

MEDICAL RECORDS RELEASE

Medical Protective Clinical Risk Management Department

NOVEMBER 2013

For questions, products, or services, please contact 800-4MEDPRO or visit <http://www.medpro.com/>. This document should not be construed as medical or legal advice. Since the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney if you have any questions related to your legal obligations or rights, application of state or federal laws, contract interpretation, or other legal questions that may potentially impact the applicability of the information provided in this document.

CONTENTS

INTRODUCTION 3

OBJECTIVES..... 3

AUTHORIZED CONSENT 4

Patients and Patient-Authorized Representatives 4

Legal, Judicial, and Military Entities 5

RECORDS RELEASE AUTHORIZATION FORM 6

RELEASE OF SENSITIVE INFORMATION 7

RELEASE OF CHILDREN’S MEDICAL RECORDS..... 7

DENIAL OF RECORD RELEASE..... 8

CHARGING FOR COPIES OF MEDICAL RECORDS 8

OTHER CONSIDERATIONS..... 8

CONCLUSION 9

RESOURCES 9

INTRODUCTION

Healthcare practices and organizations should have written policies and procedures for the release of medical records. These policies and procedures should comply with both state and federal laws. In most cases, patients must provide written authorization to permit the disclosure and use of their protected health information (PHI) for:

- Legal, marketing, sales, and research purposes;
- Life insurance requests;
- Psychotherapy note requests; and
- Requests from others not involved in the patient's care and treatment.

According to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), authorization to use or disclose PHI is not required for:

- Treatment purposes (e.g., referral to a specialist);
- Payment for health care;
- Healthcare operations (e.g., certain administrative, financial, legal, and quality improvement activities of a covered entity — i.e., a healthcare provider, a health plan, or a healthcare clearinghouse — that are necessary to run its business and to support the core functions of treatment and payment.); and
- Certain legal circumstances, public health activities, and judicial or administrative proceedings (e.g., reporting child abuse or neglect, communicable diseases, or gunshot or knife wounds).

However, healthcare professionals should be cognizant of their states' laws before they develop policies addressing the release of PHI. Some states may have privacy regulations that are more stringent than federal regulations for the release of PHI.

OBJECTIVES

The objectives of this guideline are to:

- Discuss who is authorized to consent to the release of medical records or PHI;
- Explain the minimum requirements for a HIPAA-compliant records release authorization form;
- Provide information related to the release of sensitive information and children's medical records; and
- Discuss other records release considerations, such as charging for copies of records, denying the release of records, and tracking and documenting the release of PHI.

AUTHORIZED CONSENT

Healthcare practices and organizations are required to implement and maintain written policies and procedures that guard against unauthorized or inadvertent use or disclosure of patients' PHI.

These policies and procedures should specify who is authorized to consent to the release of medical records. Further, practices and organizations should have written policies for patients that explain in plain language the authorization process and the necessary steps for releasing medical records.

Patients and Patient-Authorized Representatives

Patients or their authorized representatives must consent to the use or disclosure of their PHI for purposes other than treatment, payment, or the healthcare operations of the practice, except when a disclosure is required by law.

First and foremost, the practice's medical records release policies should address who may request and receive a copy of a patient's medical record. In addition to the patient, other individuals also may be legally authorized to request the release of PHI. Although state specific, a legally authorized representative is usually one of the following:

- A legal guardian;
- An individual who holds durable power of attorney for healthcare; or
- A birth or adoptive parent.

Another example of a legally authorized representative is the executor of an estate. When a patient is deceased, the executor of the estate takes precedence over other legally authorized representatives.

However, HIPAA § 164.510(b) also permits disclosure of PHI to a decedent's family members and others who were involved in the care — or payment for care — of the decedent prior to death, unless disclosure would be inconsistent with any prior expressed preference of the deceased individual.¹

Note specifically that, even if a patient dies, the practice must still protect the patient's PHI. HIPAA requires protection of a decedent's PHI for a period of 50 years from the date of death.² Disclosure of decedents' PHI also must comply with state laws.

Healthcare practices and organizations should have processes in place for staff to follow in the event that any questions arise about whether a person is the patient's legally

¹ HIPAA Privacy and Security Rule, 45 C.F.R. § 164.510 (amended as of August 14, 2002).

² HIPAA Privacy and Security Rule, 45 C.F.R. § 164.502 (amended as of August 14, 2002).

authorized representative. Staff should be trained to ask for verification of the identity and the authority of the individual making the request.

Legal, Judicial, and Military Entities

In certain circumstances, law enforcement agencies can compel the release of patient information. Practice staff should be aware of these circumstances and document them in the written policies for release of PHI.

Prior to the release of PHI to a law enforcement agency, review state and federal laws to ensure disclosure is appropriate. Unless a statute specifically compels disclosure, law enforcement officers have no right to review a patient's healthcare information.

HIPAA permits disclosure of PHI without the patient's consent if it is related to a legitimate law enforcement inquiry — for example, to assist law enforcement in identifying a suspect or victim, amid concerns about national security activities, and in relation to allegations of healthcare fraud. Practices, however, should ensure that release is also permissible under state law.

All permissible law enforcement inquiries should be in writing and specify the scope of information requested and purpose of the inquiry.

A request for release of medical information also may occur during the course of a judicial or administrative proceeding. HIPAA states that a covered entity may disclose PHI in the course of any judicial or administrative proceeding that is:

- In response to an order of a court or administrative tribunal (but only to the extent expressly authorized by such order); or
- In response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal, if (a) the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to notify the subject of the PHI about the request, or (b) the covered entity receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to secure a qualified protective order.³

The practice's medical records release policies also should note any state laws that stipulate or prohibit circumstances in which attorneys may subpoena the release of medical information without production of a signed authorization.

Additionally, HIPAA specifically precludes individuals serving in the military from barring release of their medical information to military authorities.

³ HIPAA Privacy and Security Rule, 45 C.F.R. § 164.512 (amended as of August 14, 2002).

RECORDS RELEASE AUTHORIZATION FORM

When a patient or his/her legally authorized representative requests the release of PHI, the requestor must complete and sign a HIPAA-compliant authorization form. At minimum, the authorization form should include:

- The patient's full name, birthdate, social security number, and phone number.
- The name or other specific identification of the person(s) authorized to make the requested use or disclosure of the patient's PHI.
- The name or other specific identification of the person(s) who may use the PHI or to whom the covered entity may make the requested disclosure.
- A description of each purpose of the requested use or disclosure of PHI. The statement, "at the request of the individual," may be used when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.
- Specific PHI that is being authorized for release (e.g., the entire medical record, X-rays, reports, ECG results, or lab results).
- Specific consent to release information related to sexually transmitted diseases, HIV/AIDS status, drug/alcohol abuse, mental illness, and/or psychiatric treatment. (**Note:** Psychotherapy notes require a separate authorization. See page 7 for more information.)
- An expiration date or an expiration event that relates to the individual or to the purpose of the use or disclosure.
- A statement regarding the individual's right to revoke the authorization and the steps that must be taken to do so.
- A statement that the covered entity may not condition treatment on the provision of an authorization, except for certain permitted research purposes.
- A statement that the information may be subject to re-disclosure and may no longer be protected by federal or state privacy laws.
- Signature of the patient, the patient's authorized legal representative, or an officer of the court who has authority to compel the release of PHI.

Once the written authorization is obtained, it should be documented in the patient's medical record. The practice should also provide the patient with a copy of the written authorization.

Further, the practice should have a written policy clarifying oral requests for release of medical records. Most state laws mandate that a valid authorization be in writing.

RELEASE OF SENSITIVE INFORMATION

As part of medical records release policies and procedures, practices and organizations should implement mechanisms designed to prevent the release of sensitive information, such as PHI related to sexually transmitted diseases, HIV/AIDS status, or drug/alcohol abuse.

Additionally, mechanisms should be in place to prevent release of psychotherapy notes, if applicable. The term “psychotherapy notes” refers only to the private notes written by a healthcare provider who is a mental health professional documenting or analyzing a conversation during an individual, group, or family counseling session.

HIPAA requires that these notes be kept separate from the rest of the individual’s medical record. In general, you must obtain a patient’s authorization to use or disclose psychotherapy notes.⁴

RELEASE OF CHILDREN’S MEDICAL RECORDS

Practices’ and organizations’ medical records release policies should include written guidance on the release of records for minors and disabled individuals who require guardians.

Generally, the child’s legal guardian or natural/adoptive parent (even if divorced, separated, or never married) can obtain copies of most records by signing an authorization — unless a court order forbids access to the records by any of these parties.

In addition, these parties cannot access copies of the child’s records related to care for which the minor has exercised his or her right to consent (determined by state law) if the minor has not agreed to allow disclosure to the parents.

Unless a stepparent adopted a child or has been legally appointed as the child’s guardian, the stepparent has no legal right of access to the records. The child’s parent can sign an authorization form allowing the stepparent access to the records. However, prior to implementing such a policy, consult with your legal counsel to ensure it complies with your state laws.

If a minor is emancipated, married, or authorized to consent to healthcare without parental consent according to federal or state law, only the minor can authorize release of healthcare information pertaining to his/her care.

⁴ HIPAA Privacy and Security Rule, 45 C.F.R. § 164.508 (2002).

DENIAL OF RECORD RELEASE

In addition to stating criteria for the release of PHI, medical records release policies should stipulate the circumstances in which access to medical records might be denied. Depending on the situation, grounds for denial may be unreviewable or reviewable. For more information, see the Code of Federal Regulations, Title 45, § 164.524(a) (2), (3) at <http://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR>.

All denials must be timely and provided to the patient in writing, with a plain language description of the basis for denial. Additionally, written denials must contain statements of the individual's rights to have the decision reviewed and how to request such a review. The notice must also inform the individual of how to file a complaint with the practice or the Secretary of the U.S. Department of Health and Human Services.

CHARGING FOR COPIES OF MEDICAL RECORDS

Medical records release policies should clearly state whether charges will be levied for medical record copies. However, the policy should acknowledge that it is unethical and, in some states, prohibited to refuse to provide copies of records because a patient's account shows an outstanding balance or the patient refuses to pay for the records at the time of receipt.

HIPAA and most state laws limit the amount that can be charged for duplication and searching services. HIPAA prohibits charging patients for handling fees, chart-pulling fees, or per-page fees in excess of the direct cost of materials. According to HIPAA, individuals must agree to these charges in advance.

Medical Protective does not recommend that a fee be charged in cases of financial hardship.

OTHER CONSIDERATIONS

Other considerations also should be included in practices' and organizations' policies for release of PHI. For example, these policies should:

- Acknowledge the practitioner's obligation to maintain the original medical records, laboratory slides, etc., but to promptly provide copies in response to valid requests. No patient is entitled to original records, X-rays, slides, etc.
- Acknowledge that unless the patient or authorized requesting party states otherwise, records of other providers that are included in the patient's chart are considered part of the chart and should be included in the material copied and provided.
- Clarify what information Labor and Industries may obtain if a patient has filed a worker's compensation claim.

The practice also should determine how access to medical records will be monitored and how to implement an effective system for tracking and documenting uses and disclosures of PHI to comply with accounting of disclosure requests. If an electronic health record system is in place, practice staff should run regular reports to review compliance with medical records release policies.

CONCLUSION

Protecting patients' health information is imperative. To carefully guard against the unauthorized release of PHI, healthcare practices and organizations should have written policies and procedures for the release of medical records.

These policies and procedures should comply with both state and federal laws, and they should clearly outline who is authorized to consent to the release of PHI, the process for authorizing release, and any special considerations related to record release.

RESOURCES

- American Health Information Management Association: Privacy and Security — <http://www.ahima.org/topics/psc>
- Georgetown University: Center on Medical Record Rights and Privacy — <http://hpi.georgetown.edu/privacy/records.html>
- Office for Civil Rights, U.S. Department of Health and Human Services: Health Information Privacy — <http://www.hhs.gov/ocr/privacy/index.html>
- Office for Civil Rights, U.S. Department of Health and Human Services: HIPAA Frequently Asked Questions — <http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html>
- The Office of the National Coordinator for Health Information Technology: Guide to Privacy and Security of Health Information — <http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>