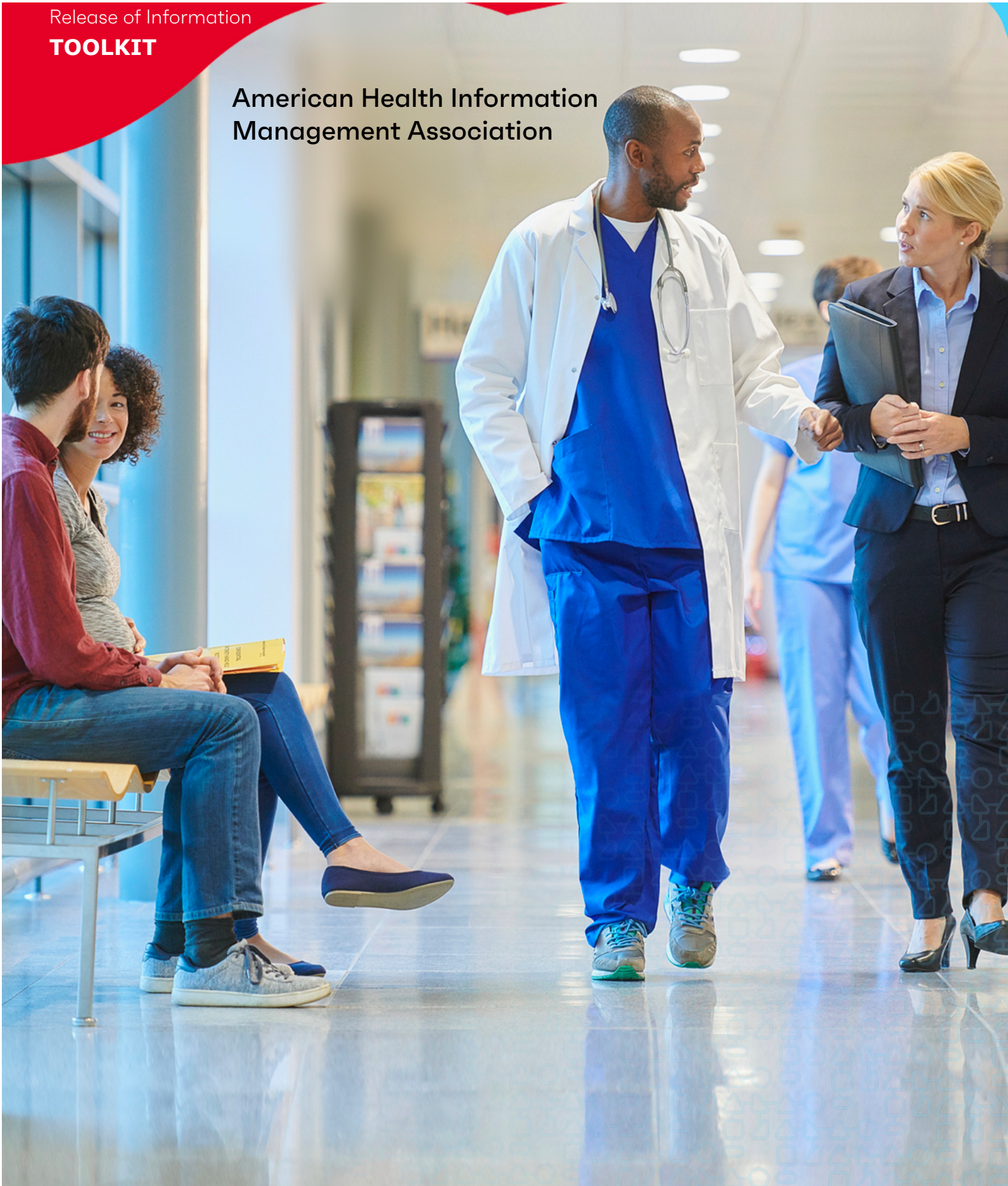
Release of Information

TOOLKIT

American Health Information Management Association



Release of Information
TOOLKIT

ISBN: 978-1-58426-057-8
AHIMA Product No.: ONB188013

AHIMA Staff:

Jessica Block, MA, Assistant Editor
Jason Malley, Director, Creative Content Development
Anne Zender, Editorial Director

For more information about AHIMA Press publications, including updates, visit
ahima.org/publications/updates.aspx

American Health Information Management Association 233 N. Michigan Ave., 21st Fl.
Chicago, Illinois 60601

AHIMA.org

MX8119

Table of Contents

Click each listing to navigate to that section

Authors

Ruth Betz, RHIT LeAnne Bouma, RHIA
Melanie Brodnik, PhD, RHIA
Sheila Burgess, RN, RHIA, CDIP, HIT PRO-CP
Jennifer Corteville, RHIT
Elizabeth Delahoussaye, RHIA, CHPS
Rose Dunn, MBA, CPA, RHIA, CHPS, FAHIMA, FACHE
Ginna Evans, MBA, RHIA, FAHIMA
Angie Fergen, RHIA, CHPS
Joe D. Gillespie, MHS, RHIA, CHPS
Elisa Gorton, RHIA, CHPS, MAHSM, CHC
Shelly Kirkland, MHIM, RHIA, FAHIMA
Evelyn May, RHIT, CPEHR, CPHIT
Amber Mayberry-DiMaria, RHIA
Kimberly Moore, RHIA
Brenda Olson, ME, RHIA, CHP
Mary Poulson, MA, RHIT, CHC, CHPC
Jill Roberson, MBA, RHIA, CCS, CHPS
Angela Dinh Rose, MHA, RHIA, CHPS
Mariela Twiggs, MS, RHIA, CHP, FAHIMA
Christina Wallner, RHIA
Traci Waugh, RHIA, CHPS

2008 ROI Project Authors

Sten Anderson
Nancy Davis, MS, RHIA
Elisa R. Gorton, MAHSM, RHIA
Cheryl Gregg Fahrenholz, RHIA, CCS-P
Karen B. Griffin
Diane Holmgren, MBA, RHIA
Marilyn M. Houston, RHIA
James R. Lantis, Jr., MHA, RHIA
Debra Mikels, OTR/L
Karen Proffitt, RHIA, CHP
Bonnie Purdy, RHIA
Laurie A. Rinehart-Thompson, JD, RHIA, CHP
Laura J. Rizzo, MHA, RHIA

Acknowledgments

Janet Asafo, MSA, RHIA
Michelle Blanchard, RHIA
Rita Bowen, MA, RHIA, CHPS
Becky Buegel, RHIA, CHP, CHC
Ben Burton, JD, MBA, RHIA, CHP, CHC
Jane DeSpiegelaere-Wegner, MBA, RHIA, CCS, FAHIMA
Julie Pursley, RHIT
Tangie Dorsey, RHIA
Kim Turtle Dudgeon, RHIT, HIT Pro-IS/TS, CMT
Sheila Hargens, MSHI, RHIA, CMT
Andrea Heikkinen, RHIA
Judi Hofman, CHPS, CAP, CHP, CHSS
Sandra L. Joe, MJ, RHIA
Susan Lucci, RHIT, CHPS, CMT, AHDI-F
Karen Marsala, RHIT
Jennifer McCollum, RHIA, CCS
Kelly McLendon, RHIA, CHPS
Godwin Odia, PhD, NHA, RHIA
Yvonne Pennell, MA, RHIA
Nancy Prade, MBA, RHIA, CHPS
Theresa Rihanek, MHA, RHIA, CCS
Margaret Schmidt, RHIA CHPS
Carol Schuster, MSM, RHIA, CHPS
Melanie Severson, RN
Christine Steigerwald, RHIA
Diana Warner, MS, RHIA, CHPS, FAHIMA
Lou Ann Wiedemann, MS, RHIA, CDIP, FAHIMA, CPERH
LaVonne Wieland, RHIA, CHP
Janet Williams, MS, RHIA
Gail Woytek, RHIA

2021 Authors

Lisa Hunter, MS, RHIT, CHPS
Lori Black, MHA, RHIA, CHPS, CHDA, CCS
Elisa Gorton, MAHSM, RHIA, CHPS, CHC
Barbara Ryznar, MSHI, RPH, RHIA, CHDA, CHPI, CPHIMS

2021 Reviewers

Laurie Peters, RHIA, CHPS
Kenneth Clyburn, RHIA, CHPS
Robyn Stambaugh, MS, RHIA
Lauren Riplinger, JD

Introduction

The disclosure, accessibility, and availability of protected health information (PHI) continues to be at the forefront of healthcare. To ensure that PHI is disclosed in accordance with all state and federal laws, health information (HI) professionals and their respective healthcare organizations must be diligent in their efforts to ensure that all requests for PHI adhere to all regulatory requirements. Healthcare organizations should have current policies and procedures for release of information (ROI) and review them annually and as needed to reflect any changes to state and federal laws. Policies and procedures should reflect and support the organization's commitment to the compliant and timely disclosure of protected health information (PHI). Knowledgeable, experienced, and well-trained staff ensure disclosures are compliant and requests are processed efficiently. To assist healthcare organizations and HI professionals in navigating this rapidly changing ROI environment, this toolkit has been revised to incorporate various types of disclosures of PHI and to reflect today's healthcare landscape.

The purpose of this toolkit is to provide general guidance and direction for the development of an effective ROI process across any healthcare setting. Its intention is to provide a framework and reference guide to ensure disclosures of PHI are compliant with state and federal regulations. It encourages the development of appropriate policies and procedures to facilitate a seamless ROI business workflow that includes timely response and turnaround times for all types of requests and policies. Those policies should include examples of common types of disclosures and how they would be triaged, tracked, and monitored for compliance.

This toolkit provides ROI best practices to guide processing requests for PHI; development of fee structures for copies of PHI; and regulatory considerations related to minors, as well as sensitive information such as mental health, substance use disorders, and certain communicable diseases. In addition, this toolkit addresses the significance of understanding the impact of the electronic health record (EHR) and how electronic health information may be shared. Also noted is the importance of the creation or updating of policies when there is an installation of a new EHR, as well as any changes that impact the patient portal. Examples are provided that address the revision of policies and procedures, including how to incorporate electronic signatures, how to manage disclosures within the patient portal, and security surrounding access; as well as how to produce records from various systems in a machine-readable format, i.e. the patient output record.

The Current and Future Landscape of ROI

The current landscape of ROI is evolving with an emphasis on patient right of access, state, and federal legislative changes such as the 21st Century Cures Act, the Promoting Interoperability Program (formally known as Meaningful Use), and information blocking. The HI professional's role in the function of ROI is changing with managing how ROI requests are received and how PHI is disclosed. The advancement in technology such as patient portals and health information exchanges has contributed to this change. In addition, HI staff who perform in this role will be seen more as subject matter experts and will need to help educate patients and other requesters on how to request and receive PHI.

Both state and federal rules and regulations that govern the disclosure of PHI continue to change and have a direct impact on ROI practices and healthcare. HI professionals must stay ahead of the rapid changes to effectively manage the daily operations of ROI—their expertise is essential given the evolving nature of ROI practices.

The future of ROI is anticipated to change even more. With the implementation of the Cures Act Final Rule as a requirement in the 21st Century Cures Act, providing access to electronic health information (EHI) holds healthcare organizations to even greater responsibility and accountability to ensure EHI is not restricted. [1] On January 21, 2021, the U.S. Department of Health and Human Services (HHS) published a notice of proposed rulemaking (NPRM) that will modify the HIPAA Privacy Rule and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The proposed changes will have a direct impact on ROI and other areas of healthcare.

Additional Resources

HHS: Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement

ROI Education

The covered entity is responsible for training all workforce members on policies and procedures with respect to disclosure of PHI. [2] The HIPAA Privacy Rule is flexible and scalable when it comes to HIPAA training as there is not a standardized program to follow, which can be challenging for some organizations. Training should be tailored and relevant to the job role. HI professionals who work closely with the release of information function should have focused and continuous education on practices involving ROI.

Recommended Practices

- Focused training on different areas of ROI practices on a continuous basis (monthly, quarterly, etc.). Keeping training consistent, fresh, and updated can help with efficient training.
- Creation of annual assessments for staff to apply HIPAA, ROI practices and 21st Century Cures Act requirements as it relates to information blocking.
- Invite guest speakers to in-service or team meetings, such as the privacy or compliance officer to discuss relevant topics.
- Perform routine audits and use findings for educational opportunities for staff.

[1] 45 CFR 171.102-EHI definition
[2] eCFR :: 45 CFR 164.530 -- Administrative requirements.

Defining Release of Information

What Is ROI?

Release of information is defined as the process of disclosing protected health information from the health record to another party.[3] All disclosures of PHI by the covered entity must be in accordance with federal and state laws or upon the request of an individual, authorized representative, or authorized entity.

In regard to permitted uses and disclosures of PHI, the federal Privacy and Security Rule applies to covered entities, business associates, and their subcontractors. Covered entities include healthcare providers, health plans, and healthcare clearinghouses.[4]

Federal regulations define PHI as individually identifiable health information that is transmitted by electronic media, maintained in electronic form, or transmitted in any other form or medium.[5] PHI does not include individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA), or employment records held by a covered entity in its role as an employer. Please see the following examples:

FERPA versus HIPAA:

- A school nurse providing services to a student: the health records will be covered by FERPA, not HIPAA.
- A physician employed by the school who bills a health plan electronically for the care provided is covered by HIPAA, not FERPA.

Employment records:

- An employee receives healthcare services by an employee health nurse is not covered by HIPAA.

Additional Resources

HHS: “Are there circumstances in which the HIPAA Privacy Rule might apply to an elementary or secondary school?"

HHS: Employers and Health Information in the Workplace

[3] Brodnik, M. S., Rinehart-Thompson, L. A., & Reynolds, R. B. (2017). Fundamentals of law for health informatics and information management (3rd ed.). Chicago, IL: American Health Information Management Association
[4] Covered Entities and Business Associates | HHS.gov
[5] eCFR :: 45 CFR 160.103 -- Definitions.

Use Versus Disclosure

The terms "use and disclosure" came into common use with the creation of the HIPAA Privacy Rule and are foundational building blocks to understanding how to apply the rule. The HIPAA Privacy Rule breaks this down into uses and disclosures:

Term	Definition	Examples
Use	"The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information" 45 CFR § 160.103	- Patient safety activities - Quality activities - Compliance activities
Disclosure	"The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information" 45 CFR § 160.103	- Disclosure to outside provider for purpose of treatment - Legal request for PHI - Electronic proxy access to PHI

Individual state laws must be reviewed for additional definitions for use and disclosure as well as any privacy provisions that may differ from the HIPAA Privacy Rule.

Additional Resources

HHS: Understanding Some of HIPAA's Permitted Uses and Disclosures

Minimum Necessary

"Minimum necessary" is a concept that was introduced by the Federal Privacy Act of 1974 and was further defined by the HIPAA privacy regulations in 2003.[6] However, for the purposes of this introductory section, regardless of whether information is used within or disclosed to an outside covered entity, or to non-covered entities, a covered entity must not share more information than is minimally necessary to perform the intended task or respond to an authorized request. Continuous training is necessary to ensure that only the minimum information is released.

Additional Resources

HHS: Minimum Necessary Requirement

[6] 45 CFR 164.502(b), 164.514(d) -Minimum Necessary

Types of Requests

A covered entity may receive a variety of requests for PHI that include disclosing PHI for continuity of care, legal purposes, insurance claims, third party reviewers, or patient right of access to information. When a request is received, it is the covered entity's responsibility to determine if the request can be disclosed with or without an authorization. This can be broken down into two distinct categories: permitted and authorized uses and disclosures. In general, patient authorization is required for the use and disclosure of PHI, unless it meets an exception where authorization is not required.[7]

Permitted Uses and Disclosures

A covered entity is permitted, but not required, to use and disclose PHI without an individual's authorization under specific purposes or circumstances. Covered entities should rely on organizational policy and best judgments when making such disclosures.

Examples of uses and disclosures permitted without a patient authorization:

- To the individual and legal representative (generally, a person with authority under State law to make health care decisions for the individual
- Third-party requester that falls outside of the permitted uses and disclosures

Additional Resources

Code of Federal Regulations: Title 45, 164.508 - "Uses and disclosures for which an authorization is required"

AHIMA Body of Knowledge (BoK): Sample Authorization Form

Legal Requests and Related Documents

Legal documents may or may not accompany a request for PHI. HI professionals will need to carefully review any legal requests to verify the validity of the request and whether additional documents are needed. There are various types of legal documents for the disclosure of PHI, and they vary in time constraints, type of information requested, how it is requested, and the method of delivery, including how to properly execute and meet the requirements of a specific legal request. They can become confusing to manage and require a careful review and timely response. This section provides a breakdown of the different types of legal requests and documents that can be involved in a request for PHI.

Subpoenas and Court Orders

Courts may issue subpoenas to compel an individual or an organization's representative to appear before the court for sworn testimony and/or to provide specific information or evidence.

[7] Brodnik, M. S., Rinehart-Thompson, L. A., & Reynolds, R. B. (2017). Fundamentals of law for health informatics and information management (3rd ed.). Chicago, IL: American Health Information Management Association

A subpoena (which translates as "subject to sanction") is often issued for stored paper files or data (as from an electronic health record). The subpoena should be specific as to the type of documents requested. An "any and all" subpoena is not an acceptable delineation of the documentation requested. The subpoena should state medical records if it is the care and treatment documentation being requested; conversely, if the requestor is asking for access to metadata, the subpoena should so state. The latter type of request may cause undue burden on the organization and cause the organization to object to the subpoena and request, in its place, a court order.

HI professionals will most commonly encounter two different types of subpoenas:

- Subpoena duces tecum: Mandates a person to produce documentation specified in the subpoena. Their personal testimony in court is seldom necessary.
- Subpoena ad testificandum: Directs the person to appear and provide sworn testimony at a legal proceeding, such as a deposition or a trial.

Subpoenas contain distinguishing characteristics, including:

- The full name of a court in the document's title, or letterhead
- The word "Subpoena" in bold in the top third of the document
- The words "You are commanded to report" or a similar variation
    - Name of custodian or organization being subpoenaed
    - A specific date, time, and location for appearance, and/ or for the custodian to provide the requested materials
    - In some cases, the penalty for non-compliance will be included8

Subpoenas differ from court orders in that subpoenas may be issued by someone other than a judge, such as a court clerk or even an attorney involved in a case.[9] Court orders are typically written orders issued by a court, administrative tribunal, or state commission. More rarely, orders may be issued orally in court to an attorney who represents the healthcare entity. On occasion, there are subpoenas that are sent to a facility where the patient was never treated. In a case like this, it is necessary to inform the court that the patient was not at the facility.

[8] Digital Media Law Project. "Responding to Subpoenas." www.dmlp.org/legal-guide/responding-subpoenas

[9] Department of Health and Human Services. "Health Information Privacy: Court Orders and Subpoenas." hhs.gov/ocr/privacy/hipaa/understanding/consumers/courtorders.html

A subpoena for production of medical records by a covered entity is allowed under HIPAA, but the entity may only disclose the information specifically described in the subpoena. However, according to HHS, before complying with the subpoena, the covered entity must "receive evidence that reasonable efforts were made to:

- Notify the person who is the subject of the information about the request, so the person has a chance to object to the disclosure, or
- Seek a qualified protective order for the information from the court." [10]

If the entity receives an authorization with the subpoena, then the HIPAA requirement is met.

If an HI professional does appear in court, they must never interpret the medical records being presented to the court. The testimony provided will relate to how the organization maintains records, policies, and procedures around this, and if there are any circumstances in which the policies are not followed. Testimony should be limited to the specific questions asked, and no additional narrative should be added. Meeting with the organization attorney for preparation tips is recommended as a best practice for a court appearance.

Objections to Subpoenas

Objections to subpoenas can be filed by the individual or the attorney representing the individual who is the subject of the PHI. Formal objections to subpoenas are made in writing in the form of a motion to quash, which is a document filed with the court that asks the judge to nullify the subpoena for any number of reasons. There are many valid reasons why objections are made. A most common example is that the records requested are too broad and should be limited to a specific time or record requested. As mentioned previously, HI professionals should never produce records too soon in order to allow time for all parties to be notified that records are being subpoenaed. If an objection is received by the organization, it is recommended that a flag or notice be placed on the patient chart for ROI staff to see an objection has been made so records are not disclosed.

Federal Subpoenas

Rule 45 of the Federal Rules of Civil Procedure regulates the issuance of federal subpoenas, which should be handled in the same fashion as court orders. There is a significant amount of detail in Rule 45 that necessitates close inspection to ensure the subpoena was issued correctly and by the district court with appropriate jurisdiction. The rule also describes the manner in which these subpoenas must be served. There are even aspects of Rule 45 that protect the named person or "subject" of the subpoena. For example, if the subject is not a party to the lawsuit and must travel more than 100 miles from the subject's place of business, this may be considered grounds for the court to quash the subpoena.[11]

Grand Jury Subpoenas

When deemed necessary by a state, county, or city prosecutor, a grand jury of ordinary citizens (who are not screened for bias) is convened to see and hear witnesses give evidence to decide whether or not there is sufficient merit for a case to go to trial. These cases usually involve crimes above the level of misdemeanor. When federal laws are broken resulting in capital or "infamous" crimes, the US federal government will convene a grand jury to hear the evidence in all such cases.

Legal counsel should always be sought when receiving a grand jury subpoena.

---

[10] eCFR :: 45 CFR 164.512(e)(1)(v)- Qualified Protective Orders

[11] Cornell Law School. Federal Rules of Civil Procedure: Rule 45. Subpoena. Retrieved from https://www.law.cornell.edu/rules/frcp/rule_45

Court-Martials

These are courts convened to determine guilt of members of the military where there has been a breach of military discipline. The Uniform Code of Military Justice governs how these proceedings are conducted. The military has rules for evidence that are generally recognized in criminal cases in US district courts. These rules also give the accused some authority in how evidence is used in a court-martial. [12]

Search Warrants

The Fourth Amendment to the US Constitution restricts government searches and seizures but does allow a "search warrant" to be issued when there is probable cause as substantiated with a court. These are used in criminal investigations, not in civil lawsuits. This method of discovery is not commonly used in healthcare settings to obtain PHI on a specific person. However, search warrants are commonly used when government agencies are investigating healthcare fraud, especially when there is concern for the preservation of specific documentation.

If presented with a search warrant by a law enforcement officer, an HI professional should not resist or interfere with the officer's search. Legal counsel and senior leadership should immediately be notified. It is appropriate to record the name and badge number of the officer(s) present as well as names and contact information of any witnesses present. At the conclusion of the search, it is reasonable to request an inventory of what was seized, but the HI professional should not sign any statement that the inventory is accurate or complete.

Affidavits

An affidavit is a voluntarily written document containing facts related to an issue at hand by an individual or "affiant." It is made under an oath or affirmation administered by someone authorized to do so under law, such a court clerk or a notary.[13]

There are two types of affidavits:

1. When the production of PHI has been ordered by a court but the HI professional is not expected to personally provide the PHI in court, the HI professional may be asked to submit an affidavit with the PHI stating the authenticity of the information and validating that the PHI was collected in the regular course of business, such as delivery of care to the patient.
2. When a covered entity is presented with a subpoena to produce records, it is required under HIPAA that evidence be provided demonstrating that the person who is the subject of the information was given a chance to object to the disclosure or to seek a protective order with the court. This evidence may be provided in the form of an affidavit.

Depositions

Depositions are formal interviews with attorneys and a court reporter present to gather information for use in a lawsuit. They are a form of pre-trial discovery and are initiated by subpoena from the attorney who will conduct the deposition. The subpoena may be issued to a party in the lawsuit, or to a non-party to the suit that has information of interest to the attorney.

HI professionals may be subpoenaed to provide PHI of interest to the plaintiff 's attorney. If the information requested was gathered from an EHR system, some typical questions that the HI professional can expect are:

- How did the HI professional arrive at a set of provided documents?
- What were the parameters of the search?
- From what areas of the system were the documents produced?[14]

---

[12] The Uniform Code of Military Justice (UCMJ) | Military.com

[13] The Free Dictionary. "Affidavit." http://legal-dictionary.thefreedictionary.com/affidavit

[14] Dimick, Chris. "Preparing for a Deposition on an EHR: New Types of Information Lead to New Types of Questions." Journal of AHIMA 82, no.3 (March 2011): 44–45.

- Note: In long-term care facilities, it is common for the director of nursing to be the one making such presentations at depositions.

Recommended Practices:

- Never ignore a legal document (such as subpoena or court order), but it is appropriate to ask an attorney for guidance in reviewing the document for validity. This must be done within the time frame identified in the document. A standard practice is to contact the attorney who initiated the document to ascertain if the intent is for someone to present the documentation in court or for it to be mailed to the attorney's office. Ask the attorney if the format of documentation would be satisfactory to comply with the legal document (for example, hard copy documents, documents scanned onto compact disks, etc.).
- Be clear on the extent of the documentation that is covered by the request. Identify all locations and systems that contain the requested PHI.
- If the organization does not possess any or all of the documentation being ordered, it is imperative to notify the attorney involved in the initiation of the request. The best course is to call the attorney, then follow up with a letter.
- Develop a protocol for maintaining the integrity of the documentation, including such steps as:
  - Taking whatever steps are necessary to immediately preserve or protect the requested documentation. This may mean sequestering the paper or electronic files to the extent possible.
  - Obtain any requested records maintained in paper form if the organization uses an off-site record storage vendor.
  - If any requested documents are missing, document this fact and immediately notify legal counsel for guidance on how to proceed. Require any staff to justify their need to review the documentation or data that has been sequestered. Typically, such access is only allowed when necessary for direct patient care or to protect others from harm.
  - To the extent necessary, only allow access in the presence of the information's custodian.

Additional Resources

Cornell Law School Legal Information Institute: Federal Rules of Civil Procedure, Rule 45 - Subpoena

HIPAA Patient Rights for ROI

Patient Rights of Access

Section 164.524 of the HIPAA Privacy Rule states individuals have the right of access to inspect and obtain a copy of their own PHI that is contained in a designated record set (DRS).[15] The DRS will be covered in more detail in the following sections of this toolkit. HI professionals are at the front lines when patients and their personal representatives request medical records and must understand the patient right of access in order comply with HIPAA and not violate the rights of individuals. Patients' rights of access and how PHI is used and disclosed is covered in organizations' Notice of Privacy Practices.

Patient rights of access include:

- Timely access within 30 days of receipt; if unable to do so, a one-time extension of 30 days is permitted, not to exceed 60 days. Notification of extension must be made in writing to the individual.
- Reasonable cost-based fees for copies
- Right to request in specific form or format (paper or electronic)
- Right to direct PHI to another person
- Right to receive written denial and right to review of denial

[15] (45 CFR 164.524- Right of access)

Additional Resources

- Code of Federal Regulations: Title 45, 164.524 - "Access of individuals to protected health information"
- AHIMA BoK: Explanation for Use of AHIMA Patient Request for Health Information Model Form

Accounting of Disclosures (AoD)

The HIPAA Privacy Rule states that an individual has the right to receive an accounting of disclosures of protected health information made by a covered entity, and that the covered entity must provide the individual with a written accounting.[16] Additionally, the covered entity must also provide an accounting on behalf of their business associates (BA), or the BA must respond to requests that are made directly to them.

The rule also states that the covered entity must provide the first accounting to an individual in any 12-month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. It is important for an HI professional to understand the required timeframe for responding to an AoD request, content of the accounting, and the documentation requirements.[17]

Right to Restrict Disclosure

Individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment, or healthcare operations; disclosure to persons involved in the individual's healthcare or payment for healthcare; or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions. A covered entity that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[18]

When a patient pays for services in full at time of services, and the disclosure is for payment or health care operations and not otherwise required by law, they have a right to restrict disclosures to their health plan and the provider must accept the request.[19] There are no timeframe requirements to respond to a restriction request.

Restriction requests can also be directed to health information exchanges (HIE). An HIE allows clinical staff and other healthcare providers appropriate and secure access to PHI electronically.[20] Patient consent laws for HIEs vary by state where patients may be required to opt-in or opt-out of sharing their PHI electronically.

Additional Resources

[16] 45 CFR 164.528-Accounting of Disclosure
[17] Ibid
[18] 45 CFR 164.522
[19] Under HIPAA, may an individual request that a covered entity restrict how it uses or discloses that individual's protected health information (PHI)? | HHS.gov
[20] What is HIE? | HealthIT.gov

- Code of Federal Regulations: Title 45, 164.522 - "Rights to request privacy protection for protected health information"
- ONC: What Is HIE?
- ONC: Meaningful Consent Overview
- AHIMA BoK: Managing a Patient's Right to Request Restrictions of Disclosures to Health Plans

Significance of the Legal Health Record and Designated Record Set

The HIPAA Privacy Rule requires that organizations identify their designated record set (DRS), which is defined by HHS as "a group of records maintained by or for a covered entity.[21]

Simply stated, the DRS includes those documents or records that were used or may be used to make decisions about the treatment of the patient and/or payment for the patient's services. The DRS serves as a basis for the rights defined in HIPAA for patient access, copies, amendment, restriction, and more.

The legal health record (LHR) is an AHIMA-defined term that describes a subset of the DRS that is the healthcare organizations business record. [22] It is important to note that in response to a patient access request CEs must provide the DRS in addition to the LHR.

In a paper environment, AHIMA describes the LHR as the traditional health record. In an electronic or hybrid environment, the components of the LHR may reside in paper form, in an electronic application (electronic health record), and in scanned formats. Similar to traditional paper records, the LHR does not affect the discoverability of other information such as policies, contracts, and electronically stored information held by the organization.

The custodian of the LHR is typically the health information professional; however, because the LHR may reside in a variety of media—some of which may be electronic—a strong collaborative relationship must exist between HIM and information technology. HI professionals oversee the operational functions related to collecting, protecting, and archiving the legal health record, while information technology staff manages the technical infrastructure of the electronic health record.

HI professionals, in collaboration with information technology and legal counsel or risk management, should list the specific data elements or documents within the designated record set, as well as those that comprise its legal health record. When developing this list, it may be beneficial to define the media (e.g., paper, electronic, microfilm, scanned, etc.) in which the document is stored.

Records from other facilities (commonly known as "outside records") is an example of records can be considered both LHR and DRS, depending on the covered entity. However, since records from other facilities may aid or have been considered in the treatment of the patient, they qualify as being part of the covered entity's DRS and may be considered a component of the LHR. In collaboration with legal counsel, covered entities should clearly define which documents created during the encounter are to be considered part of the LHR, and whether documents from entities outside of the covered entity are part of the LHR. Again, the LHR is not the complete record regarding the treatment of an individual, however it is the business record of that treatment. The DRS will most likely encompass more than the LHR and with the new regulations regarding information blocking, discussed later in this toolkit, organizations can run risk of possible penalties in the future if not sharing information. Consideration should be given if information is received from a designated substance abuse Part 2 facility, as there would be more stringent regulations on the disclosure of substance abuse records.

[21] DRS defined
[22] Legal Process and Electronic Health Records (ahima.org)

For covered entities that maintain patient care documents in an electronic format that allows for variable displays (e.g., episodic, longitudinal, portrait, landscape, by provider, etc.), the definition of the LHR should define the display format that will be released. Monitoring release of information activities is essential in this area to ensure that staff are following the policies and procedures established by the covered entity. This is particularly important because often in legal proceedings, more than one attorney may request copies of medical records at different times, and both attorneys should receive copies of medical records that are in identical display formats.

Organizations are encouraged to clearly define their LHR and its relationship to the DRS. Since the LHR is typically a subset of the DRS, disclosure about the treatment provided should be made from the LHR. For example, a disclosure to an insurance company. However, there may be times when a disclosure will result in producing a document from the DRS—for example, a copy of the patient's bill.

Recommended Practices

Develop a matrix that clearly distinguishes the following:

- Whether each document used in the treatment of a patient and/or payment for patient's services qualifies as a designated record set document and/or a legal health record document
- The storage media of the document
- The source system in which it can be located
- The orientation or format display that should be released upon receipt of a valid authorization

Checklist for maintaining your matrix:

- Review the matrix annually for any updates and/or new document types.
- Involve information technology, risk management, legal counsel, patient financial services, compliance, and HIM in the process of defining the DRS or the LHR.
- Ensure that legacy EHR's are available for disclosure when needed.

Additional Resources

AHIMA BoK: Fundamentals of the Legal Health Record and Designated Record Set

Successful Management Practices

It is critical for a healthcare organization to manage its ROI processes in a competent and compliant manner. Historically, the options for managing ROI process were limited to maintaining the ROI

function in-house or outsourcing it altogether. Today, many new approaches to ROI workflow have emerged that can include maintaining the process completely in-house, to outsourcing pieces of the process or even full outsourcing.

Whether the ROI process is handled in-house or outsourced, HI professionals will need to manage and oversee the ROI process. Depending on their size, organizations can see high volumes of requests daily. The tracking of ROI requests from receipt to completion is critical to ensure timely processing and compliance with HIPAA. The ROI specialist will need to understand the type of request and authority of the requestor. In addition, HI professionals will need to manage turnaround times, backlogs, accuracy, and security of the disclosure. Again, even if ROI is outsourced to a third party, it is the organization's (and HI professional's) responsibility to direct that third party and provide the parameters by which the work will be done.[23]

If a request cannot be fulfilled, correspondence to the requestor should be written in plain language that is clearly understandable to the requestor. See Appendixes B and C, respectively, for a sample Certification Form and Return Request Letter.

Additional Resources

- AHIMA BoK: "Management Practices for Release of Information" Practice Brief, 2012 update
- AHIMA BoK: Outsourcing ROI: Does it Make Sense for You?

Release of Information and Retention

The HIPAA Privacy Rule does not include retention requirements for PHI and defers to state laws. HI professionals should review their state guidelines and organizational policies for potential retention requirements for medical records maintained by the organization, and release of information documents such as logs, authorizations, and correspondence.

Under HIPAA, a covered entity must maintain documentation of its HIPAA forms (such as complaints, breaches, restrictions, amendments, accounting of disclosures, correspondence, and assessments) for at least six years from the date of creation or the date when they last were in effect—whichever is later.

Federal and State Laws

Federal and state laws impact the processing of PHI requests in numerous ways, and variation in such laws has led to confusion throughout the healthcare industry. When reviewing the various federal laws that include patient health information privacy protections, it is essential for the health information professional to also understand respective state laws. It is common within federal law to be deferential to state laws by using language such as "unless superseded by state law." It is imperative to understand when to apply preemption rules.

This section reviews the various federal laws that can affect the decisions made when fulfilling a request for PHI. However, it is not a conclusive list and does not consider the influence of state laws.

Federal Laws

Clinical Laboratory Improvement Amendments (CLIA)

The HIPAA Privacy Rule permits covered entities, including clinical laboratories, to disclose protected health information for treatment, payment, and healthcare operations without an individual's permission or when certain additional circumstances are met. However, while such disclosures may be permitted by the HIPAA Privacy Rule, they may not be permissible under CLIA.

[23] Is a covered entity liable for, or required to monitor, the actions of its business associates? | HHS.gov

Under the current CLIA regulations, a lab is restricted to disclosure of test results to one of three categories of individuals:

- The authorized person
- The person responsible for using the test results in the treatment context
- In the case of reference labs, the referring lab

CLIA defines an authorized person as the individual authorized under state law to order or receive test results, or both. The HIPAA Privacy Rule allows individuals the right to access their PHI when held by covered entities including clinical laboratories.[24]

Additional Resources

Federal Register: CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports

eDiscovery

The term e-discovery (electronic discovery) is often used to refer to the 2006 amendments to the Federal Rules of Civil Procedure. These amendments imposed specific requirements for handling electronically stored information (ESI) during litigation in federal court. Preparing for the rules governing the discovery of electronic information and the legal process will require healthcare organizations to reevaluate the management of ESI. Today, this means an organization must consider not only the ESI stored in workstations, servers, electronic document management systems, and the like, but also on mobile devices used by clinicians, USB drives, and other forms of electronic storage media.[25]

Furthermore, an essential part of responsible information stewardship is an awareness of what metadata exists. As noted by AHIMA, metadata can "validate and quantify the authenticity, reliability, usability, and integrity of information over time and enable the management and understanding of electronic information (physical, analog, digital)."[26]

To successfully manage e-discovery, health organizations must develop a well-defined plan for managing and preparing for litigation. Collaboration among legal counsel, health information management, and information technology professionals is essential to successfully manage the e-discovery process.

Additional Resources

AHIMA BoK: Litigation Response Planning and Policies for E-Discovery

HIPAA Authorizations for ROI

The HIPAA Privacy Rule established basic standards so that all patient information generated, used, disclosed, and managed by covered entities is protected to these minimum standards. Each covered entity must develop and maintain policies and procedures that govern the management, safeguarding, use, and disclosure of the PHI in its possession. Section 164.508 of the HIPAA Privacy Rule states that covered entities may not use or disclose protected health information without a valid authorization, except as otherwise permitted or required in the Privacy Rule.[27]

General Authorization Content

The rule states that a valid authorization must be in plain language and contain at least the following core elements:

- A specific and meaningful description of the information to be used or disclosed
- The name or other specific identification of the person(s) or class of persons authorized to use or disclose the information

[24] OCR guidance on CLIA
[25] Washington, Lydia. "Managing Health Information in Mobile Devices" *Journal of AHIMA* 83, no.7 (July 2012): 58-60.
[26] Dougherty, Michelle. "How Legal Is Your EHR?: Identifying Key Functions That Support a Legal Record" *Journal of AHIMA* 79, no.2 (February 2008): 24-30.

- The name or other specific identification of the person(s) or class of persons to whom the covered entity may make the use or disclosure
- A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is sufficient when an individual initiates the request and does not provide a statement of the purpose
- An expiration date or event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure for research, including for the creation and maintenance of a research database or repository
- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of the representative’s authority to act for the individual.

Note: For proof-of-authority legal documents such as guardianships (versus conservatorships), living wills, power of attorney or healthcare power of attorney, and executor of estate or personal representative, consult legal counsel and refer to individual state laws for further guidance.

In addition to the core elements, the HIPAA Privacy Rule states that a valid authorization must include:

1. A statement of the individual’s right to revoke the authorization in writing and either:
- A reference to the revocation right and procedures described in the notice, or
- A statement about the exceptions to the right to revoke and a description of how the individual may revoke the authorization

Exceptions to the right to revoke include situations in which the covered entity has already taken action in reliance on the authorization, or the authorization was obtained as a condition of obtaining insurance coverage.

1. A statement about the ability or inability of the covered entity to require the patient to sign the authorization in order to receive treatment, payment, enrollment, or eligibility for benefits.
- The covered entity must state that it will not make treatment, payment, enrollment, or eligibility for benefits contingent on whether the individual signs the authorization, or
- The covered entity must describe the consequences of a refusal to sign an authorization when the covered entity makes research-related treatment, enrollment or eligibility for benefits, or the provision of healthcare solely for the purpose of creating protected health information for a third-party contingent upon obtaining an authorization.

2. A statement that information used or disclosed according to the authorization may be subject to redisclosure by the recipient and may no longer be protected by the privacy rule or law.

When authorization is requested by a covered entity, the covered entity must provide the individual with a copy of the signed authorization when the covered entity seeks the authorization.

Compound Authorizations

Compound authorizations, authorizations that are combined with other legal permissions, are generally prohibited under the HIPAA Privacy Rule with the following exceptions described below:

Research: An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same research or another research study. This includes authorization for the creation or maintenance of a research database or depository, or with a consent to participate in the research. When a provider has conditioned the provision of research related treatment to one of the authorizations, the compound authorization must: (1) differentiate between the conditioned and unconditioned components; and (2) offers the individual an opportunity to opt-in to the unconditioned research activities.

- Psychotherapy notes: An authorization for the use or disclosure of psychotherapy notes may be combined with only another authorization for a use or disclosure of psychotherapy notes[27]. An authorization for psychotherapy notes may not be combined, however, with an authorization for disclosure of general health information or research.

- General: An authorization for the disclosure of general health information may be combined with another authorization except when a covered entity has conditioned the provision of treatment, payment, enrollment in a health plan, or eligibility of benefits. For example, an insurance company may not combine an authorization they require as a condition of enrolling in their plan with another authorization.

Additional Resources

- HHS: HIPAA FAQ on Disclosures for Professionals
- Code of Federal Regulations: Title 45, 164.502 – "Uses and disclosures of protected health information: General rules"
- Code of Federal Regulations: Title 45, 164.504 – "Uses and disclosures: Organizational requirements"
- Code of Federal Regulations: Title 45, 164.506 – "Uses and disclosures to carry out treatment, payment, or healthcare operations"
- Code of Federal Regulations: Title 45, 164.510 – "Uses and disclosures requiring an opportunity for the individual to agree or to object"
- Code of Federal Regulations: Title 45, 164.524 - "Access of individuals to protected health information"
- HHS: Disclosures for Emergency Preparedness - A Decision Tool: Overview

21st Century Cures Act (Information Blocking)

The 21st Century Cures Act of 2016 defined information blocking as a practice by a health information technology developer, health information exchange, health information network, or healthcare provider who knows or should know that the practice is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI) unless the practice is required by law, or allowed under one or more exceptions as defined by law.

The Cures Act directs the Office of National Coordinator for Health IT (ONC) to develop rules for information blocking, and in May 2020, the ONC finalized the Cures Act Final Rule. Provisions of this rule challenge the status quo of day-to-day operations for the healthcare industry and its philosophy on providing access to electronic health information.

[27] eCFR :: 45 CFR 164.508 -- Uses and disclosures for which an authorization is required.

Health information technology developers, health information exchanges (HIEs), health information networks (HINs), and healthcare providers, including providers who do not use certified health IT under the ONC Health IT Certification Program, are considered actors and are subject to information blocking rules.[28] Knowledge requirements for information blocking practices are less stringent for providers. Providers must know that the practice is unreasonable and would likely be considered interference [with respect to the access, use, or exchange of EHI] while other types of actors such as health IT developers should know that the practice could be considered interference. [29]

At the time of writing this toolkit, the information blocking provisions of the Cures Act Final Rule applies to electronic health information that is included in the United States Core Data for Interoperability version 1 (USCDI v1). On October 6, 2022, the definition will be broadened to include ePHI to the extent it is maintained in the designated record set as defined by the HIPAA Privacy Rule. [30]

The ONC defined eight exceptions where, when certain conditions are met, a practice may not be considered an interference with the access, exchange, or use of electronic health information.

Exceptions that involve not fulfilling requests to access, exchange, or use EHI:

- Preventing harm
- Privacy
- Security
- Infeasibility
- Health IT performance

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI:

- Content and manner
- Fees
- Licensing

To learn more about each exception, see Cures Act Final Rule: Information Blocking Exceptions (healthit.gov).

While HIPAA specifies time limits to fulfill certain types of requests for health information (i.e., 30 days for patient requests), any delay in fulfillment of a request for EHI that does not meet the conditions of an exception under the Cures Act Final Rule would likely be considered interference.[31]

It is important to note that information blocking provisions apply to EHI that was created before the information blocking applicability dates and an actor must fulfill a request if they have the technical capability unless an exception applies.[32]

To assess organizational policies and procedures for compliance with the Information Blocking rule, it is helpful to have some practical knowledge of the Health IT Certification Program, the HIPAA Privacy Rule, and state-specific statutes regulating health information access, exchange, and disclosure. HIM release of information professionals are subject matter experts on federal and state laws that impact privacy, access, and disclosure of health information. Accordingly, they are well-positioned to evaluate the current state of ROI operations, and to determine how to integrate the information blocking provisions of the Cures Act Final Rule into current operations to ensure continued organizational compliance.

[28] If an entity offers or sells certified health IT, it is considered a health information technology developer under the Rule (45 CFR 171.102)
[29] Sections 3022(a) and 3001(c)(5)(D)(i) of the Public Health Service Act
[30] 45 CFR 164.501)
[31] ONC's Cures Act Final Rule (healthit.gov)
[32] ONC's Cures Act Final Rule (healthit.gov)

Recommended Practices

- Read 45 CFR, part 170 – Health IT Certification Criteria and Programs; and part 171 – Information Blocking.
- Understand what information is accessible via the patient portal and through patient-facing apps, when the information is made available, and who has access.
- Understand what information is electronically exchanged via HIEs and HIN's, when the information is exchanged, and for what purpose.
- Determine if/what certified health IT functionality is available in the current EHR environment and whether there are plans to roll out additional functionalities (to determine what technical capabilities exist).
- Evaluate current ROI policies and standard processes to determine whether any practices might constitute interference with access, use, and exchange of EHI.
- Align manual and automated release of EHI policies and practices.
- Review requirements for traditional ROI requests and whether they are more stringent than electronic access requirements; determine whether this is covered by an information blocking exception. This includes reviewing the following:
    - Authorization and request for health information forms
    - Identity verification requirements
    - Disclosure of psychiatric, substance use treatment, and other sensitive information
    - Restrictions for minor access and disclosure
    - Methods for request and delivery of health information offered
- Align denial reasons with information blocking exceptions and develop processes to document when and why exceptions were invoked.
- Develop system or EHR capabilities to notify ROI staff when an exception is applied to electronic sharing of EHI based on individualized provider determination.
- Define and document the contents of the designated record set.
- Determine which department or persons will be responsible for EHI request intake, response, and fulfillment. If the process will be shared, clearly delineate responsibilities.

Additional Resources

- ONC: Information Blocking
- ONC: Information Blocking Exceptions
- ONC: Information Blocking FAQs
- ONC: Information Blocking Fact Sheets

Sensitive Health Information

Sensitive health information such as mental health and substance use disorder records may be subject to additional federal and state privacy laws and regulations. Healthcare providers must have policies and procedures in place to ensure compliance and address any requirements relating to its disclosure. Additionally, if PHI is improperly used or disclosed, the nature of the information may be used to determine the potential extent of patient harm and culpability for privacy violations.

Sexually Transmitted and Other Communicable Diseases

This type of information may be used or disclosed for public health activities and purposes. There may be state laws that apply to the privacy of communicable disease information and impose more stringent requirements for release of information. State and federal laws and regulations should inform a covered entity's practices.

Abuse, Neglect, and Endangerment Circumstances

Unless there is a conflicting state law, a covered entity may decide to not disclose health information to a patient's personal representative if the entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by the person, and decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

Substance Use Disorder Program Records

Substance use disorder records are protected by federal law. U.S Code Section 290dd-2 and 42 CFR Part 2 specify that records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained by any substance use "program" which is conducted, regulated, or directly or indirectly assisted by the federal government are confidential and should only be disclosed as expressly authorized by these statutes. A "program" or "part 2 program" is defined by 42 CFR Part 2 as:

1. An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
2. An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
3. Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.[33]

Generally, substance use treatment records may be disclosed only with written authorization of the individual or legal representative, or upon a valid court order. Exceptions include disclosure to medical personnel to meet the need of a bona fide medical emergency and qualified service organizations. When disclosing to medical personnel without patient authorization, the nature of the emergency must be documented in the patient record. Note that written consent or authorization is required for payment and healthcare operations purposes.

Patient access requests are not prohibited, and the Part 2 program is not required to obtain a patient's written consent or other authorization to provide such access to the patient.

Consent Requirements (May be paper or electronic)

1. Patient name
2. Specific name(s) or general designation(s) of the Part 2 program(s), entity or entities, or individual(s)

[33] 42 CFR 2.11 "Program"

permitted to make the disclosure
3. How much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed
4. Recipient
5. Purpose (disclosure must be limited to that information which is necessary to carry out the stated purpose)
6. A statement that the consent is subject to revocation at any time except to the extent that the Part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer
7. Expiration date, event, or condition
8. Signature of the patient or legal representative. Electronic signatures are permitted
9. Date of signature

Prohibition on Re-disclosure
Each disclosure made with the patient's written consent must be accompanied by one of the following written statements:

1. This record which has been disclosed to you is protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this record unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or, is otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (42 U.S.C. 290dd-2, subpart C. § 2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided 42 U.S.C. 290dd-2, subpart C. §§ 2.12(c)(5) and 2.65; or

2. 42 CFR part 2 prohibits unauthorized disclosure of these records.

The Cares Act of 2020, section 3221, included certain provisions to align Part 2 Program confidentiality requirements with HIPAA[34]. Key provisions include:

- Patient may give a single, initial written consent to disclose part 2 information for purposes of treatment, payment, and healthcare operations as permitted under HIPAA. Patient may revoke the consent. Required elements of consent are not specified at this time.
- Part 2 Programs may redisclose part 2 information provided initial consent is obtained and patient has not revoked.
- Require Part 2 Programs, including those who are not a HIPAA covered entity, to provide patients/clients with a Notice of Privacy Practices (NPP) which includes how the program will use and disclose part 2 information.
- Breach notification will be required of Part 2 Programs in alignment with the HITECH Act.

The Office of Civil Rights (OCR) is expected to release a Notice of Proposed Rulemaking (NPRM) regarding Jessie's Law in 2022.

Additional Resources

Code of Federal Regulations: Confidentiality of Substance Use Disorder Patient Records

HHS: HIPAA FAQs for Professionals

Psychotherapy Notes
Psychotherapy notes are notes recorded in any medium by a mental health professional

[34] https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf

documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.[35]

Recommended Practices

- Update and review all organizational policies and procedures on the protection of psychotherapy notes.
- Educate staff on policy and procedures including the disclosure of psychotherapy notes.

Minors

Under the HIPAA Privacy Rule, parents or the legal guardian generally have the right to access health records about their minor child when they are the child's personal representative and when such access is not inconsistent with state or other law. State laws should be reviewed regarding age of majority for each specific state.

According to the US Department of Health and Human Services, there are three situations when the parent would not be the minor's personal representative under the Privacy Rule. These exceptions are:

1. When the minor is the one who consents to care, and the consent of the parent is not required under state or other applicable law;
2. When the minor obtains care at the direction of a court or a person appointed by the court; and
3. When, and to the extent that, the parent agrees that the minor and the healthcare provider may have a confidential relationship.

However, even in these exceptional situations, the parent may have access to the health records of the minor related to this treatment when state or other applicable law requires or permits such parental access. Parental access would be denied when state or other law prohibits such access. If state or other applicable law is silent on a parent's right of access in these cases, the licensed healthcare provider may exercise his or her professional judgment to the extent allowed by law to grant or deny parental access to the minor's medical information.

[35] Nicholson, Ruby. "The Dilemma of Psychotherapy Notes and HIPAA." Journal of AHIMA 73, no.2 (2002): 38-39.

It should be noted that a provider, based on their professional judgement, may choose to not disclose PHI or other sensitive information to a minor's personal representative when the provider reasonably believes that the minor has been or may be subjected to domestic violence, abuse, or neglect, or that treating the parent as the child's personal representative could endanger the child.[36]

Following are some examples of unique situations related to minors and their guardians' access to PHI:

- Emancipation of a minor: State laws will stipulate the means by which a minor becomes emancipated. Typically, a minor may become emancipated through:
  - Court order after filing a petition stating that emancipation is in his or her best interest and said minor is able to manage his/her own financial, social, and professional affairs
  - Marriage
  - Actively serving in the military
- Step-parents: Step-parents do not have the legal authority to consent for treatment of a minor or obtain their PHI unless they have been appointed legal guardian or have legally adopted the minor.
- Noncustodial parents: Noncustodial parents cannot be denied access to a minor's information unless they have been prohibited by court order.
- Portal access to minor information: This is an area that has been creating some confusion in regard to access to a minor's PHI through an electronic portal. This must be addressed through internal policies and procedures within an organization on how to allow or not allow such access, as the information visible in the portal may contain diagnoses and treatment that a minor may have sought without parental knowledge based on specific state law.

Additional Resources

HHS: Privacy Guidance Materials - Personal Representatives

Associated Costs

Paper Versus Electronic Media

In today's healthcare settings, various types of media are available for creating, storing, and releasing PHI. To determine the most reasonable and appropriate fee, covered entities must consider how and where the PHI is stored, the format requested by the recipient or the method of access, and the type of requester, such as patient, attorney, or payer.

Patients or Individuals

The HIPAA Privacy Rule permits covered entities to charge a reasonable, cost-based fee to provide copies of PHI to patients/individuals or their personal representative, or to direct copies to a third party. Fees may include:

- Labor costs for copying, creating, or delivering the PHI; or preparing a summary of the PHI if the patient requests a summary and agrees to the fee in advance. (It is important to note that costs associated with reviewing the request; or searching, retrieving, compiling, segmenting, or otherwise preparing the PHI for delivery may not be included in labor costs.)
- Supplies such as paper, toner, or electronic media
- Postage

While HIPAA permits fees for individuals, they must not create a barrier to access and records should not be withheld when an individual is unable to pay. Individuals have the right to request that their PHI be delivered via email. Covered entities may not charge individuals to electronically access PHI where no manual intervention is

[36] Does the HIPAA Privacy Rule allow parents the right to see their children's medical records? | HHS.gov

required. Similarly, a covered entity may not charge a fee for individuals to simply inspect PHI, or when the individual is making copies using their own resources such as a personal smart phone. Finally, individual fees allowed under state law preempt those allowed under the Privacy Rule only if the state law provides greater rights to the individual. For example, a state law may require that copies of PHI to patients and individuals are always provided at no cost.

Recommended Practices

Whether developing or updating your organization's policies and procedures:

- Understand the HIPAA Privacy Rule, as well as any other federal and state laws and that address the patient's right to access and obtain copies of PHI.
- Check your state government website annually for any updates or changes to copying charges.
- Encourage electronic access such as the patient portal to help with costs to patient and organization.

Additional Resources

HHS: "May a covered entity charge individuals a fee for providing the individuals with a copy of their PHI?"

HHS: "Can an individual be charged a fee if the individual requests only to inspect her PHI at the covered entity?"

HHS: "Does the HIPAA Privacy Rule preempt state laws?"

Attorneys, Insurance Companies, and Other

Because requirements of the HIPAA Privacy Rule do not address fees outside of patient/individual requests and directives, state regulations continue to provide the most specific guidelines for third-party requestors. Some states have specific regulations which guide the method in which a covered entity is able to charge for delivery of records in electronic media/format. If there is no regulation, the covered entity should apply standard rates for paper copies. Additionally, fees for copies of records may be specified within third-party contracts and other agreements.

Appendix A
Glossary of Terms

Access: The ability or means necessary to make electronic health information available for exchange and use.

Accounting of Disclosure (AOD): HIPAA requirement to list, upon patient request, all disclosures that meet the criteria. Currently, this does not require accounting for disclosures for treatment, payment, and healthcare operations (TPO), but under ARRA these changes to include these disclosures, awaiting final regulations.

Authorization: 1. The granting of permission to disclose confidential information; as defined in terms of the HIPAA Privacy Rule, an individual's formal, written permission to use or disclose his or her personally identifiable health information for purposes other than treatment, payment, or healthcare operations. 2. A patient's consent to the disclosure of protected health information (PHI); the form by which a patient gives consent to release of information.

Authorized Person (under CLIA): The individual authorized under state law to order or receive test results, or both.

Behavioral/Mental Health: A broad array of psychiatric services provided in acute, long-term, and ambulatory care settings; includes treatment of mental disorders, chemical dependency, mental retardation, and developmental disabilities, as well as cognitive rehabilitation services.

Breach: A violation of a legal duty or wrongful conduct that serves as the basis for a civil remedy.

Breach of Confidentiality: A violation of a formal or implied contract in which private information belonging to one party, but entrusted to another party, is disclosed by that individual without the consent of the party to whom the information pertains; an unauthorized disclosure of confidential information.

Business Associate: 1. According to the HIPAA Privacy Rule, an individual (or group) who is not a member of a covered entity's workforce but who works on behalf of the covered entity and creates, receives, maintains or transmits protected health information. 2. A person or organization other than a member of a covered entity's workforce that works on behalf of the covered entity and creates, receives, maintains or transmits protected health information.

Compliance: 1. The process of establishing an organizational culture promoting the prevention, detection, and resolution of instances of conduct not conforming to federal, state, or private payer healthcare program requirements or the healthcare organization's business policies. 2. The act of adhering to official requirements.
3. Managing a coding or billing department according to the laws, regulations, and guidelines that govern it.

Continuum of Care: The range of healthcare services provided to patients, from routine ambulatory care to intensive acute care; the emphasis is on treating individual patients at the level of care required by their course of treatment with the assurance of communication between caregivers.

Covered Entity: Under HIPAA, a covered entity means:

1. A health plan
2. A healthcare clearinghouse
3. A healthcare provider who transmits any health information in electronic form

Designated Record Set (DRS): 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 patient care-related decisions.

Disclosure: The act of making information known; in the health information management context, the release of confidential health information about an identifiable person to another person or entity.

Electronic Health Information (EHI): Electronic protected health information as defined in CFR 45 160.103 to the extent that it would be included in a DRS.

Electronic Health Record (EHR): An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization.

Healthcare Operations: Certain activities undertaken by or on behalf of, a covered entity, including: conducting quality assessment and improvement activities; reviewing the competence or qualifications of healthcare professionals, underwriting, premium rating, and other activities relating to the creation; renewal or replacement of a contract of health insurance or health benefits; conducting or arranging for medical review, legal services, and auditing functions; business planning and development; and business management and general administrative activities of the entity.

Health Information: According to the HIPAA Privacy Rule, any information (verbal or written) created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse that relates to the physical or mental health of an individual, provision of healthcare to an individual, or payment for provision of healthcare.

Health Information Technology for Economic and Clinical Health Act (HITECH): Legislation created to stimulate the adoption of EHR and supporting technology in the United States. Signed into law on February 17, 2009, as part of the American Recovery and Reinvestment Act.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): The federal legislation enacted to provide continuity of health coverage, control fraud and abuse in healthcare, reduce healthcare costs, and guarantee the security and privacy of health information; limits exclusion for pre-existing medical conditions, prohibits discrimination against employees and dependents based on health status, guarantees availability of health insurance to small employers, and guarantees renewability of insurance to all employees regardless of size; requires covered entities (most healthcare providers and organizations) to transmit healthcare claims in a specific format and to develop, implement, and comply with the standards of the Privacy Rule and the Security Rule; and mandates that covered entities apply for and utilize national identifiers in HIPAA transactions; Also called the Kassebaum-Kennedy Law; Public Law 104–191.

Individually Identifiable Health Information (IIHI): According to HIPAA privacy provisions, that information which specifically identifies the patient to whom the information relates, such as age, gender, date of birth, and address.

Information Blocking: A practice by a health IT developer of certified health IT, health information network, health information exchange, or health care provider that, except as required by law or specified by the Secretary of Health and Human Services as a reasonable and necessary activity, is likely to interfere with access, exchange, or use of electronic health information.

Legal Health Record (LHR): Documents and data elements that a healthcare provider may include in response to legally permissible requests for patient information.

Promoting Interoperability Program (Formally known as Meaningful Use (MU): A regulation that was issued by the Centers for Medicare and Medicaid Services on July 28, 2010, outlining an incentive program for eligible professionals, eligible hospitals, and critical access hospitals participating in Medicare and Medicaid programs that adopt and successfully demonstrate meaningful use of certified electronic health record technology.

Metadata: Descriptive data that characterize other data to create a clearer understanding of their meaning and to achieve greater reliability and quality of information. Metadata consists of both indexing terms and attributes. Data about data: for example, creation date, date sent, date received, last access date, last modification date.

Minimum Necessary Standard: A stipulation of the HIPAA Privacy Rule that requires healthcare facilities and other covered entities to make reasonable efforts to limit the patient-identifiable information they disclose to the least amount required to accomplish the intended purpose for which the information was requested.

Notice of Privacy Practices: A statement (mandated by the HIPAA Privacy Rule) issued by a healthcare organization that informs individuals of the uses and disclosures of patient-identifiable health information that may be made by the organization, as well as the individual's rights and the organization's legal duties with respect to that information.

Office of Civil Rights (OCR): Department in HHS responsible for enforcing civil rights laws that prohibit discrimination on the basis of race, color, national origin, disability, age, sex, and religion by healthcare and human services entities over which OCR has jurisdiction, such as state and local social and health services agencies, and hospitals, clinics, nursing homes, or other entities receiving federal financial assistance from HHS. This office also has the authority to ensure and enforce the HIPAA Privacy and Security Rules; OCR is responsible for investigating all alleged violations of the Privacy and Security Rules.

Preemption: A legal doctrine that requires a covered entity to comply with federal law when federal and state law conflict.

Privacy: The quality or state of being hidden from, or undisturbed by, the observation or activities of other persons, or freedom from unauthorized intrusion; in healthcare-related contexts, the right of a patient to control disclosure of protected health information.

Privacy Rule: The federal regulations created to implement the privacy requirements of the simplification subtitle of the Health Insurance Portability and Accountability Act of 1996; effective in 2002; afforded patients certain rights to and about their protected health information.

Protected Health Information (PHI): Individually identifiable health information that is transmitted by electronic media, maintained in electronic form, or transmitted in any other form or medium; Under HIPAA, all individually identifiable information, whether oral or recorded in any form or medium, created or received by a healthcare provider or any other entity subject to HIPAA requirements; Under the HITECH Final Rule, decedent health information older than 50 years is no longer considered PHI.

Qualified Protective order: An order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that 1) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested, 2) Requires the return to the covered entity or destruction of the protected health information (including copies made) at the end of the litigation or proceeding. (45 CFR 164.512(e)(1)(v).

Regulation: A rule established by an administrative agency of the government. The difference between a statute and a regulation is regulations must be followed by any healthcare organization participating in the related program. Administrative agencies are responsible for implementing and managing the programs instituted by state and federal statutes.

Release of Information: The process of disclosing protected health information from the health record to another party.

Retention: 1. Mechanisms for storing records, providing for timely retrieval, and establishing the length of times that various types of records will be retained by the healthcare organization. 2. The ability to keep valuable employees from seeking employment elsewhere.

Security: 1. The means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration, destruction, or loss. 2. The physical protection of facilities and equipment from theft, damage, or unauthorized access; collectively, the policies, procedures, and safeguards designed to protect the confidentiality of information, maintain the integrity and availability of information systems, and control access to the content of these systems.

Security Rule: The federal regulations created to implement the security requirements of the Health Insurance Portability and Accountability Act of 1996.

Subcontractor: A person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate; a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate.

Substance Abuse: Defined by the Diagnostic and Statistical Manual of Mental Disorders, 4th edition as a maladaptive pattern of substance use leading to clinically significant impairment or distress, as manifested by one (or more) of the following, occurring within a 12-month period.

Treatment, Payment, Operations (TPO): Term used in the HIPAA Privacy Rule pertaining to broad activities under normal treatment, payment, and operations activities, important because of the rule's many exceptions to the release and disclosure of personal health information. Collectively, these three actions are functions of a covered entity which are necessary for the covered entity to successfully conduct business.

Use: Respect to identifiable health information, the sharing, employment, application, litigation, examination, or analysis of such information within an entity that maintains such information.

Appendix B

Sample Certification Form

Certification of Medical Records

DATE: _____

TO WHOM IT MAY CONCERN:

This is to certify that, to the best of my knowledge, the attached represents a true and complete copy of the medical records described in your request, subpoena, summons or court order. As the duly authorized custodian of health information, I have the authority to certify the records of patient:

Patient Name: _____

These records were prepared by the personnel of this facility, medical staff members, or persons acting under the control of either, in the ordinary course of this facility's business at or near the time of the act, condition or event. The copies were prepared by the personnel of (Name of Healthcare Organization).

Custodian of Medical Records

*NOTE that certification requirements vary from state to state regarding actual verbiage required. In some states, certifications must be notarized, or affidavits are required.

(For Office Use Only)
Account Number: *Medical Record Number:*

Appendix C

Sample Return Request Letter

HEALTHCARE FACILITY NAME:

DATE:_____

REGARDING PATIENT:_____

To Whom It May Concern:

Unfortunately, we are unable to process your request for health information at this time due to one or more of the following reasons:

☐ Missing date on authorization

☐ Missing signature of the patient or legal representative

☐ Missing expiration date or event

☐ Missing the description of the representative's authority to sign on behalf of the patient

☐ Missing the purpose of the disclosure

☐ Missing a statement describing the individual's right to revoke authorization and description on how to revoke

☐Missing statement that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and is no longer protected by HIPAA

☐ Missing the name of the person/entity to receive the information

☐ Missing a statement that the treatment and payment may not be conditioned on the individual's authorization

☐ The authorization or request form is signed by someone other than the patient. Please provide supporting documentation such as: properly executed letters of administration, power of attorney, guardianship papers or certified copies of any court documents that show authority to sign on behalf of the patient.

☐ An executor of estate/administrator or next responsible family member that was involved in the care or payment of care will be required to sign an authorization or request form on behalf of the patient.

If you would still like to obtain records, please resubmit your request with a valid authorization form and any additional information if required.

Sincerely,

Health Information Management

Appendix D

Sample Release of Information Specialist Job Description

Position Summary:
The Release of Information (ROI) Specialist maintains and protects health information within the designated record set and is responsible for disclosing information in a timely, accurate, and compliant manner in accordance with laws, system policies, and standard operating procedures. This position will be responsible for providing and ensuring high quality customer service to both internal and external customers.

Essential Functions:
The ROI Specialist responsibilities include, but are not limited to, the following:

- Accurately and efficiently processes requests for health information access and disclosure in compliance with HIPAA and other federal and state statutes, as well as organizational policies and standard operating procedures
- Logs and tracks all requests for access and disclosure of information in the information system in accordance with policies and standard operating procedures
- Monitors and manages multiple sources for requests for information such as patient portal, email, fax, mail, and in-person
- Reviews health information within multiple source systems, locations, and formats; discerns whether information is part of the legal medical record, billing record, or designated record set and understands access rights and requirements for each
- Comprehensively and concisely identifies and discloses information requested and/or authorized
- Ensures and expedites requests for health information in compliance with regulatory timeframes as required for the specific request types
- Reviews medical records for legally protected and sensitive information and obtains additional authorization, approval, or documentation when necessary
- Provides knowledgeable and competent customer service and uses various tools and information systems to facilitate the process
- Serves as a health information ambassador and patient liaison by ensuring rights to health information including privacy and right of access while encouraging patient engagement in healthcare by providing easy and timely access
- Serves as a subject matter expert resource for privacy and disclosure matters

Qualifications:

- 2 years of experience in health information management or working with health information in other area; degree in Health Information Management/Health Information Technology may be substituted
- AHIMA Certifications of RHIT, RHIA, or CHPS preferred
- Release of information or disclosure management experience is preferred
- Previous experience with health language literacy with ability to locate and interpret information on forms, documents, and other sources within clinical information systems
- Working knowledge of HIPAA and other federal and state rules preferred
- Previous experience with computer systems and telecommunications technology required