIPAA. But HIPAA has exceptions for treatment, payment, and business operations.”
  – “The lawyers agree that the use of identifiable data in population health management can be justified as quality improvement activities that are a part of operations.”
  – The author continues by stressing the “minimum necessary” release of information required under the HIPAA rules. Where will the lines be drawn?

• Consideration also has to be given to various state laws.

STATE LAWS GOVERNING MEDICAL RECORDS

• Some state laws indicate that the medical record is owned by the health care provider, hospital, or patient.
• Court decisions regarding ownership impact providers in specific states.
  – In a Michigan case - McGarry v. J.A. Mercer Co. in 1935, the court held that x-ray negatives were the property of the physician who made them, not the patient. (Health Information & the Law; HealthinfoLaw.org); “Who Owns the Medical Records: 50 State Comparison”.
  – A case in Illinois (Holtkamp Trucking Co. v. David J. Fletcher, M.D., L.L.C.) in 2010 held that the medical records were the physician’s property. (Health Information & the Law; HealthinfoLaw.org); “Who Owns the Medical Records: 50 State Comparison”.
• The following graphic provides information on the state law in 50 states.
“Who Owns the Medical Record?”

- Although the medical record contains patient information, the physical documents belong to the physician. Indeed, the medical record is a tool created by the physician to support patient care and is an asset of the practice.

- When a physician leaves a multiple-physician setting, the question often arises, “Which physician owns which record?”
  - Answer: Unfortunately, there is no single answer because ownership often depends on specific facts. Ideally, to avoid any ambiguity over medical records ownership, the physicians should agree about ownership “up-front”, before entering into the group arrangement. Otherwise, the parties may have to rely upon general Texas business law, and such disagreements may turn nasty and costly.

- When physicians, each in private practice, share office space, no legal combination actually takes place. The physicians own their records separately.

- Be sure to consult an attorney regarding an agreement or dispute about medical records. If you have questions, e-mail the TMA Knowledge Center or call 800-880-7955.

Source: https://www.texmed.org
NEW HAMPSHIRE

• “The state of New Hampshire considers all medical records the property of the patient, although an individual with power of attorney or a party that has been given written consent may also access these records.”


• “As it turns out, New Hampshire is the only state in which patients are explicitly deemed to have ownership of their medical record. Though it should be noted the law states patients own the data and information contained in the record.”

Source: Health Information Technology, ”Who owns patient records? In N.H. only, the patients do” Written by Akanksha Jayanthi | November 10, 2015

WHAT IS A SUBPOENA?

• A Latin phrase sub poena – meaning under penalty.
• A legal document that:
  – Commands a person or entity to testify as a witness at a specified time and place (at a deposition, trial, or other hearing); and/or
  – To produce documents or other tangible objects in a legal proceeding.
  – Subpoenas are time-sensitive with court-imposed deadlines.
  – Who can issue a subpoena?
    • In most cases, “a subpoena can be issued and signed by an attorney on behalf of a court in which the attorney is authorized to practice law.
    • If the subpoena is for a high-level government official (such as the Governor, or agency head), then it must be signed by an administrative law judge.
    • In some cases, a non-lawyer may issue a subpoena if acting on his or her own behalf (known as pro se representation).

SUBPOENA OF MEDICAL RECORDS

• Civil subpoena – also known as “subpoena duces tecum”:
  – “duces tecum” – “You shall bring with you”.
  – Seeks copies of your medical records;
  – May be asked to provide an authenticating affidavit for the records. (Affidavit - a written statement confirmed by oath or affirmation, for use as evidence in court);
  – If you are concerned that you cannot confirm the records are “true and correct” (such as when the records have been created by another physician or provider), it is best to contact your malpractice liability insurance carrier for advice.

SUBPOENA OF MEDICAL RECORDS

– Obtaining patient permission for complying with a subpoena:
  • Do not need a patient’s permission if the patient is a party to the suit;
  • If unclear as to whether patient is a party to the suit or when the records contain sensitive information, always better to have the patient provide a written release;
  • If patient permission cannot be obtained, ask the requesting attorney for written assurances from the requesting party that the patient received proper notice (e.g., get a signed medical release);
  • (NOTE: IMPORTANT POINT – ALWAYS BETTER TO GET PATIENT TO SIGN A PROPER WRITTEN RELEASE IF POSSIBLE.)
  • Depending on the set up of your entity, you will have to follow written policies and procedures in place, or confer with physician involved before releasing records.
  • If policy and procedures are not written and in place, consult with practice’s legal counsel. If the subpoena is too broad or there is sensitive information, you may be able to challenge the subpoena and get the requested information restricted or even get the subpoena quashed.


HIPAA – MEDICAL RECORD SUBPOENAS

• Requires that you follow your state law in responding to subpoenas.
• Also requires:
  – Receipt of adequate assurances from patient that they have been put on notice by the requesting party (e.g., obtaining a written statement or documentation); or
  – Requesting party to demonstrate that they have made a reasonable attempt to get a protective order (e.g., by providing a copy of a court order or stipulation); or
  – You to obtain an appropriate written release from the patient.
  – Failure to respond – may result in an “order to produce”, and “order to show cause”, and possibly an accusation of “contempt of court”.
  – Any issues with subpoenas must be addressed in a timely fashion.
  – Contact your malpractice insurance carrier if you are unable to get sufficient permission from patient and/or assurances from attorney involved.

SUBPOENAS WITH NOTICE– FROM AN ATTORNEY’S PERSPECTIVE

- For many litigators, subpoenas are the most common method of obtaining medical records.
- Under HIPAA, the simple issuance of a subpoena is no longer sufficient to obtain medical records.
- However, subpoenas can still be used to obtain records as long as the provider receives written satisfactory assurances that the patient has received notice and the opportunity to object.
- This translates into the extra step of issuing a notice letter to the patient’s attorney that gives a date certain upon which any objections must be made.
- Then a copy of the letter must be included when the subpoena is served upon the records custodian.
- Some attorneys have started responding to notice letters by issuing their own letter stating they have no objection to the subpoena. This is a commendable practice since it enables the requesting party to issue the subpoena before the objection deadline expires.
- In notifying the records custodians, the requesting party should include a copy of the letter stating no objection.


SUBPOENA FOR TESTIMONY

- Subpoena ad testificandum (pronounced “ad test-te-fi-kan-dum”)”
  - Requires you to testify before a court, or other legal authority.
- Subpoenas can be civil or criminal related.
- Claims of negligence such as malpractice allegations will be in civil court.
- A civil subpoena – may seek someone in your office for testimony (deposition);
- A notary public or court reporter may issue this type of subpoena – but if you are being summoned to testify at trial, the court clerk will issue the subpoena.
- Details giving instructions to what you must do to comply will be stated on the face of the subpoena.

CRIMINAL SUBPOENAS

• In Texas – issued by the court;
• Will more than likely require that you provide your original record, rather than a copy of the record.
• Always make a copy of the record for office before you release original.

MEDICAL RECORDS FACT SHEET - OHIO

MEDICAL RECORDS FACT SHEET
STATE AND FEDERAL REQUIREMENTS CONCERNING DISCLOSURES OF MEDICAL RECORDS

Physicians are regularly requested to provide health information related to or about their patients. Both the Ohio Revised Code and the provisions of HIPAA (collectively, “HIPAA”) contain provisions obligating the physician to provide information and, in other cases, impose restrictions on the circumstances under which the information can be provided. In a number of respects the provisions of Ohio law and HIPAA are not consistent. As a general rule, in any particular situation a physician would need to comply with the more restrictive of the two. What this means is that where Ohio law would permit the disclosure, but HIPAA would not, then HIPAA would control. Where HIPAA would permit the disclosure, but Ohio law would not, then Ohio law must be complied with.

Permitted Disclosures Without Patient Authorization

HIPAA permits a physician to disclose patient information in connection with treatment, payment, or what are known as “health care operations.” An example of “health care operations” is the disclosure of patient information to the physician’s malpractice defense counsel in a situation where the patient sued the physician for medical malpractice. Ohio law does not have a specific provision limiting the disclosure of health information in the context of treatment, payment, or health care operations.

EXAMPLE OF ONE POLICY

GREATER DAYTON AREA HOSPITAL ASSOCIATION
POLICY AND GUIDELINES
FOR RESPONDING TO
SUBPOENAS FOR MEDICAL RECORDS

There has been a recognized variance in the method of releasing medical records pursuant to subpoenas among the members of GDAHA. The members of GDAHA, wishing to operate in a consistent manner, have authorized and approved the following policy and guidelines for responding to subpoenas for medical records.

The general policy and procedure for the release of medical records in all cases will be to secure a signed patient authorization or a court order authorizing the disclosure. It is the responsibility of the party requesting the record to supply the signed patient authorization or the court order. It is the responsibility of the party requesting the record to supply a reason with the appropriate documentation why a signed authorization or court order is not necessary.

The purpose of this policy and these guidelines is to protect the privacy of Hospital patients and to assist Hospitals in compliance with the law regarding the disclosure of confidential patient information.

HOW A SUBPOENA IS SERVED

• Typically requested by an attorney and issued by a court clerk, a notary public, or a justice of the peace.
• Once issued, a subpoena may be served on an individual in one of several ways:
  – “Hand-delivered (also known as “personal delivery” method);
  – E-mailed to the last known e-mail address of the individual (receipt acknowledgement requested);
  – Certified mail to the last known address (return receipt requested); or
  – Hearing it read to you aloud.”

HOW TO RESPOND TO A SUBPOENA

1. Don’t ignore it.
   • It is part of a court's legal process
   • Failure to respond to a subpoena is considered contempt of court in most states

2. Read through the subpoena.
   • Determine what is being requested and/or who is being asked to appear
   • Subpoena requests for documents and other items are usually very detailed and specific
   • Make sure to protect and keep any documents in your possession safe

3. See who is requesting the information and why:
   • You need to adequately prepare if testimony is required.
   • Note hearing date and time to avoid potential penalties and other consequences.

4. Consult with an attorney.
   • Your attorney may be able to assist you in getting additional time if that is necessary to gather the requested information, or develop you may have concerning what is being asked of you.

5. Follow the entity’s Policies and Procedures, document properly and copy only what is requested.

DEFINITION OF “BREACH” ACCORDING TO HIPAA

• Under HIPAA, a breach is defined as “the unauthorized acquisition, access, use or disclosure of protected health information (PHI) which compromises the security or privacy of such information.”

• Protecting Health Information: the HIPAA Security and Breach ...

Source: https://www.privacyrights.org/printpdf/67499
COMMON EXAMPLES OF HIPAA VIOLATIONS

• Entity Rescinds Improper Charges For Medical Record Copies to Reflect Reasonable, Cost-based Fees:
  – Patient alleged covered entity failed to provide access to his medical records.
  – After OCR notified entity of allegation, they released medical records but charged $100 for "a records review fee.
  – Privacy rule permits a "reasonable cost-based fee that includes only cost of copying, postage and preparing an explanation or summary if agreed to by individual.
  – Resolution – Covered entity refunded $100 "records review fee.


COMMON EXAMPLES OF HIPAA VIOLATIONS

• HMO Revises Process to Obtain Valid Authorizations:
  – Complaint alleged HMO incorrectly disclosed PHI by sending entire medical record to disability insurance company without authorization.
  – OCR investigation indicated form used by HMO was not a valid authorization under the Privacy Rule.
  – OCR required corrective actions:
    • HMO had to create a new HIPAA-compliant authorization form; and
    • Implement new policy that directed staff to obtain patient signatures on these forms before responding to any disclosure requests, even if patients bring in their own “authorization form”.
    • New Authorization form specifies what records and/or portions of the files to be disclosed and the authorization will be kept in patient’s record, together with the disclosed information.

HIPAA RESOLUTION AGREEMENTS AND CIVIL MONETARY PENALTIES

• Careless handling of HIV information jeopardizes patient’s privacy, costs entity, costs entity $387,000.
  - St. Luke’s-Roosevelt Hospital Center
    - 09/2014 – HHS Office for Civil Rights (OCR)
      - Complaint alleging staff member disclosed impermissibly PHI to complainants employer.
      - PHI included sensitive information:
        - Concerning HIV status, medical care, sexually transmitted diseases, medications, sexual orientation, mental health diagnosis and physical abuse
        - PHI was faxed to patient’s PHI to his employer rather than sending it to the requested personal post office box.
    - In addition, OCR discovered:
      - A center within the hospital was responsible for a related breach of sensitive information that had occurred 9 months prior to the 09/2014 incident; and
      - Had not addressed the vulnerabilities in their compliance program to prevent impermissible disclosures.
  - OCR stated, “Individuals cannot trust in a health care system that does not appropriately safeguard their most sensitive PHI,” said Roger Severino, OCR director.
  - “Covered entities and business associates have the responsibility under HIPAA to both identify and actually implement these safeguards. In exercising its enforcement authority, OCR takes into consideration aggravating factors such as the nature and extent of the harm caused by failure to comply with HIPAA requirements.”

Source: HHS.gov; HIPAA Resolution Agreements; https://www.hhs.gov/about/new/2017/careless-handling-hiv-information-costs-ent.html

TEXAS HEALTH SYSTEM SETTLES POTENTIAL HIPAA VIOLATIONS - $2.4 MILLION

• Memorial Hermann Health System (MHHS)
  - Agreed to pay $2.4 million to U.S. Dept of HHS; and
  - Adopt a comprehensive corrective action plan to settle potential violations of disclosing a patient’s PHI without an authorization in September, 2015.
  - Patient presented an allegedly fraudulent I.D. card to office staff who immediately alerted authorities and patient was arrested.
  - Disclosure of PHI to law enforcement was permitted under HIPAA rules.
  - However, MHHS subsequently published a press release concerning incident in which MHHS senior management approved the impermissible disclosure of patient’s PHI by adding the patient’s name in the title of the press release.
  - In addition, MHHS failed to timely document the sanctioning of its workforce members for impermissibly disclosing patient’s information.
  - In addition to fine, a correction action plan required MHHS to:
    - Update its policies and procedures on safeguarding PHI from impermissible uses and disclosures;
    - To train its workforce members; and
    - Required MHHS facilities to attest to their understanding of permissible uses and disclosures of PHI, including disclosures to the media.

Source: HHS.gov; HIPAA Resolution Agreements; https://www.hhs.gov/about/new/2017/careless-handling-hiv-information-costs-ent.html
$2.5 MILLION SETTLEMENT SHOWS THAT NOT UNDERSTAND HIPAA REQUIREMENTS CREATES RISK
– APRIL 24, 2017

• Settlement based on impermissible disclosure of unsecured electronic PHI:
  – CardioNet – 1st settlement involving a wireless health care provider who provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.
  – January, 2012 – Workforce member’s laptop stolen from a parked vehicle outside employee’s home; laptop contained ePHI of 1,391 individuals.
  – OCR’s investigation revealed CardioNet had an insufficient Risk Analysis and Risk Management Program/processes in place at time of theft.
  – Additionally, CardioNet’s Policies and Procedures implementing required standard of HIPAA Security Rule were in draft form and had not been implemented.
  – Further, the Pennsylvania-based organization was unable to produce any final Policies or Procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.
  – “Mobile devices in the health care sector remain particularly vulnerable to theft and loss,” said Roger Severino, OCR Director. “Failure to implement mobile device security by Covered Entities and Business Associates puts individuals’ sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected.”

Source: HHS.gov; :HIPAA Resolution Agreements”; https://www.hhs.gov/about/new/2017/careless-handling-hiv-information-costs-entity.html

AHIMA – RECOMMENDED PRACTICES FOR AUTHORIZATIONS

• Privacy and security experts recommend HIPAA-covered entities adhere to the following practices:
  – Study both federal and state requirements for authorizations
  – Draft an authorization form that complies with federal and state laws and regulations (see “Sample Authorization to Use or Disclose Health Information,” in appendix A)
  – Ask the risk manager and legal counsel to review your draft authorization form
  – Update or generate new policies and procedures relative to the new authorization
  – Order appropriate quantities of the approved authorization form
  – Educate and train staff
  – Post the approved authorization form on the organization’s website
  – Distribute new authorization forms to frequent requestors

FAQ’S MEDICAL RECORDS AND HIPAA

1. Are state fee schedules permitted to be charged to individuals when providing them with a copy of their PHI under the HIPAA Privacy Rule?
   – Answer: No, except in cases where the State authorized costs are the same types of costs permitted under the HIPAA Privacy Rule, and are reasonable.
   – HIPAA permits a covered entity to charge a reasonable, cost-based fee that covers only certain limited labor, supply, and postage costs that may apply in providing an individual with a copy of PHI in the form and format requested or agreed to by the individual.
   – Therefore, labor (e.g., for search and retrieval) or other costs not permitted by the Privacy Rule may not be charged to individuals even if authorized by State law.

2. If a State law requires that a health care provider give individuals one free copy of their medical records but HIPAA permits the provider to charge a fee, does HIPAA override the State law?
   – Answer: No, so the health care provider must comply with the State law and provide the one free copy.
   – In contrast to State laws that authorize higher or different fees than are permitted under HIPAA, HIPAA does not override those State laws that provide individuals with greater rights of access to their health information than the HIPAA Privacy Rule does.
   – This includes State laws that:
     • prohibit fees to be charged to provide individuals with copies of their PHI; or
     • allow only lesser fees than what the Privacy Rule would allow to be charged for copies.

Source: “Individuals’ Right under HIPAA to Access their Health Information”; HHS.gov.; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
FAQ’S MEDICAL RECORDS
AND HIPAA

3. Can a health care provider charge an individual a fee to only inspect his/her PHI at the covered entities office (i.e., does not request that the covered entity produce a copy of the PHI)?
   – Answer: No. The fees that can be charged to individuals exercising their right of access to their PHI apply on in cases where the individual is to receive a copy of the PHI, versus merely being provided the opportunity to view and inspect.
   – HIPAA Privacy Rule provides the right for an individual to inspect their PHI held in a “designated record set”, either in addition to obtaining copies or in lieu thereof, and requires Covered Entities (CEs) to arrange with the individual a convenient time and place to inspect their record.
   – In addition, a CE may not charge an individual who, while inspecting his/her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information.
   – A CE may establish reasonable policies and safeguards regarding an individual’s use of his/her own camera or other device for copying PHI to assure that equipment or technology used by the individual is not disruptive to entity’s operations or used in a way that enables the individual to copy or otherwise memorialize only the records to which he/she is entitled.
   – In addition, a CE is not required to allow individuals to connect a personal device to the CEs systems.

Source: Individuals’ Right under HIPAA to Access their Health Information”; HHS.gov.; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/

4. What is a covered entity’s obligation under the Breach notification Rule if it transmits an individual’s PHI to a third party designated by the Individual in an access request, and the entity discovers the information was breached in transit?
   – Answer: If the PHI was “unsecured PHI” as defined under HIPAA, the CE generally is obligated to notify the individual and HHS of the breach and otherwise comply with the HIPAA Breach Notification Rule at 45 CFR, 164, Subpart D.
   – However, if the individual requested that the CE transmit the PHI in an unsecured manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the insecure transmission, still wanted to have the PHI sent in that manner, the CE is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required.
   – In addition, a CE is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.
   – Where the PHI was breached as “secured” as provided in the HHS Guidance Specifying the Technologies and Methodologies that Render Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html) the CE does not have reporting obligations under the Breach Notification Rule.

• Moral to that story: Be aware of the information contained in the above referenced information or make sure your forms specify that the individual agreed to have the PHI sent unsecured with patient’s signature.

Source: Individuals’ Right under HIPAA to Access their Health Information”; HHS.gov.; https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access.
FAQ’S MEDICAL RECORDS AND HIPAA

5. **Does an individual’s right under HIPAA to access their health information apply only to the information a health care provider maintains about the person in an Electronic Health Record (EHR) or paper medical record?**
   - **Answer:** No. An individual has a broad right under the HIPAA Privacy Rule to access the PHI about them in all designated record sets maintained by or for a CE, whether it be in electronic or paper form, not just the designated record set that comprises the “medical record.”
   - A “designated record set” includes billing and payment records, claims and insurance information, as well as other records that are used, in whole or in part, by or for the CE to make decisions about individuals. See the definition of “designated record set” at 45 CFR 164.501.

6. **Does the individual have a right to access PHI about themselves from a CE that is very old or is archived?**
   - **Answer:** Yes. They have right of access regardless of the date the information was created and maintained by the CE or whether the information is onsite, held remotely, or is archived.
   - There are only very limited grounds under which a CE may deny an individual access to PHI about themselves in a designated record set, which do not include age or location of the information.

HHS.GOV – YOUR MEDICAL RECORD

- **Can telemarketers obtain my health information and use it to call me to sell goods and services?**

  **Answer:**
  "Under the HIPAA Privacy Rule, a covered entity can share protected health information with a telemarketer only if the covered entity has either obtained the individual’s prior written authorization to do so, or has entered into a business associate relationship with the telemarketer for the purpose of making a communication that is not marketing, such as to inform individuals about the covered entity’s own goods or services."

  "If the telemarketer is a business associate under the Privacy Rule, it must agree by contract to use the information only for communicating on behalf of the covered entity, and not to market its own goods or services (or those of another third party)."

HHS.GOV – YOUR MEDICAL RECORD

• How does the HIPAA Privacy Rule affect my rights under the Federal Privacy Act?

• Answer
  – The Privacy Act of 1974 (U.S. Department of Justice) protects personal information about individuals held by the Federal government.
  – Covered entities that are Federal agencies or Federal contractors that maintain records that are covered by the Privacy Act not only must obey the Privacy Rule’s requirements, but also must comply with the Privacy Act.

Source: HHS.GOV, YOUR MEDICAL RECORD

HHS.GOV – YOUR MEDICAL RECORD

• If I do not object, can my health care provider share or discuss my health information with my family, friends, or others involved in my care or payment for my care?

• Answer:
  • Yes. As long as you do not object, your health care provider is allowed to share or discuss your health information with your family, friends, or others involved in your care or payment for your care.
  • Your provider may ask your permission, may tell you he or she plans to discuss the information and give you an opportunity to object, or may decide, using his or her professional judgment, that you do not object. In any of these cases, your health care provider may discuss only the information that the person involved needs to know about your care or payment for your care.
  • Here are some examples:
    – An emergency room doctor may discuss your treatment in front of your friend when you ask that your friend come into the treatment room.
    – Your hospital may discuss your bill with your daughter who is with you at the hospital and has questions about the charges.
    – Your doctor may talk to your sister who is driving you home from the hospital about your keeping your foot raised during the ride home.
    – Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
    – Your nurse may tell you that he or she is going to tell your brother how you are doing, and then your nurse may discuss your health status with your brother if you did not say that he or she should not.
  • BUT your nurse may not discuss your condition with your brother if you tell your nurse not to.

Source: HHS.GOV, YOUR MEDICAL RECORD
HHS.GOV – YOUR MEDICAL RECORD

• If my family or friends call my health care provider to ask about my condition, will they have to give my provider proof of who they are?
  – **ANSWER:** HIPAA does not require proof of identity in these cases. However, your health care provider may have his or her own rules for verifying who is on the phone. You may want to ask your provider about her or his rules.

• Can I have another person pick up my prescription drugs, medical supplies, or x-rays?
  – **ANSWER:** Yes. HIPAA allows health care providers (such as pharmacists) to give prescription drugs, medical supplies, X-rays, and other health care items to a family member, friend, or other person you send to pick them up.

Source: HHS.GOV, YOUR MEDICAL RECORD

HHS.GOV – YOUR MEDICAL RECORD

• Since the HIPAA Privacy Rule protects a decedent’s health information only for 50 years following the individual’s death, does my family health history recorded in my medical record lose protection when it involves family members who have been deceased for more than 50 years?
  – **Answer:** No. When a covered health care provider, in the course of treating an individual or otherwise, collects an individual’s family health history, this information becomes part of the individual’s medical or other record and is treated as protected health information about the individual and not about the family member(s).
  – Thus, even where an individual’s family health history includes information about family members who have been deceased for more than 50 years, the information is protected under the Privacy Rule as the health information of the individual.

Source: HHS.GOV, YOUR MEDICAL RECORD
PROPER DESTRUCTION OF MEDICAL RECORDS?

• In general, examples of proper disposal methods may include, but are not limited to:
  – For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
  – Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
  – For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).
  – For more information on proper disposal of electronic PHI, see the HHS HIPAA Security Series 3: Security Standards – Physical Safeguards - PDF. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization. - PDF.

THE MEDICAL BOARD OF CALIFORNIA

• How long does a physician have to send me the copy of medical records I requested?
  – If you made your request in writing for the records to be sent directly to you, the physician must provide copies to you within 15 days.
  – The physician can charge a reasonable fee for the cost of making the copies.
  – If the physician's office advises you that a fee will be charged for the records, the medical records do not need to be provided until the fee is paid.
  – If the physician does not comply within the time frame you can file a written complaint with the Medical Board.
THE MEDICAL BOARD OF CALIFORNIA

• Can a doctor charge to send a copy of my records to another doctor?
  – Most physicians do not charge a fee for transferring records, but the law does not govern this practice so there is nothing to preclude them from charging a copying or transfer fee.
  – There is also no time limit for record transfers, or no penalty for failure to transfer the records, since this is a professional courtesy.
  – You might wish to contact your local medical society to see if it has developed any guidelines on record transfer issues.

VIRGINIA BOARD OF MEDICINE

• How do I get a copy of my medical record?
  • A request for copies of medical records must be in writing, dated and signed by the person making the request, and include a reasonable description of the records sought. If someone is making a request on your behalf, he or she must provide evidence of the authority to receive the records (such as a power of attorney). The provider must accept a photocopy, facsimile, or other copy of the original signed by the requester as if it were an original (Virginia Code § 32.1-127.1:03).
  • Upon receipt of such a request, the health care provider has 30 days to do one of the following:
    – provide copies of the records or allow electronic access to the requested health records to any requester authorized to receive them in electronic format if so requested;
    – inform the requester if the information does not exist or cannot be found;
    – inform the requester of the provider who now maintains the records;
    – deny the records for specific reasons set out in Section F of the statute.
  • § 32.1-127.1:03 also provides that the patient's physician or clinical psychologist may make a notation in a patient's record that furnishing of the records "would be reasonably likely to endanger the life or physical safety of the individual or another person, or that such health record makes reference to a person other than a health care provider and the access requested would be reasonably likely to cause substantial harm to such referenced person." If a patient’s request for his record is denied for this reason, the provider must permit the record to be copied and reviewed by a provider, selected by the patient, of similar background to the individual who made the notation in the chart, and that practitioner may make a judgment as to whether the records should be made available to the patient.

Source: https://www.dhp.virginia.gov/medicine/medicine_faq.htm#Medical_Records
NEW YORK STATE

- **Records Retention - New York State Department of Health**
  
  - Patient care data files containing medical treatment and/or billing information must be retained for 6 years or 3 years past the patient's eighteenth birthday, whichever is longer.
  
  - **Summary record** of all patients treated and/or transported must be retained for 3 years. ...
  
  - Reports containing **billing information** - 7 years

Source: https://www.health.ny.gov/professionals/ems/policy/08-03.htm

Utah Code Ann. § 78B-5-618

- **Medical Records Collection, Retention, and Access in Utah**
  
  - Patient access to medical records - Third party access to medical records
    
    - If a health care provider is considered a covered entity under HIPAA, a patient or personal representative may inspect or receive a copy of the patient's record from that provider in accordance with 45 C.F.R. Parts 160 and 164.
      
      - If a health care provider is not considered a covered entity under HIPAA, a patient or personal representative may inspect or receive a copy of the patient's records unless access to the records is restricted by law or judicial order.
    
    - Any health care provider who provides a copy of a patient's records must comply with the deadlines required by HIPAA (45 C.F.R. 164.524(b)), and may charge a reasonable cost-based fee that only includes the cost of copying (including supplies for and labor of copying), and postage (when the patient or representative requested that the copy be mailed).
    
    - Any health care provider or other person authorized to provide records who provides a copy of a patient's records to an authorized third party must provide a copy within 30 days after receipt of notice; and
    
    - May charge a reasonable fee to cover the provider's costs of up to $20 per request for locating the records, copying charges up to $0.30 per page for pages 1-40 and up to $0.30 per page for pages 41 and above, the cost of postage (when the third party requested that the copy be mailed), and any sales tax owed.

Current as of June 2015
Medical Records

Documentation Standards

A. EMAC and HSO Documentation Standards
1. Maintain each medical record on paper and/or in electronic format in a manner that is timely, legible, current, and organized that permits effective and coordinated patient care and quality review.
2. Access to the medical record must be restricted to authorized personnel involved in the patient’s care.
3. Medical record entries must be dated and signed by the provider or other qualified person.
4. Provide for clear identification of authors for all entries.
5. Document the reasoning behind diagnostic and therapeutic decisions.
6. Document patient education for the presenting complaint(s) or problem(s).
7. Document discussion of advance directives at least annually.

B. DC-DHHM Documentation Standards
In addition to the EMAC and HSO standards, DC-DHHM has established the following standards with which its providers are also expected to comply:
1. Have appropriate safeguards in place to protect the confidentiality of the medical record in accordance with applicable state and federal laws.
2. Access the medical record in a centralized secure location, accessible only to authorized personnel and retrievable in timely manner by office staff and practitioners.
3. Periodically provide training to office staff and practitioners for maintaining the confidentiality and security of patient information.
4. Only release confidential information in accordance with applicable laws and regulations.
5. Ensure the medical record contains sufficient biographical and demographic information (e.g., date of birth, sex, address, marital status, emergency contact information).
6. Allogeneic and the adverse reactions in a uniform location of the record, or the data, if known drug allergy (HDA), if applicable.
7. For medications prescribed, documentation must include name, strength, amount, duration for use, and refills. Efficacy should be documented on follow-up.
8. Treatment follow-up plan and patient discharge instructions for each patient.
9. Document all health services reviewed and documented for patients of all ages, such as but not limited to, immunizations, well visits, weight counseling, and BMI assessment, etc. (physical health only).
10. Diagnostic test results and other prescribed therapies with evidence of the provider’s review and patient modification of assigned results.
11. Documentation of any outpatient surgery, hospitalization, referred and evidence of practitioner review reports, signed release of information allowing for communication between practitioners.

Table A-7. State Medical Record Laws: Minimum Medical Record Retention Periods for Records Held by Medical Doctors and Hospitals* (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>Medical Doctors</th>
<th>Hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connecticut</td>
<td>7 years from the last date of treatment, or, upon the death of the patient, for 7 years. Conn. Agencies Regs. §§ 10a-14-42 (2006).</td>
<td>16 years after the patient has been discharged. Conn. Agencies Regs. §§ 19-13-03(3)(b) (2006).</td>
</tr>
<tr>
<td>Delaware</td>
<td>7 years from the last entry date on the patient’s record. Del. Code Ann. tit. 24, §§ 1761 and 1702 (2006).</td>
<td>N/A</td>
</tr>
<tr>
<td>Georgia</td>
<td>10 years from the date the record was created. Ga. Code Ann. §§ 31-33-10(a)(13) and 31-33-2 (2008).</td>
<td>Adult patients 5 years after the date of discharge. Minor patients 5 years past the age of majority (i.e., until patient turns 21). Ga. Code Ann. §§ 31-33-10(a)(13) and 31-33-2 (2008); 31-7-2 (2008) (granting the department regulatory authority over hospitals) and 12a. Comp. B &amp; R. Regs. 390-6-7-16 (2008).</td>
</tr>
<tr>
<td>Guam</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

SOURCE: https://www.healthit.gov/sites/default/files/appa7-1.pdf
### Table A-7: State Medical Record Laws: Minimum Medical Record Retention Periods for Records Held by Medical Doctors and Hospitals

<table>
<thead>
<tr>
<th>State</th>
<th>Medical Doctors</th>
<th>Hospitals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pennsylvania</strong></td>
<td><strong>Adult patients</strong> 10 years following the date of the last medical service.</td>
<td>Adult patients 75 years following discharge.</td>
</tr>
<tr>
<td></td>
<td>Minor patients 7 years following the date of the last medical service or 1 year after the patient reaches age 21 (i.e. until patient turns 22), whichever is later.</td>
<td>Minor patients 7 years after the patient’s majority, or as long as adult records would be maintained. 28 Pa. Code § 115.23 (2008).</td>
</tr>
<tr>
<td><strong>Puerto Rico</strong></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>South Carolina</strong></td>
<td><strong>Adult patients</strong> 10 years from the date of last treatment.</td>
<td>Adult patients 10 years from the date of last treatment.</td>
</tr>
<tr>
<td></td>
<td>Minor patients 15 years from the date of last treatment.</td>
<td>Minor patients 15 years from the date of last treatment.</td>
</tr>
<tr>
<td><strong>South Dakota</strong></td>
<td>When records have become inactive or for which the whereabouts of the patient are unknown to the physician. S.D. Codified Laws § 39-4-38 (2008).</td>
<td>Adult patients 10 years from the actual visit date of service or resident care.</td>
</tr>
<tr>
<td></td>
<td>Minor patients 10 years from the actual visit date of service or resident care.</td>
<td>Minor patients 10 years from the actual visit date of service or resident care.</td>
</tr>
<tr>
<td></td>
<td>(continued)</td>
<td>(continued)</td>
</tr>
</tbody>
</table>

Source: https://www.healthit.gov/sites/default/files/appa7-1.pdf
TEXAS MEDICAL BOARD – “DISCIPLINARY ACTIONS APRIL, 2017”

QUALITY OF CARE

- Agusala, Madhava, M.D., Lic. No. J1178, Odessa
  On March 3, 2017, the Board and Madhava Agusala, M.D., entered into Mediated Agreed Order requiring him to have his practice monitored by another physician for eight consecutive monitoring cycles; and within one year complete at least 36 hours of CME, divided as follows: 12 hours in medical record-keeping, 12 hours in vascular interventions and complications, and 12 hours in peripheral arterial disease. The Board found Dr. Agusala did not adequately document physical examinations, assessments, and indications for peripheral interventions on a patient, failed to consider another diagnosis other than claudication on one patient and interpreted and relied on insufficiently documented ultrasound and peripheral angiogram reports on a patient. This order resolves a formal complaint filed at the State Office of Administrative Hearings.

Source: http://www.tmb.state.tx.us/id/B35F98D0-7F66-6F8B-8D5D-6A1520FF9C3F

TEXAS MEDICAL BOARD – DISCIPLINARY ACTIONS, SEPTEMBER, 2016

Ince, Christopher Werner, M.D., Lic. No. N4491, Willow Park
On June 10, 2016, the Board and Christopher Werner Ince, M.D., entered into an Agreed Order requiring Dr. Ince to within one year complete at least 16 hours of CME, divided as follows: eight hours in risk management and eight hours in assessing the risk of opioid dependence. The Board found Dr. Ince failed to adequately document a patient’s history and potential for substance abuse, failed to adequately document the patient’s past and current treatments for pain, and failed to adequately obtain prior medical records and consult with the patient’s other treating physicians which would have disclosed the patient’s history of opioid substance abuse.
“MEDICAL RECORD DOCUMENTATION FOR PATIENT SAFETY AND PHYSICIAN DEFENSIBILITY, A HANDBOOK FOR PHYSICIANS AND MEDICAL OFFICE STAFF”, JANUARY, 2008

“Nothing is more devastating to an innocent physician’s defense against the allegations of medical malpractice than an inaccurate, illegible or skimpy record, except for a record which has been changed after the fact, and therefore inevitably compromises the otherwise defensible case.”

Brad Cohn, MD, Pediatrician
Chairman, MIEC Board of Governors
Oakland, California

AUTHORS: David Karp, MA, BA; Judith M. Huerta, BS, MA; Claudia A. Dobbs, MA, BA; Dorothy L. Dukes, BS; Kathy Kenady, BA.
THIRD-PARTY ADDITIONAL DOCUMENTATION REQUESTS

Upon request for a review, it is the billing provider’s responsibility to obtain supporting documentation as needed from a referring physician’s office (for example, physician order, notes to support medical necessity) or from an inpatient facility (for example, progress note). The Medicare Program Integrity Manual, Chapter 3, Section 3.2.3.3, “Third-Party Additional Documentation Request” states:

The treating physician, another clinician, provider, or supplier should submit the requested documentation. However, because the provider selected for review is the one whose payment is at risk, it is this provider who is ultimately responsible for submitting, within the established timelines, the documentation requested by the MAC, CERT, Recovery Auditor and ZPIC.

INSUFFICIENT DOCUMENTATION ERRORS

Reviewers determine that claims have insufficient documentation errors when the medical documentation submitted is inadequate to support payment for the services billed (that is, the reviewer could not conclude that some of the allowed services were actually provided, were provided at the level billed, or were medically necessary). Reviewers also place claims into this category when a specific documentation element that is required as a condition of payment is missing, such as a physician signature on an order, or a form that is required to be completed in its entirety.

Insufficient documentation errors identified by the CERT RC may include:

- Incomplete progress notes (for example, unsigned, undated, insufficient detail)
- Unauthenticated medical records (for example, no provider signature, no supervising signature, illegible signatures without a signature log or attestation to identify the signer, an electronic signature without the electronic record protocol or policy that documents the process for electronic signatures)
- No documentation of intent to order services and procedures (for example, incomplete or missing signed order or progress note describing intent for services to be provided)

Some of the more common procedures that have resulted in insufficient documentation errors, description of errors, and links to the requirements are summarized below.
DEPARTMENT OF HEALTH AND HUMAN SERVICES – OFFICE OF INSPECTOR GENERAL, 2013 – (WARNINGS)

Copy-Pasting. Copy-pasting, also known as cloning, allows users to select information from one source and replicate it in another location. When doctors, nurses, or other clinicians copy-paste information but fail to update it or ensure accuracy, inaccurate information may enter the patient’s medical record and inappropriate charges may be billed to patients and third-party health care payers. Furthermore, inappropriate copy-pasting could facilitate attempts to inflate claims and duplicate or create fraudulent claims.

Overdocumentation. Overdocumentation is the practice of inserting false or irrelevant documentation to create the appearance of support for billing higher level services. Some EHR technologies auto-populate fields when using templates built into the system. Other systems generate extensive documentation on the basis of a single click of a checkbox, which if not appropriately edited by the provider, may be inaccurate. Such features can produce information suggesting the practitioner preformed more comprehensive services than were actually rendered.
Medicare Contractor Downcodes Claims Because of Copy and Paste in EHRs

After years of warning about the risks of cloning and other electronic documentation shams, Medicare administrative contractors (MACs) are starting to hit providers in this area. At least one MAC has downcoded an academic medical center’s claim for evaluation and management (E/M) services — which means it refused to pay at the level of service billed — because it appears that physicians copied and pasted notes from previous patient encounters.

Meanwhile, a top auditor from the HHS Office of Inspector General said in March that Medicare reviewers will develop new techniques to ensure auditors can tell when providers change electronic health record (EHR) documentation.

The MAC’s downcoding of the academic medical center’s subsequent hospital visits reflects CMS escalating concern about cloning or copy/paste, which may undermine support for medical necessity and exaggerate the services billed. According to the MAC’s letter to the academic medical center, obtained by RAC, “documentation from prior visits was carried over, making it difficult to determine what was documented for each specific encounter. Copying information from prior visits and pasting it into the record for a current visit could carry forward information that is not accurate and not appropriate for the encounter.”

continued on p. 5

APPENDIX – FOR YOUR REVIEW

EXCERPTS FROM MEDICAL RECORDS REVIEW GUIDELINES
(CALIFORNIA DEPT. OF HEALTH)
## Medical Record Review Guidelines

**California Department of Health Services**  
**Medical Record Management Division**

**Purpose:** Medical Record Survey Guidelines provide standards, directives, instructions, rules, regulations, permits, or indicators for the medical record survey, and shall be used as a guide or template for assessing, evaluating, strengthening, and modifying decisions.

**Scoring:** Survey scores are based on a review standard of 10 records per individual provider. Documented evidence found in the hard copy (paper) medical records and/or electronic medical records is used for survey criteria determinations. Full Pass is 100%. Conditional Pass is 75-99.9%. No Pass is below 75%. The minimum passing score is 90%. A corrective action plan is required for all medical record review deficiencies. Not applicable (N/A) applies to our criteria that do not apply to the medical record being reviewed, and must be explained in the comment section. Medical records shall be randomly selected using methodology decided upon by the reviewer. Ten (10) medical records are reviewed for each provider, five (5) adult medical records and five (5) pediatric records. For sites with only adult, only children, or only pediatric patient populations, all ten records reviewed will be in only one preventive care service area. Sites where documentation of patient care by all PCPs on site occurs in an insensitive shared medical records shall be reviewed as a "shared" medical record system. Access calculated on shared medical records shall apply to each PCP sharing the records. Access calculated on closed medical records shall be reviewed for each PCP, twenty records for 4-6 PCPs, and thirty records for 7 or more PCPs. Survey criteria to be reviewed only by a N or physician's discrete "EHR INSIDE Review only".

**Scoring Example:** Score your total points of omission is not correct. Locate zero partial points for each omission. If 100 records are reviewed, score calculations shall be the same as for 100 records reviewed for a single provider. If 10 records are reviewed, divide total points given by 10 for the "adjusted" total points possible. If 100 records are reviewed, divide total points given by 100 for the "adjusted" total points possible. Multiply by 100 to calculate percentage rate. Reviewers have the option to require additional records to review, but must calculate scores accordingly. Reviewers are expected to determine the most appropriate method on each rule to assign points if information needed to complete the survey.

### Scoring Example

#### Step 1: Add points given in each section.

<table>
<thead>
<tr>
<th>Section</th>
<th>Points</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Name of patient in medical record is established for each family member.</td>
<td>27</td>
<td>Name of patient in medical record is established for each family member.</td>
</tr>
<tr>
<td>B. Member identification is on each page.</td>
<td>39</td>
<td>Member identification is on each page.</td>
</tr>
<tr>
<td>C. C. Personal and biographical information is documented.</td>
<td>18</td>
<td>Personal and biographical information is documented.</td>
</tr>
<tr>
<td>D. Emergency &quot;control&quot; is identified.</td>
<td>24</td>
<td>Emergency &quot;control&quot; is identified.</td>
</tr>
<tr>
<td>E. Medical records are consistently organized.</td>
<td>30</td>
<td>Medical records are consistently organized.</td>
</tr>
<tr>
<td>F. Chart continues are securely fastened.</td>
<td>25</td>
<td>Chart continues are securely fastened.</td>
</tr>
<tr>
<td>G. Patient's assigned primary care physician (PCP) is identified.</td>
<td>15</td>
<td>Patient's assigned primary care physician (PCP) is identified.</td>
</tr>
<tr>
<td>H. Primary language and linguistic services needs of non- or limited English proficient (LEP) or hearing-impaired persons are prominently noted.</td>
<td>8</td>
<td>Primary language and linguistic services needs of non- or limited English proficient (LEP) or hearing-impaired persons are prominently noted.</td>
</tr>
</tbody>
</table>

**Source:** http://www.dhcs.ca.gov/provgovpart/Documents/Medical%20Record%20Review%20Guidelines.pdf

#### Step 2: Add points given for all sections.

<table>
<thead>
<tr>
<th>Section</th>
<th>Points</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Name of patient in medical record is established for each family member.</td>
<td>27</td>
<td>Name of patient in medical record is established for each family member.</td>
</tr>
<tr>
<td>B. Member identification is on each page.</td>
<td>39</td>
<td>Member identification is on each page.</td>
</tr>
<tr>
<td>C. C. Personal and biographical information is documented.</td>
<td>18</td>
<td>Personal and biographical information is documented.</td>
</tr>
<tr>
<td>D. Emergency &quot;control&quot; is identified.</td>
<td>24</td>
<td>Emergency &quot;control&quot; is identified.</td>
</tr>
<tr>
<td>E. Medical records are consistently organized.</td>
<td>30</td>
<td>Medical records are consistently organized.</td>
</tr>
<tr>
<td>F. Chart continues are securely fastened.</td>
<td>25</td>
<td>Chart continues are securely fastened.</td>
</tr>
<tr>
<td>G. Patient's assigned primary care physician (PCP) is identified.</td>
<td>15</td>
<td>Patient's assigned primary care physician (PCP) is identified.</td>
</tr>
<tr>
<td>H. Primary language and linguistic services needs of non- or limited English proficient (LEP) or hearing-impaired persons are prominently noted.</td>
<td>8</td>
<td>Primary language and linguistic services needs of non- or limited English proficient (LEP) or hearing-impaired persons are prominently noted.</td>
</tr>
</tbody>
</table>

### Scoring Example

#### Step 3: Subtract the "N/A" points from 350 total points possible.

<table>
<thead>
<tr>
<th>Points</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>350</td>
<td>Total points possible.</td>
</tr>
<tr>
<td>350 - 20</td>
<td>&quot;N/A&quot; points.</td>
</tr>
<tr>
<td>330</td>
<td>&quot;Adjusted total points possible.</td>
</tr>
</tbody>
</table>

#### Step 4: Divide total points given by 350 or by the "adjusted" points, then multiply by 100 to calculate percentage rate.

<table>
<thead>
<tr>
<th>Points</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>350</td>
<td>Total points</td>
</tr>
<tr>
<td>201</td>
<td>Adjusted points</td>
</tr>
<tr>
<td>330</td>
<td>&quot;Adjusted total points possible.</td>
</tr>
<tr>
<td>201</td>
<td>Total points</td>
</tr>
<tr>
<td>330</td>
<td>&quot;Adjusted total points possible.</td>
</tr>
</tbody>
</table>

**Source:** http://www.dhcs.ca.gov/provgovpart/Documents/Medical%20Record%20Review%20Guidelines.pdf
### Practice Management Institute

**Webinar/Audio Conference**

**September 28, 2017**

---

#### Criteria: Documentation Reviewer Guidelines

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Allergies are prominently noted.</td>
<td>Allergies and adverse reactions are listed as a contained segment in the medical record. If multiple allergies or adverse reactions, &quot;No Known Allergies&quot; (NKA), &quot;No Known Drug Allergy&quot; (NODA), or &quot;O&quot; is documented.</td>
</tr>
</tbody>
</table>
| B. Fever if 
| C. Correct continuous medications are listed.                             | Documentation may be on a separate problem list page, or a clearly identified problem list in the progress notes. All chronic or substantial problems are considered ongoing as "will be reevaluated". |
|                                         | Note: Chronic conditions are current long-term, ongoing conditions with three or more clinic visits. |
| D. Signed informed consents are present, when appropriate.               | Adults, prior legal guardians of a minor or emancipated minors, may sign consent forms in the medical record. Signed consents are signed for operative and invasive procedures. Humans experiments require IRB Consent Forms. Signed authorizations are documented in the medical record for release of medical information. Nota: Patients under the age of 18 years are not required to have been evaluated in a visit setting, nor are patients under the age of 16 years on any medical documentation. |
| E. Advance Health Care Directive Information is offered. (Adults 18 years or older) | Medical records include documentation of whether patient has been offered an advance health care directive, prepared per the standards established by the California Health Care Directive Task Force. |
The table and equations provided are related to pediatric preventive care guidelines. The table outlines various criteria and scoring procedures for pediatric preventive care visits, while the equations demonstrate how scores are calculated.

### Table: Pediatric Preventive Reviewer Guidelines

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Initial Health Assessment (IHA)</td>
<td>The IHA must be completed on all patients within 127 days of the effective day of treatment in the plan, or documented within the past 7 months prior to member’s enrollment. The IHA is a comprehensive history and physical that includes an individual Health Education Behavioral Assessment (e.g., ‘‘Going Healthy’’ or other IHA approved tool) or age-appropriate milestones. The IHA must include some of the assessment criteria. If evidence of an IHA is not present in the medical record, the remuneration must be discontinued in accordance with the applicable PMP, Medicaid, Medicare, etc.).</td>
</tr>
<tr>
<td>B. Individual Health Education Behavioral Assessment (IHEBA).</td>
<td>New Members: Age-appropriate IHEBA is considered within 130 days of effective date of coverage or dates of initial health service. Existing Members: Age-appropriate IHEBA is conducted in accordance with the age-appropriate care visit date, but no later than the next scheduled health screening event. The IHEBA must be conducted at the age-at-risk: 0-3 years, 4-5 years, 6-19 years and 10 years and older. The IHEBA tool and instruction plan is reviewed at least annually with members who present for a scheduled visit (not documented date and ICP approval). Provider of health education and anticipatory guidance is documented in the health encounter visit, which includes providing appropriate educational materials and providing re-assessment and counseling. Problems, interventions and referrals are recorded in the progress notes or otherwise in the medical record.</td>
</tr>
<tr>
<td>C. Age-appropriate physical events according to most recent AAP schedule.</td>
<td>Pediatric health services are provided according to the AAP recommended schedule for the pediatric preventive health care.</td>
</tr>
<tr>
<td>D. Vision screening.</td>
<td>Age-appropriate visual screening occurs at each health maintenance visit, utilizing a standardized screening tool. Vision screening should be conducted at age at risk.</td>
</tr>
<tr>
<td>E. Hearing screening.</td>
<td>Age-appropriate hearing screening occurs at each health maintenance visit, utilizing a standardized screening tool. Age-appropriate hearing screening should be conducted at age at risk.</td>
</tr>
<tr>
<td>F. Nutrition assessment.</td>
<td>Following includes: 1. Anthropometric measurements. 2. Laboratory tests to correct for serious deviations. 3. Based on problematic conditions identified, nutritionist at risk. Children under 3 years of age are referred to the Wisconsin, Illinois, Children’s Nutrition Program for medical nutrition therapy or other in-depth nutritional assessment as appropriate.</td>
</tr>
</tbody>
</table>

### Scoring Procedure

Scoring is based on 10 medical records:

1. **Format**: Score 90 (10)
2. **Determination**: Score 70 (10)
3. **Continuity of Care**: Score 70 (10)
4. **Pediatric Preventive**: Score 50 (5)
5. **Adult Preventive**: Score 54 (5)
6. **OB/CaSP Preventive**: Score 50 (5)

**Total** (Points gained) = 590

### Medical Record Scores

- **Full Pass**: 100%
- **Conditional Pass**: 80-99%
- **Not Pass**: Below 80%

### Compliance Rate

- **CAP Required**
- **Other Follow-up**

Next Review Due:

---

(Rationale: The pediatric preventive services are provided in accordance with the American Academy of Pediatrics Guidelines. The table and equations are designed to ensure quality and completeness of pediatric preventive care visits.)
Questions?

• Thank you for your attendance!

• Get your questions answered on PMI's Discussion Forum:
  http://www.pmimd.com/pmiForums/rules.asp