American Health Information Management Association

RELEASE OF INFORMATION

TOOLKIT

A Practical Guide for the Access, Use, and Disclosure of Protected Health Information

AHIMA
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

TABLE OF CONTENTS

TABLE OF CONTENTS

FOREWORD

In 2008, AHIMA worked on a project focusing on the release of healthcare information for the purpose of patient continuity of care. This project was based on information obtained from a 2006–07 comprehensive study sponsored by the **Agency for Healthcare Research and Quality (AHRQ)** to understand the barriers regarding the transfer of information between healthcare providers. AHIMA participated in this study, which reflected practices that were occurring throughout the continental United States.

The intent of the 2008 project was to provide a framework for covered entities in relation to how the **disclosures** of **protected health information (PHI)** were to be made by encompassing all current regulations in place at that time.

With the passing of the **American Recovery and Reinvestment Act's (ARRA's)** and the **Health Information Technology for Economic and Clinical Health (HITECH) Act**'s privacy modifications, breach notification requirements, and new enforcement rules, the information collected and produced from the 2008 project has been reviewed and updated. Content has been added to reflect new legislative components and current industry practices impacting the disclosure of PHI for all purposes including continuity of care. This toolkit is a result of that work.

Disclaimer: For the purposes of this toolkit, federal guidelines are included for reference, but state laws must always be reviewed to determine whether preemption applies.

Note: Boldface *terms throughout the toolkit indicate defined items in the glossary (See Appendix A).*

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
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 Dooling, 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

INTRODUCTION

The accurate disclosure of protected health information (PHI) is paramount. From the receipt of the request to the delivery and logging of the PHI disclosed, many factors must be considered and accounted for, such as federal and state laws, response times, and necessity of the PHI requested, to name a few. Policies and procedures must be in place for timely and accurate disclosures. Policies and procedures set the tone for the organization and its staff on the significance of accountability and responsibility in disclosing PHI. Knowledgeable, experienced, and well-trained staff are also required for compliant and efficient processing of requests. To help healthcare organizations and health information management (HIM) professionals navigate their way through **release of information** (ROI) practices within today's heavily regulated and rapidly changing environment, this toolkit has been revised to incorporate various types of disclosures of PHI and reflect today's practices.

The purpose of this toolkit is to help an individual develop an effective ROI process across any setting. It is to be used as a framework and reference guide to ensure disclosures of PHI are made in accordance with all state and federal **regulations** in a timely manner to guarantee the integrity of the PHI is maintained. For adequate response and turnaround times, types of requests must be anticipated before they are received with appropriate policies and procedures in place to facilitate smooth business process flow. This includes addressing the common types of disclosures anticipated and how they would be handled, the quality management and tracking procedures, as well as research of state and federal laws that will impact the processes. See Appendix B for a sample release of information policy and procedure.

The toolkit discusses recommended practices that should be undertaken in regards to processing PHI requests regarding fees and specific regulations related to HIV, drugs and alcohol, **mental health**, and genetics. With the implementation of **electronic health records (EHRs)**, the toolkit was amended to include guidance on processes and workflows with a focus on electronic ROI and electronic disclosure management systems. Examples are provided that address how HIM departments can revise current policies and practices to incorporate electronic signatures, patient portals (disclosures within the portal and **security** surrounding access), and producing records from various systems in a readable format (patient output record), to name a few.

THE CURRENT LANDSCAPE OF ROI

Release of information continues to be challenging for many HIM professionals. The current healthcare environment is changing, not only with a new emphasis on patient rights in regard to disclosure for personal health records and portals, but in regard to reimbursement and **meaningful use**. The disclosure of PHI is also becoming more transparent and mandated by government entities (Centers for Medicare and Medicaid [CMS], Recovery Audit Contractor [RAC], Center for Education on Research and Therapeutics [CERTs], etc.).

Both state and federal rules and regulations must be considered and accounted for when disclosing PHI. HIM professionals are often faced with the challenges of accurately disclosing PHI in a manner that is consistent with common industry practice. EHRs have increased the need for more oversight regarding the disclosure and release of PHI in a secure and safe manner. Furthermore, the release of the final HITECH Act's modifications to the privacy and security rules on January 25, 2013, has made official the first major changes to current privacy and security practices since the HIPAA privacy rule was implemented in 2003. The act strengthens privacy and security requirements as well as broadening patient rights to accessing and restricting the uses and disclosures of their PHI.

Traditionally, the paper record was maintained by the HIM department and secured in one location. With the EHR, the disclosure of PHI can occur outside of the HIM department, thus creating an environment for unauthorized disclosure and **breach of confidentiality.**

The HIM professional must maintain a working knowledge of ROI practices when faced with completing requests for PHI to ensure the request meets the requirements under **HIPAA** (for **treatment, payment, and healthcare operations–TPO**) and that "other" **authorizations** are HIPAA compliant.

HIM PROFESSIONALS AND ROI

HIM professionals are not only responsible for overall documentation integrity; they also directly control who sees the information, how much information is seen, and to whom the information is disclosed. Strong collaborative relationships with senior leadership and all department staff releasing PHI is necessary and will impact organizational success for compliance.

It is the HIM professional's role to ensure all staff, including staff outside the HIM department, are educated and policies and procedures are developed to guarantee appropriate disclosure. As organizations move toward an electronic environment, "old" policies need to be reviewed and revised based on new regulations and software. See Appendix C for a sample listing of release of information policies and procedures a HIM department should have.

Sufficient knowledge in both state and federal rules pertaining to the disclosure of PHI is imperative. With the increase in healthcare systems reaching into physician practice management, the education of HIPAA and ROI must fall to the highly skilled HIM professional.

DEFINING RELEASE OF INFORMATION

WHAT IS ROI?

Release of information (ROI) is defined as a process of providing access to protected health information (PHI) to an individual or entity authorized to receive or review it.[1] This disclosure of PHI outside the covered entity must be in accordance with federal and state laws and 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.[2] Covered entities are expected to take specific precautions when they release health information. The rule broadly defines **health information** as any information, whether oral or recorded in any form or medium, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.[3]

Individually identifiable health information (IIHI) is information that includes demographic information collected from an individual, and that is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and health information that can identify an individual or reasonably could be used to identify an individual.[4]

The 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), certain records that have substantial **privacy** protection, or employment records held by a covered entity in its role as an employer.[6,7,8,9] However, HIPAA may apply if these records are considered part of the covered entity's designated record set.[10]

To release information, the covered entity must either receive a valid authorization or the request must fall within an exception under either HIPAA or state law that allows the disclosure of PHI without an authorization. See Appendix D for a sample authorization form.

USE VS. DISCLOSURE

The term "Use and Disclosure" came into common use with the creation of the Privacy Rule under HIPAA and are foundational building blocks to understanding how to apply the rule.[11] Individual state laws must be reviewed for additional definitions for use and disclosure and any privacy provisions that may differ from the Privacy Rule.

Use

As defined under federal regulations, use of PHI is "the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information."[12] The key word here is within because it addresses how entities covered under HIPAA are allowed to use PHI for internal purposes without patient authorization. For example, physicians may consult freely with other physicians about a patient's course of treatment. Another example would be when a covered entity uses PHI for patient safety purposes.

Disclosure
Federal regulations define disclosure as "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information."[13] The key word here is *outside*, such as disclosing a patient's medical record to an attorney.

A variation of the outside distinction occurs when entities disclose PHI to third-party payers to obtain reimbursement, such as payment for the services rendered. This type of disclosure often is addressed in the organization's **notice of privacy practices,** but many entities ask the patient to authorize release to the insurer, even though disclosure for payment purposes does not require an authorization.[14]

Another variation may be for the covered entity that discloses PHI to ensure the patient receives continuity of treatment with a healthcare provider who is not a member of its medical staff. While disclosure for treatment does not require an authorization, an organization may choose to require a patient authorization before releasing to a provider who is not a member of its medical staff and hence not *inside*.

Two examples of a disclosure not permissible without patient authorization is (1) in states where a patient must "opt in" to allow the submission of patient data to a health information exchange (2) PHI protected by federal **substance abuse** regulations.[15, 16]

Minimum Necessary
Minimum necessary is a concept that was introduced by the Federal Privacy Act of 1974 and further defined by the HIPAA privacy regulations in 2003. It will be addressed in further detail in later sections of this toolkit. However, for the purposes of this introductory section, regardless of whether information is used within or disclosed to an outside covered entity, the 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 the minimum information is released.

An example of the former would be limiting access to a ROI specialist to those records for which a request has been received. The limitation allows the clerk to perform his or her job but does not provide the clerk with greater access than is necessary to accomplish his or her work tasks. An example of the latter would be when a patient authorizes a copy of his or her blood typing to be provided to the local Red Cross. The covered entity should not release all of the laboratory data that is available in the patient's record. The disclosure should be limited to only the blood typing report. Request for continuity of care or a patient's personal use, the minimum necessary provision does not apply.

Incidental Disclosure
The potential exists for PHI to be disclosed in an incidental fashion.[17] For example: A patient's name may be called out in HIM release of information waiting room. Or it may be possible for an individual waiting on copies of records to overhear the ROI specialist take a call from another patient. These incidental disclosures are permitted so long as the organization has taken reasonable safeguards to minimize such occurrences.

Recommended Practices

- If a common waiting room is used for patients scheduled to be seen as well as individuals waiting for copies of their records, consideration could be given to using vibrating pagers (like those used in restaurants) instead of calling out patient names. This would avoid an inadvertent disclosure of the patient's name by a given clinic and thereby disclosing the patient's condition or purpose for being at the clinic.
- When a patient and/or the patient's legal representative has made an appointment to access the patient's records, arrange for the review to occur in a supervised private location (like mini-conference rooms, offices, etc.) to keep others from overhearing the discussions that may take place.
- A "clean desk" policy should be followed which means that at the end of a shift, each employee's workspace should be clear of any PHI. This practice is equally important for release of information staff. Documents displaying PHI should be turned over to avoid being seen by a patient or other requestor when they approach the ROI desk.
- Computer screens should have privacy shields to limit incidental viewing.
- Phone calls should be conducted in a private setting with a quiet voice.
- Voice messages should be left to a minimum. For example: "Hello, Mrs. Smith. This is Jane Doe at XYZ Hospital; please contact me in reference to the information you have requested."

TYPES OF REQUESTS

A covered entity may receive a variety of requests for PHI that include continuity of care, legal purposes, insurance reasons, third party reviewers, patient access to information or requesting changes to information, etc. 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. In general, if the requested information is for treatment, payment or operations, an authorization by the patient or personal representative is not required.[18] Refer to the Legal Section of the toolkit for additional information.

Continuity of Care: Requests to disclose information for the continuity of care of the patient.
Examples:

- Nursing home requesting information from a patient's previous hospitalization
- Physician clinic requesting lab report from visit

Legal: Requests from attorneys or judges. Examples:

- An attorney request for litigation
- An attorney office requests all records for a deceased patient from hospital to pursue closing an estate
- An attorney sends a court order requesting records related to a guardianship

Government Agency: Requests that may not require a patient's authorization because the disclosure is permitted by regulation.
Examples:

- State Disability Determination Program—requests received to determine the patient's physical and mental condition to assess whether patient should receive benefits under the disability program plan
- Workers' Compensation—requests received by the agency that determines whether an injury occurred as a result of the patient's work and to assess whether the patient should receive benefits under the workers' compensation plan

Insurance: Requests for patient information for purposes of determining the appropriateness of healthcare insurance payment.
Examples:

- Commercial insurers such as Blue Cross or United Healthcare
- Governmental insurers such as Medicare, TriCare, Medicaid, or their third party representative

Patient: Requests from patient or their legal/personal representative to see or obtain a copy of their health information for services provided.
Example:

- Patient asks for a copy of a radiology report and film of a recently conducted test

Law Enforcement: Requests to provide information to assist with an investigation.
Example:

- Police requests emergency room records for a victim of a violent crime

Third Party Reviewers (such as QIO/RAC/MIC/MAC/other reviewers for commercial insurers):
Requests to provide copies of records for review by an entity that determines the appropriateness of care provided, determines whether the care met quality expectations, or determines whether the care provided is accurately reflected on the claim that will be or has been paid by the organization that the review entity represents.
Example:

- Request to send copy of record to the Recovery Audit Contractor to review for suspected inappropriate billing practices

Release of Information for External Database Reporting: (such as state cancer registries, core measure reporting, state trauma registries, center of excellence reporting):
These requests are usually mandated by state or federal regulations; however, a covered entity may volunteer to participate in a reporting initiative for benchmarking and quality improvement purposes. These requests may or may not identify the patient and may include aggregate patient information or single patient occurrence (i.e. Center for Disease Control) for surveillance or outcomes purposes. Because of their nature, often this information may be released for external database reporting purposes without prior consent.
Example:

- Reporting of all cases that presented to the hospital with an initial diagnosis of cancer

Research: Requests to provide copies of information for review by an external researcher. These are typically accompanied by a patient authorization when the request is received from an organization not associated with the covered entity. However, for research projects approved by an institutional review board (IRB) an authorization is not required. Example:

The American Cancer Research Organization requests records of a patient for cancer research. A valid authorization is submitted with the request.

SIGNIFICANCE OF THE LEGAL HEALTH RECORD AND ROI

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

(i) The medical records and billing records about individuals maintained by or for a covered healthcare provider
(ii) The enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health plan; or
(iii) Used, in whole or part, by or for the covered entity to make decisions about individuals.[19]

Simply stated, the DRS includes those documents or records that were used in or 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, etc.

The **legal health record (LHR)** is a subset of the DRS. AHIMA defines the LHR as "generated at or for a healthcare organization as its business record and is the record that would be released upon request."[20]

In a paper environment, the LHR is 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 manager; 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. "HIM 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."[21]

HIM professionals, in collaboration with information technology and legal counsel or risk management, should list the specific data elements and/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 (paper, electronic, microfilm, scanned, etc.) in which the document is stored.

Traditionally, records from other facilities (commonly known as "outside records") were not released when a request was received. However, since records from other facilities may have aided 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. This is particularly important when a covered entity is responding to an "any and all records" request.

For covered entities that maintain patient care documents in an electronic format that allows for variable displays (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, disclosures about the treatment provided should be made from the LHR. 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
- 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.
- Periodically review copies of records that have been prepared for disclosure purposes to ensure staff is preparing copies in the format defined by the LHR policy and that the minimum necessary are released.

PROCESSES AND WORKFLOW

Disclosure of health information is a critical function to the provision of high-quality and cost-effective healthcare. The information should be complete and timely for the intended purpose. While this sounds straightforward, it is not an easy task in the complex medical and legal environment in which the healthcare community operates. The HIPAA Privacy Rule contains specific requirements for managing health information to ensure the privacy and confidentiality of the individual. It also tries to balance the need for prompt and informed delivery of healthcare services while protecting the privacy of the individual. Generally, the HIPAA Privacy Rule allows disclosure of health information between providers without patient authorization when the purpose is for continuity of care. This, according to CMS, is "to avoid interfering with an individual's access to quality health care…."[22] There is no standard uniform state privacy law that is used by all 50 states plus territories. State laws vary in focus topic (HIV, substance abuse, mental health, genetic information, etc.) as well as degree of strictness or protectiveness of patient privacy. Some states have no additional laws while others require additional specific patient authorization language be obtained prior to release.

ROUTINE PROCESS WORKFLOW IN RESPONDING TO A REQUEST

The HIPAA Privacy Rule permits use and disclosure of protected health information, with certain limits and protections, for treatment, payment, and healthcare operations activities. A requestor asks for information of the provider who has existing information about an individual. The provider's staff processes the request to ensure that it is a valid request, that their response to the request provides sufficient information for the intended purpose, and that their response is delivered in a manner that is timely for the need. Under HIPAA, requests are to be processed within 30 days of receipt for records stored on-site and within 60 days for records stored off-site. One 30-day extension is permitted, if needed. The extension request must be sent to the requestor to notify them that there is a delay. (The HITECH Act's final rule removes the 60-day time limit for records stored off site.) Therefore, starting September 23, 2013 (compliance date of HITECH Privacy Modification), all requests must be processed within 30 days regardless of record location. The one-time 30-day extension remains.

Requests for information should be logged either in a manual or electronic format. While HIPAA does not require logging of requests for treatment, payment, or healthcare operations, it is beneficial to log all requests for tracking and productivity purposes. This log should include, at a minimum, the date the authorization was received, the date the authorization is processed, patient name, patient identification number (medical record number), date(s) of service requested, requestor, purpose of disclosure, and fee if applicable. The flow process below describes the step-by-step process for a response to a general request for information. It is followed by a flow chart representing the same process in a simple graphic form. See Appendix E for recommended minimum data sets by requestor.

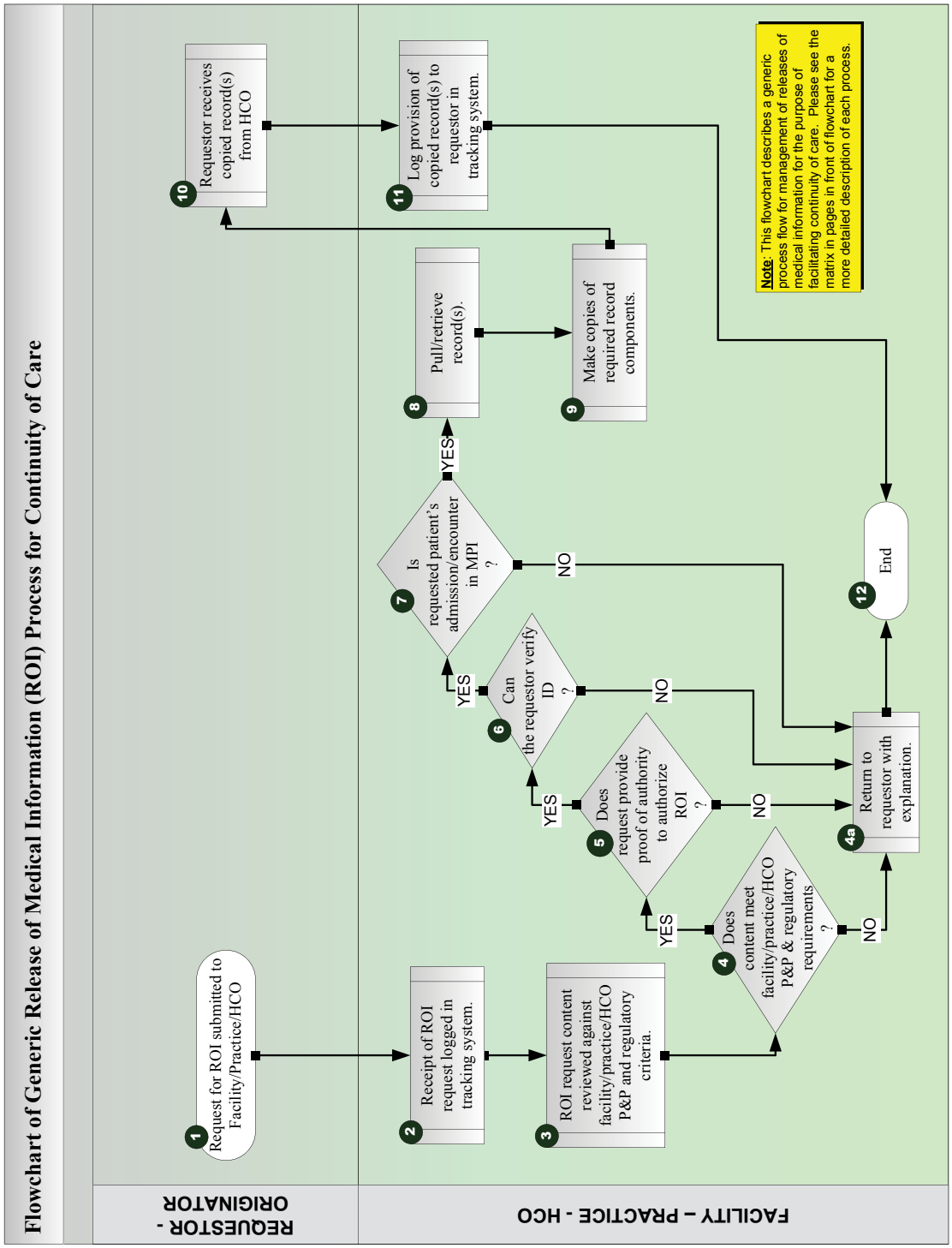
ROUTINE PROCESS WORKFLOW

Flowchart Content Description: Generic Release of Information (ROI)

#	FLOW PROCESS CONTENT	ACTION COMPLETED BY	ACTION	NEXT STEP
1	Requestor submits a request for ROI. Request may be verbal or written.	Request originator.	Submission of a request for ROI initiates the process. Request originators may submit ROI requests in narrative form, on a form of their own design, or on a form designed by the covered entity holding the records of concern. Requests for ROI may be delivered in person by the requestor, or received through the mail, by facsimile, e-mail, or telephone. Organizations should have policies addressing the means by which it will accept requests for ROI. Organizations should have policies in place for verifying requestor if request is made verbally.	2
2	Receipt of the ROI request is logged into the system. System may be manual or electronic. If manual, the ROI must be date stamped with date received so that the turnaround time can be monitored to ensure compliance with regulations.	Covered Entity	Receipt of the ROI request is logged, initiating its tracking process. This step and all subsequent tracking of the status of each request received should be logged.	3
3	ROI request content is reviewed against policies and procedures and regulatory criteria.	Covered Entity	The request is reviewed to determine compliance with both internal policies/procedures and regulatory requirements. Procedure must address differences in process depending on type of request (i.e., routine, emergency, etc.), consideration of compliance with minimum necessary standard, etc.	4
4	Decision Point: Does the request content meet the required policies, procedures and regulatory requirements?	Covered Entity	If no, the request does not comply, proceed to step 4a. If yes, the request does comply, proceed to step 5.	4a, or 5
4a	No: Return the request to the originator with a return letter.	Covered Entity	Content of request does not meet required criteria. It is returned to the originator. An explanation as to why the request cannot be processed is provided. It can be recommended that a standard form letter be created by an organization for returned requests.	11 or 12

#	FLOW PROCESS CONTENT	ACTION COMPLETED BY	ACTION	NEXT STEP
5	Yes: Decision Point: Does the request provide proof of authority to authorize ROI?	Covered Entity	Determines whether the requestor/ROI request demonstrates the requestor's authority to authorize the release. If no, go back to step 4a. If yes, go to step 6.	4a, or 6
6	Yes: Decision Point: Can requestor verify identity?	Covered Entity	Verify the identity of the entity requesting the release. Verify signature with signature on file. If ROI is not signed by patient, review record to determine who is the authorized representative if not the patient. If no, go back to step 4a. If yes, go to step 7.	4a, or 7
7	Yes: Decision Point: Is requested patient's admission(s)/ encounter(s) in Master Patient Index (MPI).	Covered Entity	Consult the MPI to identify all admissions/ encounters for the patient(s) concerned to ensure it can identify all records/record components to be retrieved in order to comply with the ROI request. If no, go back to step 4a. If yes, go to step 8.	4a, or 8
8	Pull/retrieve/electronically access record(s) of concern.	Covered Entity	Locates/retrieves/accesses all records/ record components necessary to comply with the ROI request. Review PHI related to request for any applicable restrictions and minimum necessary.	9
9	Produce copies of required record components in the format requested by the requestor.	Covered Entity	Makes the necessary copies of the record(s)/record components. These copies are certified if required. Include with the documents a statement that the information is protected under specific state or federal regulations if the information is sensitive in nature; include a cover sheet stating that the information is protected by HIPAA.	10
10	Provide copied record(s) to requestor or designated entity in the format requested by the requestor according to organizational policy.	Covered Entity	Copies of the record(s) are provided to the designated recipient.	11
11	Log completed request in the tracking system	Covered Entity	Record completion.	12
12	End.	Not Applicable (N/A)	This process is complete. No further action is required.	N/A

Routine Process Workflow Diagram (See also Appendix F)



SUCCESSFUL MANAGEMENT PRACTICES

Successful management for release of information is a critical decision to be made by organizational leadership to include HIM. Historically, the options 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, backlog help, or full outsourcing. There are many factors in the decision to determine what is best for your hospital, clinic, or physician practice. It should be noted that customer service should always be considered regardless of how the ROI workflow is accomplished. Correspondence related to return request letters should be in a format that is clearly understandable to the requestor. Should a record need to be certified, the certification should clearly identify the individual and their title on the certification. See Appendix G and H, respectively for a sample Certification Form and Return Request Letter.

RELEASE OF INFORMATION IN-HOUSE

Many considerations must be accounted for when deciding to keep the ROI function in house, such as performing a cost analysis or risk analysis. If choosing to keep the ROI process in house, there are many elements of the program that need to be discussed and addressed. These include, but are not limited to:

- Staffing
  - Credentialed versus noncredentialed ROI staff
  - ROI staff should be placed at a higher pay grade due to the significant detail, experience, and potential for risk that is part of the release process
  - Coverage issues: Short-term (sickness/illness) versus long-term (FMLA)
  - See Appendix I for a sample job description
- Training
  - New hire
  - Ongoing
- Request workflow processes
  - Customer care call center (depending on size of your covered entity)
  - Verbal versus faxed requests for continued care
  - Cross-training for full service staffing or specialized training for specific request types
  - Process consistency: Receipt of request, logging and/or tracking of request, processing of request, distribution of request.
    - If processing is greater than 30 days, a letter should be sent notifying the requestor of the delay.
- ROI staff auditing
  - Request processing
  - Customer service
  - Monitoring productivity, turnaround times, and backlogs
- Invoicing and collections
  - Once the request has been processed, where does the responsibility of collection of revenue fall?
  - Evaluation of time for the collections process. Will the HIM department own this process, or will there be a partnership with their business office?

RELEASE OF INFORMATION OUTSOURCING

In today's vendor environment, there are many models available that can be easily tailored to a healthcare entity's needs. When reviewing the option to outsource, the first step is to evaluate internal processes and determine the direction best suited for the organization. The specific outsourcing models listed below may be modified to meet needs and ensure the partnership between your entity and the outsourcing vendor is successful. Be aware that even though the following models are named, depending on the vendor, the name of the service may be different, but with the core responsibilities listed in the description they still are essentially the same.

Full-Service Model:
In this model, the vendor performs all ROI functions, such as sending and receiving mail and faxes, handling walk-in requests, collections, and more. The ROI staff are hired, trained, paid, and managed by the outsourcing company. This model can be modified per the healthcare entity needs. The vendor is generally on-site daily with this model. The full service model normally includes the following items:

- Data entry of all requests
- Review of the authorization to validate HIPAA/state compliance
- Creation of status letters
- Chart retrieval
- Completion of the requests
- Invoicing and collections, if one is generated
- Continuous quality monitoring of PHI released
- Customer service and handling walk-in requestors

Blended/Dual Model:
This model combines the ROI functions between the healthcare entity and the outsourcing company. It is a modified version of the full-service model mentioned above, with the healthcare entity normally responsible for fax and patient walk-ins. The outsourcing company will still provide software, on-site staff, training and management for their on-site staff and all necessary "back-end" services.

Off-Site/Technology/Back-end Model (Revenue Share):
Some outsourcing companies also have an off-site model. This model requires that the healthcare entity staff complete all "front end" ROI functions, including but not limited to opening mail, data entry of the request into the vendor's software system, retrieving charts, validating authorization. The outsourcing company provides the "back end" service, which may include software, additional QA, mailing paper records, and/or uploading records electronically to the requestor, and all collection duties. The PHI is typically scanned and sent from the facility to an off-site print center. The outsourcing company then "shares" the revenue collected with the healthcare entity.

RELEASE OF INFORMATION AND RETENTION

HIM professionals should review their state guidelines and organizational policies for potential retention requirements for release of information logs and authorizations.

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

Logs:
Many types of logs may be used to record and monitor request-processing activities. Some healthcare entities may have a log that is created by using a simple database or spreadsheet program or some may use an electronic log provided as part of an ROI vendor program. Others may use the actual authorization as their log. The type of log referred to here is for management of the ROI process, not the accounting of disclosures function (discussed later in the federal and state laws section). As there are no specific federal laws governing these types of logs, the retention of these would be in accordance to any state laws or hospital retention policy that may exist.

Authorizations:
Most healthcare entities file the authorization with the patient record whether paper, hybrid, or electronic. The authorizations are then retained in accordance with State laws or hospital retention policies. Some entities utilize actual authorizations as the required HIPAA accounting of disclosure log. If that is the direction your specific entity utilizes, it is recommended the actual authorization is maintained for six years, which is the required reporting time for HIPAA.

AHIMA Practice Brief

In February 2012, AHIMA updated the "Management Practices for Release of Information" practice brief, which is an invaluable resource in providing guidance to help determine which type of ROI model works best based on organizational types and needs. The practice brief can be found at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049364.hcsp?dDocName=bok1_049364.

FEDERAL AND STATE LAWS

Federal and state laws impact the processing of PHI requests in numerous ways and are the root cause of much 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 manager 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." Federal laws and state laws should both be complied with when possible, but it is imperative to understand where preemption applies and when.

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 take into account 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.

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, but CLIA is exempt from this rule. As a result, the individual's right to access test results directly from a clinical laboratory generally depends on whether state law permits such access. Please follow state law for release of test results directly to patients.

Note: As of the publication date of this toolkit, changes to CLIA were still in a proposed rule status. The suggested changes would give patients access to their lab results directly from the laboratory. For more information please visit federalregister.gov/articles/2011/09/14/2011-23525/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports.

ADDITIONAL RESOURCES:

- CMS Memorandum on Clinical Laboratory Improvement Amendments of 1988 (CLIA)—Issuance of Revised Survey Procedures and Interpretive Guidelines: cdc.gov/cliac/pdf/Addenda/cliac0811/U_addendum_CMS_SCLetter10_12.pdf
- Health IT Buzz: "Electronic Health Records (EHR)s Now Permitted By CLIA": healthit.gov/buzz-blog/privacy-and-security-of-ehrs/electronic-health-records-ehrs-permitted-clia/
- *Federal Register:* CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports federalregister.gov/articles/2011/09/14/2011-23525/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports
- HealthIT.gov summary of health IT rules and regulations: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__regulations_and_guidance/1496

E-Discovery

The term e-discovery (electronic discovery) is often used to refer to the 2006 amendments to the Federal Rules of Civil Procedure.[23] These 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 re-evaluate the management of electronically stored information. Today, this means an organization must consider not only the ESI stored in workstations, servers, e-document management systems, and the like, but also on mobile devices used by clinicians, USB drives, and other forms of electronic storage media.[24]

Furthermore, an essential part of responsible information stewardship is an awareness of what **metadata** exists.[25] In other words, what data exists about the data being stored (for example, when it was created and by whom it was created). This helps to place the ESI within the context of why it was created in the first place. 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.

For more information about e-discovery, refer to these resources:

- Baldwin-Stried Reich, Kim. "Trends in E-Discovery: Four Cases Provide a Glimpse of Healthcare Litigation's Future." *Journal of AHIMA* 83, no. 5 (May 2012): 44–46.
- AHIMA. "Mandates Encourage E-Discovery." *Journal of AHIMA* 83, no. 5 (May 2012): 68.
- AHIMA e-HIM Work Group on e-Discovery. "New Electronic Discovery Civil Rule." *Journal of AHIMA* 77, no. 8 (September 2006): 68A–H.
- *eDiscoveryJournal:* http://ediscoveryjournal.com/

AHIMA's guidance on "Litigation Response Planning and Policies for E-Discovery" identifies five key steps to developing a litigation response plan and process:

- Conduct an evaluation of applicable rules
- Identify a litigation response team
- Analyze issues, risks, and challenges
- Develop organizational policy and procedures
- Develop a system for ongoing monitoring and evolution

For more information on developing a litigation response plan and policies for e-discovery, refer to: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_036581.hcsp?dDocName=bok1_036581

Healthcare organizations should consider the following when developing ESI policies:

1. Identify all ESI that exists. This may be done by way of a survey of IT and HIM personnel to collect the basic information. At a minimum, understand the following:
   - The types and sources of accessible and inaccessible ESI
   - Industry-specific or other peculiar application software and file formats being used or used in the recent past, including non-readable or software generated "operating" or "background" files not normally accessed by the user. Non-readable files are typically accessible and are considered ESI.
   - License agreements for software applications that might restrict the copying or production of ESI
   - At what point is ESI truly deleted? When can ESI no longer be restored?

2. Implement an ESI retention policy as part of an overall document retention policy. Suggested ESI document retention policy checklist:
   - An inventory of the types of ESI that exist
   - What sources possess ESI? (e.g., systems, departments, employee position titles)
   - What ESI is stored?
   - How and where is ESI stored?
   - How long is each type of ESI stored?
   - How is ESI to be destroyed?
   - When and how is ESI destruction to be suspended?
   - Set employee discipline for noncompliance
   - Document the compliance training of employees
   - Require employees to sign policy acknowledgment annually to coincide with performance evaluation
   - Monitor or audit policy compliance
   - Review policy annually and update as needed
3. Designate IT or HIM personnel as e-discovery witnesses who are knowledgeable about the computer systems.

Freedom of Information Act (FOIA)
The FOIA took effect in 1967 and is often described as the law that allows citizens to know about their government. As noted by the United States Supreme Court, "The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[27]

The FOIA provides:

…that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. A FOIA request can be made for any agency record.[28]

Today, each federal agency's website is required to provide information on the type of records maintained by that agency and the means by which such records may be requested. The agencies must disclose the information requested except when it is protected from public disclosure.

FOIA Implications Related to Protected Health Information

Since the FOIA applies to federal agencies, it is highly unlikely a HIM professional in most healthcare settings would ever encounter a FOIA request for PHI. There are other laws, such as the USA PATRIOT Act, which are more applicable for compelling a disclosure of PHI from healthcare providers. And the HIPAA Privacy Rule accommodates such lawful requests under §164.512(a).

For an excellent review of certain federal laws and their impact on PHI disclosure, be sure to read the AHIMA Practice Brief "Homeland Security Act, Patriot Act, Freedom of Information Act, and HIM" (updated November 2010). This can be found in the AHIMA Body of Knowledge at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048641.hcsp?dDocName=bok1_048641

Federal Educational Rights and Privacy Act (FERPA)
FERPA was originally passed in 1974 and has been amended several times since then, most recently in 2001. The act protects the privacy of students' educational records of virtually any public or private educational institution or public agency that directly receives funds under any program administered by the US Department of Education (DoE). Most elementary and secondary school levels do not receive DoE funding and thus, those particular schools are not subject to FERPA.

Note: Organizations that do not electronically bill for healthcare services are not HIPAA-covered entities.

While not all student health centers (like those found on college campuses) are HIPAA-covered entities, virtually all of them are covered by FERPA. At those schools where a student health center must be compliant with both HIPAA and FERPA, there can be real challenges in balancing those two statutes. The DoE and Department of HHS have provided a "Joint Guidance" document on how to apply the rules associated with each statute.[29] This document is presented in a helpful Q&A format.

When these two rules are in occasional conflict in using or disclosing patient (student) health information, many people assume that HIPAA would supersede FERPA, and they would be wrong to take that as a general principle. The issues at stake are that a violation of FERPA could endanger the school's ability to grant financial aid; it also could endanger the federal funding stream (for example, research grants) for that university, which in some cases could be tens of millions of dollars. Thus, it is important to understand these rules, how they intersect, and how they differ.

Health Insurance Portability and Accountability Act's (HIPAA's) Privacy Rule
The HIPAA Privacy Rule is at the heart of all ROI processes because it is the federal law that sets the floor for privacy protections of PHI. It is discussed throughout this toolkit because its relevance is substantial. The HIPAA Privacy Rule is part of the federal law under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and was implemented in April 2003. The rule applies to covered entities, which are health plans, healthcare clearinghouses, and healthcare providers that transmit specific information electronically. One of the key purposes of the Privacy Rule is to address the fact that state laws vary considerably especially as they pertain to health information protections, patient rights and disclosure rules. 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 protected health information in its possession. Section 164.508 of the HIPAA final 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.

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
- 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 authorization 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: Regarding proof-of-authority legal documents such as guardianships (vs. conservatorship), 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 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. Patients also have the right to ask for a restriction of disclosure to a health plan for a service paid in full out of pocket, and the provider must accept the request.

2. 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.

3. 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.

Content 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. Therefore, covered entities may want to consider printing their authorization form on multiple-part paper (carbon or carbonless) and listing the distribution of the various copies on the front page. For example, text on the authorization form might indicate that the top copy is to be maintained by the covered entity, the second copy is to be given to the individual, and the third copy is to accompany any disclosure of protected health information.

Compound Authorizations: An authorization may be combined with another document to create a compound authorization only as 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, including the consent to participate in the research or another authorization to disclose protected health information from the research.
  Note: The HITECH Final Rule makes changes to the use of compound authorizations in research. Refer to the HITECH topic of this section for further details.
- Psychotherapy notes: An authorization for the use or disclosure of psychotherapy notes may be combined with another authorization for the use or disclosure of psychotherapy notes. For example, an individual can complete an authorization that requests his psychotherapy notes be sent to his attorney and a second mental health professional. 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 for the disclosure of general health information. However, a general authorization that conditions treatment, payment, enrollment, or eligibility for benefits on completion may not be combined with another authorization. For example, an insurance company may not combine an authorization they require as a condition of enrolling in their plan with another authorization.

For more information on an invalid or unacceptable consent, as well as other laws impacting a disclosure, refer to Appendix J.

Alternative Means of Communications
Healthcare providers must also accommodate reasonable requests for alternative means of communications and may not condition the accommodation on the basis of an explanation from the individual (164.522(b)(1)(I) and (2) (iii)). Health plans, in turn, must accommodate reasonable requests if the individual clearly states that the disclosures of all or part of the information could endanger the individual, and the plan may condition the accommodation on the receipt of such a statement in writing. If a request for a "reasonable alternative method of communication" is received, the individual requesting this must provide the alternative location, address, or telephone number or the alternative means of communication and be responsible for and explain how payment will be handled for any additional cost associated with the requested alternative method of communication.

Minimum Necessary
Minimum necessary is a key component of the HIPAA Privacy Rule. Minimum necessary requires healthcare entities to appraise current practices and enhance safeguards in order to limit disclosure of PHI and inappropriate access. Minimum necessary is based on PHI not used or disclosed unnecessarily to gratify particular purposes or carry out any functions. In order to do this healthcare entities are required to take reasonable measures to limit use or disclosure of PHI to that which is necessary to carry out the intended use of the PHI. Each healthcare facility must have policies and procedures to identify who should have access to PHI so their job task can be performed. The Final Rule as published on January 25, 2013, now extends the minimum necessary rule to business associates.

Business associates must now apply this standard in a way that is consistent with the covered entity's practices and in keeping with the business associate agreement.

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.[30] The AoD need not include disclosures related to treatment, payment, and healthcare operations (TPO). 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. For a sample accounting log, visit http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_009496.hcsp?dDocName=bok1_009496

The Office for Civil Rights (OCR) currently has a notice of proposed rulemaking (NPRM) out to update the requirements of AoD under HIPAA. However, at time of publication, the final rule had not yet been issued.

Law Enforcement
When HIPAA was enacted in 2003, it changed the way PHI is released to unauthorized persons including law enforcement agencies, putting control back in the hands of the individual allowing them to decide if they want their PHI released.

Exceptions to this rule do allow for the information to be released if it meets the following requirements:

- Release is mandatory to report injuries such as gunshot or stab wounds
- Response to judicial officer by subpoena, court order, warrant, summons or investigative demand
- For locating a suspect, fugitive, witness, or missing person if the victim cannot consent due to emergency when it would affect the investigation
- If a person has died due to a criminal act
- If the PHI is evidence of criminal conduct
- If it is averting a serious threat to the health and safety of the public
- To provide medical care to those in custody at a correctional facility or to protect the health and safety of employees and others

Since violations of these HIPAA regulations could result in penalties, the AHIMA Body of Knowledge provides a sample checklist for disclosing to law enforcement including a sample consent form.[31,32]

RECOMMENDED PRACTICES:

- Create a detailed policy and procedure on disclosing information to law enforcement agencies
- Educate staff on disclosure of such information including strict adherence
- Be sure consent form is compliant with law enforcement requirements

Additional legal resources include the Health Privacy Project website at www.cdt.org/issue/health-privacy and www.alllaw.com/state_resources/.

The Health Information Technology for Economic and Clinical Health Act (HITECH)

The American Recovery and Reinvestment Act (ARRA) was signed into law in 2009. The Health Information Technology for Economic and Clinical Health Act (HITECH) is a defined section of ARRA that deals exclusively with health information communication and technology. Changes to HITECH as made in the final rule are made effective on March 26, 2013, with the compliance date set at September 23, 2013.

Note: The Final Rule changes the definition of business associate to include subcontractors, patient safety organizations, health information organizations (HIOs), and certain personal health record (PHR) vendors.

Listed below are some of the changes that will affect disclosures of PHI as a result of the final HITECH Rule. For full compliance details of each topic, refer to the AHIMA analysis document. The pages of the analysis for each topic listed have been provided for convenience. The document can be found at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050067.pdf.

- Business Associate (page 5, 14–16)
- Marketing (pages 13–14)
- Sale of PHI (page 17)
- Compound authorizations—research (page 17–18)
- Access to decedent's records (pages 18–19)
- Immunizations (page 19)
- Restrictions (pages 22–23)
- Electronic access (pages 23–24)

Note: The final rule removes the 60-day time limit to respond to requests for access for records stored off site. Under the final rule, all requests must be responded to within 30 days regardless of record location or media type. The one time 30-day extension remains.

Genetic Information Nondiscrimination Act (GINA)

In 2008, the president signed into law the GINA, which expands on the provisions in HIPAA to protect Americans against discrimination based on their genetic information when it comes to health insurance and employment. The long-awaited measure, which had been debated in Congress for 13 years, paved the way for people to take full advantage of the promise of personalized medicine without fear of discrimination. In the final rule, health information includes genetic information. Health plans and insurers are prohibited from imposing a preexisting condition exclusion based solely on genetic information and from discriminating in individual eligibility, benefits, or premiums based on any health factor, including genetic information. GINA expands such protections in a number of ways:

- Group health plans and health insurers cannot base healthcare premiums for plans or a group of similarly situated individuals on genetic information
- Plans and insurers are prohibited from requesting or requiring an individual to undergo a genetic test
- Plans and insurers are prohibited from collecting genetic information (including family medical history) prior to or in connection with enrollment, or for underwriting purposes[33]

Health plans and insurers that perform underwriting (excluding those that issue long-term care policies) must state in their notice of privacy practices that they are prohibited from use or disclosure of genetic information. Another exception is that health plans are permitted to use or disclose minimum necessary genetic information for determination if the provision of particular benefits is medically necessary.

Patriot Act

The "Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act" (USA PATRIOT Act) was signed into law on October 26, 2001.[34]

The PATRIOT Act is primarily a vehicle for the US government to enhance its ability to monitor and detect activities that may indicate support for terrorism. The act is not necessarily targeted at protected health information (PHI) or systems that create, store, or manage such information. Nonetheless, it is conceivable that in pursuit of investigations being conducted under this act, a demand for PHI may be made of any healthcare provider who would be expected to comply AND who would be prevented from informing the subject of the investigation, (that is, the patient).

With regards to such investigations, HIPAA actually intersects with the PATRIOT Act under the section titled, "Uses and disclosures for which an authorization or opportunity to agree or object is not required" to wit, allowing government agencies to compel a covered entity to provide certain information without the covered entity being required to notify a patient and giving him or her an opportunity to object.[35]

Privacy Act

The Privacy Act of 1974, 5 U.S.C. § 552a, has been described as an "omnibus 'code of fair information practices' that attempts to regulate the collection, maintenance, use and dissemination of personal information by federal executive branch agencies." [36]

Basically, this means that individual citizens have a right to know what their government's executive branch agencies know about them, and how that information is used and disclosed. The act prohibits disclosure of an individual's information without the individual's consent, unless the disclosure is made in response to one of twelve statutory exceptions.[37] The act also allows for citizens to seek access to and amend their records as maintained by a particular agency. Each agency is to provide a list of the record systems in which an individual's records may be maintained. As an example, this link provides the systems list for the US Department of Justice (DOJ): justice.gov/opcl/privacyact.html

An additional resource about the Privacy Act would be this "Overview" as compiled by the USDOJ: justice.gov/opcl/1974privacyact-overview.htm

United States Code (USC) Title 42

Title 42 is a broad law that covers a wide variety of matters essential to protecting the constitutional rights of US citizens as well as establishing the authority of the Public Health Service, and even addressing intercountry adoptions.

For the purpose of this toolkit, there are several provisions of Title 42 that address privacy, for example:

- The Public Health Service must protect the privacy of individuals who are the subject of research by withholding from all persons not connected with the conduct of the research the names or other identifying characteristics of these individuals. Persons authorized to protect the privacy of these individuals may not be compelled in any federal, state, or local civil, criminal, administrative, legislative, or other proceedings to identify these individuals.
- The identity of donors to and patients of cord blood banks and bone marrow centers are strictly protected.
- Establishing requirements for privacy and informed consent of patients tracked through a nationwide pediatric cancer registry.
- That the Congenital Heart Disease Surveillance System is operated in a manner that complies with the HIPAA privacy provisions.

Title 42 contains language that specifically prohibits a preemption of any state law or regulation that impose additional privacy protections. Further, it does not supersede any federal privacy requirements, including HIPAA regulations. Basically, any patient data or information collected pursuant to programs covered by Title 42 should only be disclosed under proper authorization. While no specific authorization format or content specifications could be found within Title 42, it is recommended that a HIPAA-compliant authorization be obtained before any such disclosures are made.

Additional resources that may be useful in researching Title 42:

- Findlaw.com: http://codes.lp.findlaw.com/uscode/42
- US House of Representatives Downloadable US Code: http://uscode.house.gov/download/title_42.shtml

STATE LAWS

As stated numerous times throughout the toolkit, state laws vary and must be taken into account with federal laws when ensuring compliance is met for disclosures of PHI. The following resources can be used to identify some state specific requirements. The best practice is to always follow the more restrictive regulatory guidelines when releasing information.

Refer to AHIMA's practice brief, "Preemption of the HIPAA Privacy Rule," at http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048022.hcsp?dDocName=bok1_048022.

For more information on requesting personal health records, as well as process, tips, authorizations, fees, conflicting state laws, and requesting records on behalf of others, refer to *Journal of AHIMA*, "How to Request Your Medical Records," March 01, 2012. by Chris Dimick at http://journal.ahima.org/2012/03/01/how-to-request-your-medical-records/.

The state and federal consent laws affecting interstate health information exchange provides additional information on consent laws, legal and federal standards, interstate HIEs, and case studies at nga.org/cms/home/nga-center-for-best-practices/center-publications/page-health-publications/col2-content/main-content-list/state-and-federal-consent-laws-a.html.

RECOMMENDED PRACTICES

Develop policies and procedures based on state laws and applicable federal laws for releasing information, including any links or references.

SENSITIVE HEALTH INFORMATION

Sensitive health information, which includes HIV/AIDS, behavioral/mental health, and substance abuse information, is an area that has raised great debate and concern. The HIPAA Privacy Rule states that all individually identifiable health information is sensitive and equally deserving of protection. The sensitivity of patient information is subjective and varies depending on the individual's situation and the context of the information. Sensitive health information is information that carries high risks when disclosed, including social stigma, discrimination and even physical harm for certain diagnoses or conditions such as HIV/AIDS, behavioral and mental health, and substance abuse.

Facilities must have policies and procedures in accordance with their state law to address any of the areas of sensitivity relating to their privacy, protection and disclosure of sensitive information. As with all areas addressed, violations cannot only have serious penalties, but also loss of funds and services.

HIV/AIDS

HIV/AIDS is an area where healthcare providers need to balance the individual's privacy and protection and the public's need to know. In addition, the consent form must specifically indicate what sensitive information can be released and to whom it may be released.

Additional resource that may be useful:
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048022.hcsp?dDocName=bok1_048022

Sexually transmitted disease (STD), previously known as venereal disease, is spread through sexual contact, sometimes causing personal and social stigmas. Health information pertaining to STDs is protected by federal laws, and state laws mandate healthcare providers report STDs to the state's health department. Under HIPAA public safety regulations, a covered entity may use or disclose this information without a written consent or authorization of the individual.[38] Each state's regulations must be reviewed to determine if a consent or authorization is required. Regardless, each state has a required form for reporting these diseases. More information on reporting STDs and frequently asked questions can be found at health.state.mn.us/divs/idepc/dtopics/stds/frequentlyasked.html.

Substance Abuse
Substance abuse records are another area that is protected by federal law. The Federal Drug Abuse Act, 42 U.S.C. § 290ee-3(a) and CFR 42 Part 2, specify that records relating to the identity, diagnosis, prognosis, or treatment relating to alcohol or drug abuse are confidential and should only be disclosed as expressly authorized by these statutes. Records should only be disclosed with written authorization of the individual, legal representative or upon a valid signed court order. The following link is for the HHS site that provides more information on HIPAA: hhs.gov/ocr/privacy/hipaa/faq/index.html

Psychotherapy Notes:
The HIPAA privacy rule 45 CFR 164.501 defines psychotherapy notes as notes recorded in any medium by a mental health professional 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.[39]

RECOMMENDED PRACTICES

- Review all practices to ensure confidentiality is being maintained
- Update and review all policies and procedures per the organization's guidelines
- Educate staff on policy and procedures and proper completion of authorization

Minors
Under the privacy rule of HIPAA, parents 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. 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.[40]

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.

Finally, as is the case with respect to all personal representatives under the privacy rule, a provider may choose not to treat a parent as a personal representative when the provider reasonably believes, in his or her professional judgment, that the child 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.

Emancipation of a Minor:
State laws will stipulate the means by which a minor becomes emancipated. Typically, a minor may become emancipated through:

1. 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
2. Marriage
3. Actively serving in the military

Stepparents:

- Stepparents usually 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 concern and difficulty 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.

ASSOCIATED COSTS

PAPER VS. ELECTRONIC MEDIA

In today's healthcare settings, various types of media are available for creating, storing, and releasing PHI to various types of requestors. Essentially, the methodology in releasing the information, (that is, training of staff, quality assurance processes, and the like, are the same, regardless as to the media used to release PHI). To determine the charge methodology that is considered reasonable for requests, the first action is to determine the type of media the recipient of the information has requested.

Paper:
To release information either from paper to paper, or electronic to paper, the best practice is to research the covered entity's state law to determine the appropriate charges. As per HIPAA, a patient may not be charged a retrieval fee. Thus, the covered entity may not charge a patient the base fee stated within the regulation, but instead simply revert to the per page fee allowed by the covered entity's state statute. For example, if a specific state statute allows a retrieval fee of $18 for the first 5 pages, then $0.85 for pages 6-50, and $0.60 for page 51 up, the covered entity should only charge the patient the per page fee, which would be $0.85 for pages 1–50, then $0.60 for pages 51 and up.[41]

Electronic Media Charges:

Patients:

The HITECH Final Rule, 164.524(e) of title 45, Code of Federal Regulations, "Access of Individual to Protected Health Information," states that in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual:

> (1) the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific; and
> (2) notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form *shall not be greater than the entity's labor costs* in responding to the request for the copy (or summary or explanation).

The HITECH final rule still does not clearly define what an entity may incorporate as their "labor cost." It is recommended to review the costs absorbed by the department to produce copies of PHI. The final rule states that if the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form; (ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (iii) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(ii) of this section.[42] Wherever the final rule references labor costs, the organization may wish to consider including direct labor, training, management/supervisors (outsourced and internal staff) in determining their labor cost, until further clarification is provided from the federal government.

Attorneys, Insurance Companies, and Other

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 revert to the standard rates that are applicable for paper copies.

Recommended Practices

- State regulations should be researched to determine if a statute for charges of paper and/or electronic media applies.
- When retrieval fees are not allowed, use the per page or digital image fee allowed by the covered entity's state statute. See Appendix L for examples of when to charge and when not to charge.
- Assess the costs associated with either providing copies of medical records in either a paper or electronic format. See Appendix M for a list of potential costs to be considered when disclosing PHI.

Accounting of Disclosures

As stated earlier, the HIPAA Privacy Rule gives individuals the right to request an accounting of disclosures for their PHI by a covered entity. 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.[43]

In a random survey, conducted while preparing this toolkit, 25 HIM professionals responded that they had received very few, if any, requests for a first accounting of disclosure and none had received a second request for an accounting by the same individual within a 12-month period.

- Most responded that if they would receive a second request, they would follow their state laws and charge the same fees as allowed for release of information.
- Several others responded that they would charge a flat fee ranging from $15 to $25 and compared the accounting to preparing a summary of the record.
- A few indicated that subsequent requests are on a cost-based fee but they have never developed the actual fee since they have not received a second request. One stated that although they have never established exactly what that fee would be, because it is a very labor-intensive process, they would most likely develop an algorithm that could be used so that the actual costs could be entered with a resultant reasonable, cost-based fee.

Recommended Practices

- Follow state laws and charge the same fees as allowed for release of information. Perform a test review of receiving and processing a second request to determine whether the state fees are acceptable or whether a higher fee is indicated based on the labor intensive process.

References to State Information

Because the requirements of the HIPAA privacy rule do not address charging for record copy requests other than from patients, state regulations continue to provide the most specific guidelines. OCR has further explained that each covered entity (such as, healthcare organization) should determine reasonable cost-based fees for its own operations.

State health authorities are the most dependable resource for current state allowable copy fees, because state laws change periodically.

- Many states have government websites that may post laws related to healthcare. These sites typically have URLs such as http://www.statename.gov
    - These websites may have the contact information of state representatives who can be used as resources for further information.
- The law offices of Thomas J. Lamb, P.A., have compiled an online state-by-state reference to copy fees at http://www.lamblawoffice.com/medical-records-copying-charges.html. This website provides specific state statutes that oversee copy charges for further research.

Recommended Practices

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

- Become knowledgeable about the HIPAA privacy law, as well as any other federal and state laws and regulations addressing the patient's right to access and acquire copies of his or her health records. A good reference site is hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.
- Check your state government website annually for any updates or changes to copying charges.
- Avoid listing current charges for copies of medical records within your organization's policies and procedures unless it is referenced in a charge sheet as an attachment.
- Consider the factors that affect the cost of release of information to patient: labor, equipment, space, and material costs associated with reviewing or copying records. For more specific information, please refer to Appendix L.

LEGAL DOCUMENTS

Legal documents may or may not accompany a request for PHI. 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 and timely response. This section provides a breakdown of the different types of legal documents that can be involved in the request for PHI.

Subpoenas and Court Orders:
Courts may issue subpoenas as a means of discovery, (that is 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). 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 quash the subpoena and request, in its place, a court order. HIM professionals will most commonly encounter two different types of subpoenas:

- *Subpoena Duces Tecum*—mandates them 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:

- 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 who is being subpoenaed
- A specific date, time and location for appearance or for the record custodian to provide the requested materials
- In some cases, the penalty for non compliance will be included[44]

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 the case.[45] 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 occasions 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.

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, before complying with the subpoena, the covered entity must "receive evidence that reasonable efforts were made to either:

- 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 to
- Seek a qualified protective order for the information from the court."46 If the entity receives an authorization with the subpoena, then the HIPAA requirement is met.

Whenever the HIM professional does appear in court, she must never interpret the medical records being presented to the court. The only testimony concerning the records that should be offered is that they were maintained in the normal course of business.

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.[47]

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 make a determination 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 government will convene a grand jury to hear the evidence in all such cases.[48]

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

Court-Martial:
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. For example, Military Rule of Evidence 513 provides that, "a patient has a privilege to refuse to disclose and to prevent any other person from disclosing a confidential communication made between the patient and psychotherapist."[49]

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, the HIM professional should remain courteous and not resist or interfere with the officer's search. Legal counsel should immediately be notified along with the facility's administrative officers. It is appropriate to take notes such as 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 HIM 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" and is made under an oath or affirmation administered by someone authorized to do so under law, such a court clerk or a notary.[50]

HIM professionals may encounter the use of affidavits in two ways.

1. When the production of PHI has been ordered by a court but the HIM professional is not expected to personally provide the PHI in court, the HIM 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.

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

- How did the HIM 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?[51]
  Note: In long-term care facilities, it is common for the director of nursing to be the one making such presentations at depositions.

Interrogatories:
Another form of pre-trial discovery is the issuance of interrogatories. These are "sets of written questions served on the one party to another in civil litigation. They are an extraordinarily useful tool for obtaining information in discovery. With regard to EHRs and HIEs, the HIM and IT manager may be asked to testify about the 'good faith' operations of their organization's information systems."[52]

In Camera Requests:
In camera is a legal term meaning "in private," as within the judge's private chamber. This setting enables the judge and attorneys for both sides in a lawsuit to meet in private away from the jury and discuss legal matters, such as the appropriateness of a subpoena or court order for production of medical or psychiatric records. Depending upon the type of PHI requested, the HIM professional may choose to request an in-camera discussion with the attorneys and the judge. Legal counsel should always be consulted before making such a request to ensure it is appropriate and to receive guidance on how to make the request.

RECOMMENDED PRACTICES:

- Never ignore a legal document (such as subpoena, 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 the format of documentation that would be satisfactory to comply with the legal document (for example, hard copy documents, documents scanned onto compact disks).
- 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 that are stored off site or are under the control of other entities. 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:

- Federal Rules of Civil Procedure. Rule 45: Subpoena. http://www.law.cornell.edu/rules/frcp/rule_45.
- US Department of Defense. "DoD Health Information Privacy Regulation." January 2003. dtic.mil/whs/directives/corres/pdf/602518r.pdf

Notes

1. Dunn, R., and S. Edelstein. *The Practical Guide to Release of Information*. Marblehead, MA: HCPro, 2008. p. 1.
2. "Healthcare provider" subject to the security rule includes all healthcare providers, regardless of practice size, provided that they transmit health information electronically. The specific electronic transactions subject to this rule are those that are covered under the HIPAA Transactions Rule. Providers subject to the privacy rule include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies, according to www.HRSA.gov.
3. Department of Health and Human Services (HHS). "Administrative Data Standards and Related Requirements: Definitions." *Code of Federal Regulations*, 2003. 45 CFR, Part 164, Section 103.
4. Ibid.
5. HHS. "Administrative Data Standards and Related Requirements: Organizational Requirements." *Code of Federal Regulations*, 2003. 45 CFR, Part 164, Section 105.
6. For a complete list of identifiers qualifying as individually identifiable health information, see the Centers for Disease Control, "HIPAA Privacy Rule and Public Health: Guidance from CDC and the US Department of Health and Human Services," cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm.
7. "Family educational and privacy rights." US Code Title 20, Chapter 31, Subchapter III, part 4, 1232g (1974).
8. "Family educational and privacy rights." US Code Title 20, Chapter 31, Subchapter III, part 4, 1232g (a)(4)(B)(iv) (1974).
9. HHS. "Administrative Data Standards and Related Requirements: Definitions."
10. A designated record set is a group of records maintained by or for a covered entity that is the medical and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; information used in whole or in part by or for the HIPAA covered entity to make decisions about individuals, according to www.ahima.org.
11. HHS. "Permitted Use and Disclosure FAQs." hhs.gov/hipaafaq/permitted/index.html.
12. HHS. "Administrative Data Standards and Related Requirements: Definitions."
13. HHS, National Institutes of Health. "How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?" http://privacyruleandresearch.nih.gov/pr_08.asp.
14. The notice of privacy practices will include examples of disclosures and uses of data that will occur for purposes of treatment, payment, and operations.
15. AHIMA. "Understanding the HIE Landscape." *Journal of AHIMA* 81, no. 9 (Sept 2010): 60–65.
16. Public Health Service, Department of Health and Human Services. "Confidentiality of Alcohol and Drug Abuse Patient Records." *Code of Federal Regulations*, 2000. 42 CFR, Chapter I, Part 2.
17. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Privacy of Individually Identifiable Health Information: Administrative Requirements." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 530.

18. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Security and Privacy: Uses and Disclosures for Which an Authorization Is Required." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 508.

19. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR parts 160 and 162. *Federal Register 67, no. 157* (August 14, 2002).

20. AHIMA e-HIM Work Group on the Legal Health Record. "Update: Guidelines for Defining the Legal Health Record for Disclosure Purposes." *Journal of AHIMA* 76, no. 8 (Sept. 2005): 64A–G.

21. Ibid.

22. HHS. "Health Information Privacy: Uses and Disclosures for Treatment, Payment, and Health Care Operations." hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usesanddisclosuresfortpo.html2

23. Federal Rules of Civil Procedure. December 1, 2010. uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Civil%20Procedure.pdf.

24. Washington, Lydia. "Managing Health Information in Mobile Devices." *Journal of AHIMA* 83, no. 7 (July 2012): 58-60.

25. Schodde, Gregory. "E-discovery: Collect metadata to avoid ESI headaches." InsideCounsel.com, October 12, 2012. insidecounsel.com/2012/10/12/e-discovery-collect-metadata-to-avoid-esi-headache.

26. AHIMA. "Information Integrity in the EHR." AHIMA Toolkit, 2012.

27. *NLRB v. Robbins Tire Co.,* 437 U.S. 214 (1978).

28. US Department of Justice. "What is FOIA?" foia.gov/about.html

29. HHS and US Department of Education. "Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records." November 2008. 2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf.

30. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Security and Privacy: Accounting of disclosures of protected health information." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 528(a)(1).

31. Brandt & Associates. "Checklist for Disclosures to Law Enforcement Officers under the HIPAA Privacy Regulations." http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_027624.pdf.

32. Brandt & Associates. "Law Enforcement Request for Records." http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_027625.pdf

33. US Department of Labor. "Your Genetic Information and Your Health Plan–Know The Protections Against Discrimination." dol.gov/ebsa/publications/gina.html.

34. Public Law 107-56, 107th Cong. (Oct. 26, 2001), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001. gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

35. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Security and Privacy: Uses and disclosures for which an authorization or opportunity to agree or object is not required." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 512(f)(1)(ii)(A) and (C).

36. US Department of Justice. "Overview of the Privacy Act of 1974: Introduction." justice.gov/opcl/privacyactoverview2012/1974intro.htm.

37. US Department of Justice. "Overview of the Privacy Act of 1974: Twelve Exceptions to the 'No Disclosure without Consent' Rule." justice.gov/opcl/privacyactoverview2012/1974condis.htm#exceptions

38. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Security and Privacy: Uses and disclosures for which an authorization or opportunity to agree or object is not required." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 512(a).

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

40. HHS. "HIPAA Frequent Questions: Does the HIPAA Privacy Rule allow parents the right to see their children's medical records?" hhs.gov/hipaafaq/personal/227.html.

41. Tennessee Code, Title 68, Chapter 11, Part 3, 68-11-304 (a).

42. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules." *Federal Register*, vol. 78, no. 17 (January 25, 2013), 5702.

43. Department of Health and Human Services. "Administrative Data Standards and Related Requirements: Security and Privacy: Accounting of Disclosures of protected health information." *Code of Federal Regulations*, 2002. 45 CFR, Part 164, Section 528 (c)(ii)(B)(2).

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

45. HHS. "Health Information Privacy: Court Orders and Subpoenas." hhs.gov/ocr/privacy/hipaa/understanding/consumers/courtorders.html.

46. Ibid.

47. Federal Rules of Civil Procedure. Rule 45: Subpoena. law.cornell.edu/rules/frcp/rule_45.

48. University of Dayton School of Law. "Federal Grand Juries." http://campus.udayton.edu/~grandjur/fedj/fedj.htm.

49. US Department of Defense. "Part III, Military Commission Rules of Evidence." defense.gov/pubs/pdfs/Part%20III%20-%20MCREs%20(FINAL).pdf

50. The Free Dictionary. "Affidavit." http://legal-dictionary.thefreedictionary.com/affidavit.

51. 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.

52. Baldwin-Stried Reich, Kimberly A. "Sorting out Discovery Requests." *Journal of AHIMA* 81, no. 10 (October 2010): 60–62.

References

AHIMA. "Analysis of Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rule." January 25, 2013. http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050067.pdf

Brandt, Mary D. *Release and Disclosure: Guidelines Regarding Maintenance and Disclosure of Health Information*. Chicago, IL: American Health Information Management Association, 1997.

Hughes, Gwen, and Cheryl Smith. *Required Content for Authorizations to Disclose.* Chicago, IL: American Health Information Management Association, 2002.

APPENDIX A
GLOSSARY OF TERMS

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 this changes to include these disclosures; awaiting final regulations.

Agency for Healthcare Research and Quality (AHRQ): The branch of the US Public Health Service that supports general health research and distributes research findings and treatment guidelines with the goal of improving the quality, appropriateness, and effectiveness of healthcare services.

Agent: A person who is authorized to act for another (the agent's principal) through employment, by contract or apparent authority. The importance is that the agent can bind the principal by contract or create liability if he/she causes injury while in the scope of the agency. Who is an agent and what is his/her authority are often difficult and crucial factual issues.

The American Recovery and Reinvestment Act (ARRA): An economic stimulus package enacted by the 111th United States Congress in February 2009; signed into law by President Obama on February 17, 2009; to preserve and improve affordable healthcare and protect those in greatest need by strengthening privacy and security.

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 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 ARRA.

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.

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

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

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.

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, disclosures, and requests: Three types of situations in which personal health information is handled: use, which is internal to a covered entity or its business associate; disclosure, which is the dissemination of PHI from a covered entity or its business associate; and requests for PHI made by a covered entity or its business associate.

APPENDIX B

SAMPLE ROI POLICY AND PROCEDURE

General Disclosure of Protected Health Information

Policy Statement:

Purpose: The medical record is a confidential and privileged document. The medical record is the property of the Organization and is maintained for the benefit of the patient, the medical staff, and the Organization. It is the responsibility of the Organization to safeguard the information in the record against loss, defacement, or use by unauthorized persons. Original medical records shall not be removed from the premises except on a court order, subpoena from a court of law, or statute, and only when accompanied by the Custodian of Medical Records. Any release of PHI to persons not otherwise entitled to receive this information requires the patient's written authorization.

Scope: <enter your entity's name> Health information management (HIM) employees and contracted ROI staff

Policy: Specified HIM and contracted staff are responsible for processing ROI requests based on State and Federal regulation and department procedures listed below

Procedure: ROI Contact Information

<enter your entity's contact information>

Who Processes ROI Requests?

- All requests for PHI received by Organization departments, ancillary services, or nursing staff, will be forwarded to the Health Information Management Services (HIMS) department.
- No PHI will be released by anyone other than HIMS personnel or individuals authorized to do so for emergency medical care purposes.

How Are ROI Requests Received in the HIM Department?

- Mail
  - Mail for ROI will be placed in the Correspondence mailbox.
  - Staple together the request letter and authorization; discard the envelope.
  - If the request or authorization is on less than a full sheet of paper, tape or staple it to a full sheet of paper so it is easy to scan/file.
- Faxes
  - Staple pages together.
  - Faxes are routed to the appropriate staff for completion.
- Telephone
  - Physician office requests are considered continuum of patient care and will be processed as quickly as possible.
  - Customers can be given instructions on how to request copies or can listen to the scripted message on the HIM phone tree.
  - Protected Health Information (PHI) is not given over the telephone.
  - Nursing units requesting copies of medical records by telephone will be informed that:
    - Medical record copies for patients being transferred to another healthcare entity is generally copied by the nursing unit, however, if HIM is asked to do so, we will help.
    - Medical record copies for inpatients currently being treated or at discharge will generally be processed by ROI after discharge.
- Refer to ROI Request Types section below.

Walk-Ins

- Customers that come to the HIM department can complete an authorization that is available at the reception desk.
- Copies from can be generated as time permits while the customer is present and at no charge. If copies of entire visits or charts are requested, follow appropriate turnaround times, and invoice the requestor for payment of copies.

ROI Request Types

- To Another Entity:
  - When information from another entity is needed for care, fax the patient's signed authorization to the other entity.
  - Fax the authorization promptly as the caregivers are awaiting information from this entity to proceed with patient care.
- From Another Entity:
  - When another entity requests information, determine if an authorization is required. If the physician is not on the medical staff, obtain the patient's authorization prior to disclosing the patient's information to that entity.
- Inpatients Transferred to Another Entity:
  - Generally, the nursing unit will copy pertinent information to be taken with the patient on a transfer out, however if HIMS is asked to do so, we will help.
- In circumstances when HIMS is asked to help make copies:
  - Nursing staff will bring the authorization to the HIMS Department.
  - HIMS clerical staff will print the record promptly.
  - HIMS will call nursing to pick up the copies when completed.
- Inpatients Wanting Copies of Medical Records before or at Discharge:
  - Inform the patient's nurse that the patient must complete an authorization.
  - Generally, these requests will be processed after discharge.
  - When special circumstances arise, contact a HIMS Manager.

Turnaround Time of ROI Requests

- All Physician Requests:
  - Incoming calls or faxes will be completed as quickly as possible on the day received unless other arrangements have been made with the physician or facility calling.
- Immediate Access with Physician Portal:
  - Encourage physician offices to utilize the physician portal to access online patient information immediately from their office.
- All Other Requests:
  - Normally completed within <insert your time frame>.

Valid Authorization for ROI Requests

- See the policy called Authorization for Disclosure of Protected Health Information (PHI).
- An authorization will be considered valid when all core elements are present (see above policy for explanation of core elements).
- If core elements are missing the request will be returned to the requestor.
- Authorizations must be dated within <insert time frame>.
- If an authorization question occurs for any reason, do not hesitate to contact the patient for further validation, or ask a HIMS manager for input.
- A faxed authorization can be honored as an original authorization.

Prioritizing ROI Requests

- Requests will generally be handled in the order of receipt.
- Requests having a higher priority include: continuum of care, the coroner, rush or second requests, risk management.
- Exceptions can be made when special circumstances arise.

Logging ROI Requests

- Requests are entered into the ROI computer tracking system.
- Verify the patient's date of birth and Social Security number.
- If the name of the patient cannot be located:
    - Ask another employee to confirm your findings.
    - Call the requestor for clarification of the patient name.
    - Ask the ROI Manager for help.
- Write the patient's medical record number in the upper right hand corner of the request.
- Date stamp when the request was received.
- Sort requests as needed to proceed with completing the request.

Incomplete Records with Requests for ROI

- Physicians have (X) days to complete their records.
- It is recommended requestors wait until the record is completed before copies are made.
- Incomplete records can be copied, but the requestor must be informed the information is still incomplete.
- Most attorneys want completed medical records.
- Some nursing homes will accept incomplete medical records.

Records Not Located for ROI Requests

- Mail a letter with the release as to why records are not found.

On-Hold Requests for ROI

- When a request cannot be completed within the turnaround time, place the request on-hold.
- As needed contact the requestor when there is a delay.
- Audit on-hold requests/pending lists weekly.
- Reasons for requests to be put on-hold include the record is off-site, incomplete, or cannot be located.

Copying Records for ROI

Copying Guidelines

- Copies will be printed on the page straight.
- Print should be dark enough for readability. Some originals in the medical record are copies and are already light. Make appropriate adjustments to the copy machine.
- Make one-sided copies. If a page is printed on both sides make separate copies of the front and back
- It is recommended that all copies go the same direction. Depending on copying practices, some pages may need to be turned so they are all going the same way.
- The back of any form should be copied if there is space for handwritten text. Copy the other side even if it's blank.
- Overlapping pages—When copying old charts with overlapping pages, insert a plain piece of paper under the previous report so only one report is copied at a time. The older medication forms and laboratory forms are examples of this.
- Fetal Monitor Strips—If printing on 8½" x 11" paper, overlap the fetal monitor strip approximately one-inch on each page so the pages can be taped together. If a copy of a continuous strip copy is requested, forward the request to the ROI Manager.
- Copy Machine Maintenance–Clean copy machine glass so black marks do not print. Have an extra toner available on site so production is not delayed.

Copying Content

- Copy only what is requested.
- Determine if any restrictions exist and comply with restriction.
- Copy only the minimum necessary to complete the request. Use judgment in complying with requests asking for the entire or "any and all" medical records. Determine if the entire record is needed or only a specific visit. Many times only pertinent information is needed (see HIM policy titled Pertinent Information to Be Copied). Examples of those generally requiring pertinent information are physicians and sometimes insurance companies.
- Do not include copies of driver's license or insurance cards when completing requests. These documents are considered third-party information. If a patient specifically requests a copy of these documents and completes an authorization, it can be copied.
- Do not copy portions of the record from other entities (for example, other hospitals, physician offices, ambulance reports). The requestor should contact the other entity for their information.
- Call the requestor for clarification of their request as necessary.

Finalizing ROI Requests

After the request has been processed:

- File the request in the correspondence section of the paper record (left side in the correspondence section) if the record was accessed.
- If the request was completed using online patient information, scan the request into the EHR.

How ROI Requests are Delivered

- US Mail
- Any request can be mailed
- Pick-up in person
- The patient or their designee will be asked to show a picture ID, which will be documented on the authorization.
- Faxed
- Only physicians or healthcare facilities can receive faxed documents when it is needed for continuum of care. Verify fax numbers prior to faxing. Also look for a "send successful" notice to ensure the information was sent properly when manually faxing.
- CD patient requests for meaningful use
- <Any other delivery methods you may use>

ROI Copies Never Picked Up

- When customers do not pick up requested records, they should be contacted to remind them or make arrangements to mail.
- CE determines how long to keep copies in the office prior to destroying the unclaimed copies, make a note on the authorization that the customer never came in, date and sign your name.
- Make a notation in the computer about what was done.
- Audit one time monthly.

Other Departments Processing ROI Requests

- Other departments that process and complete ROI requests and will be contacted by HIM as needed.
- Medical Imaging
  - Requests for films are processed by the Medical Imaging Department.
  - The Medical Imaging Department may release a copy of the dictated report with the film.
- Patient Financial Services
  - Requests for copies of itemized statements and patient bills may be processed by the Patient Financial Services.
  - When Patient Financial Services requests copies from HIM, requests will be routed to HIMS.

Copy Charges
<insert your copy charge>

Exceptions:
<insert any exceptions your facility may have>

Monitoring:
<insert any monitoring required by your organization>

Credits: Contributors, Reviewers, and Committees:

References: **Federal or state laws, and any other requirements**

Signatures:

Definitions: <include terms and definition for key words> Examples listed below.

- **Protected Health Information (PHI)**
- **Minimum Necessary Standard**
- **Meaningful Use (MU)**
- **Individually Identifiable Health Information**
- **Electronic health record (EHR)**
- **Authorization:**

Attachments:
<add attachments such as Requirements for a valid authorization to disclose PHI; Authorization Required Content Checklist; Guidelines for Release/Disclosure>

APPENDIX C

SAMPLE LIST OF ROI POLICIES AND PROCEDURES

- After Hours Requests
- Attorneys
- Authorizations
- Business Office Requests
- Chemical Dependency Unit Requests
- Conditions of Admission
- Continuity of Care Requests
- Coroner Requests
- Correspondence Section of the Medical Record
- Electronic Delivery
- Employee Requests
- External Media Encryption
- Fax Disclosures
- Fees for Reproduction
- In-house Patient Requests
- Insurance Company Requests
- Legal Cases
- Medical Staff Requests
- Outsourced Release of Information Vendors
- Patient Requests
- Photograph Duplication Requests
- RAC Audits
- Records from Outside Facilities
- Release of Information Policy
- Release of Information Workflow Processes
- Requests for Amendment
- Requests for Authorization Revocation
- Returned Requests
- Review of PHI in the HIM Department
- Sensitive Records
- Social Security Administration Requests
- Subpoenas/Court Orders
- Third Party Audit Requests
- Verbal Release Without Written Request or Authorization
- Verification of Patient Identity
- Workers' Compensation Requests

APPENDIX D

SAMPLE AUTHORIZATION FORM

<Healthcare Facility Name> Patient Authorization for Disclosure of Health Information:

Patient Name :_____ Date of Birth: _____/_____/_____

Address: _____ City: _____ State: _____ Zip: _____

E-mail Address: _____ Phone: _____

I request that my protected health information (PHI) from <Healthcare Facility> be disclosed to:
Recipient Name: _____
Address: _____ City: _____ State: _____ Zip: _____
E-mail Address: _____ Phone: _____
Fax (healthcare provider only): _____

I authorize the following PHI to be released from my medical record(s): ☐ Emergency Room Record ☐ Laboratory Report(s) ☐ Radiology Report(s) ☐ Immunization Record ☐ Complete Medical Record (all pages) ☐ Radiology film/ imaging studies/tracing/media ☐ Pathology Slides ☐ Itemized Billing Records ☐ Abstract/ Summary (Includes Discharge Summary, History and Physical, Operative Report(s), Consultations and Test Results)
☐ Test Result (s) of: _____
☐ Other: _____

I understand that the information in my health record may include information relating to sexually transmitted disease, acquired or mental health services, and treatment of alcohol or drug abuse.

State and federal law protect the following information. If this information applies to you, please indicate if you would like this information released/obtained (include dates where appropriate):

Alcohol, Drug, or Substance Abuse Records	☐ Yes	☐ No	Dates: _____
HIV Testing and Results	☐ Yes	☐ No	Dates: _____
Mental Health Records	☐ Yes	☐ No	Dates: _____
Psychotherapy Records	☐ Yes	☐ No	Dates: _____
Genetic Records	☐ Yes	☐ No	Dates: _____

Covering the period of healthcare from: Specific Date(s): _____ to _____ **OR**
☐ All past, present, and future encounters/visits

Purpose for requesting information: ☐ Legal ☐ Insurance ☐ Personal ☐ Continuation of Care

Disclosure Format (Paper is default if not marked.): ☐US Mail ☐Fax ☐E-mail ☐Electronic format
Please indicate preference ☐CD ☐Flashdrive
☐ Other: _____

By signing this authorization form, I understand that:
- Requests for copies of medical records are subject to reproduction fees in accordance with federal/state regulations.
- I have the right to revoke this authorization at any time. Revocation must be made in writing and presented or mailed to the Health Information Management Department at the following address: (ADDRESS). Revocation will not apply to information that has already been disclosed in response to this authorization.
- Unless otherwise revoked, this authorization will expire on the following date/event/condition: _____. If I fail to specify an expiration date/event/condition, this authorization will expire one year from the date signed.
- Treatment, payment, enrollment, or eligibility for benefits may not be conditioned on whether I sign this authorization.
- Any disclosure of information carries with it the potential for unauthorized redisclosure, and the information may not be protected by federal confidentiality rules.

_____ _____
Patient or Authorized Representative Signature Date

_____ _____
Print Name Relationship to Patient (if applicable)

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

APPENDIX E
RECOMMENDED MINIMUM DATA SET BY REQUESTOR

The following chart is a suggested reference guide when responding to requests for information. It is not meant to be used as a rigid tool, but rather as a starting place for the general types of information that would be released in these situations.

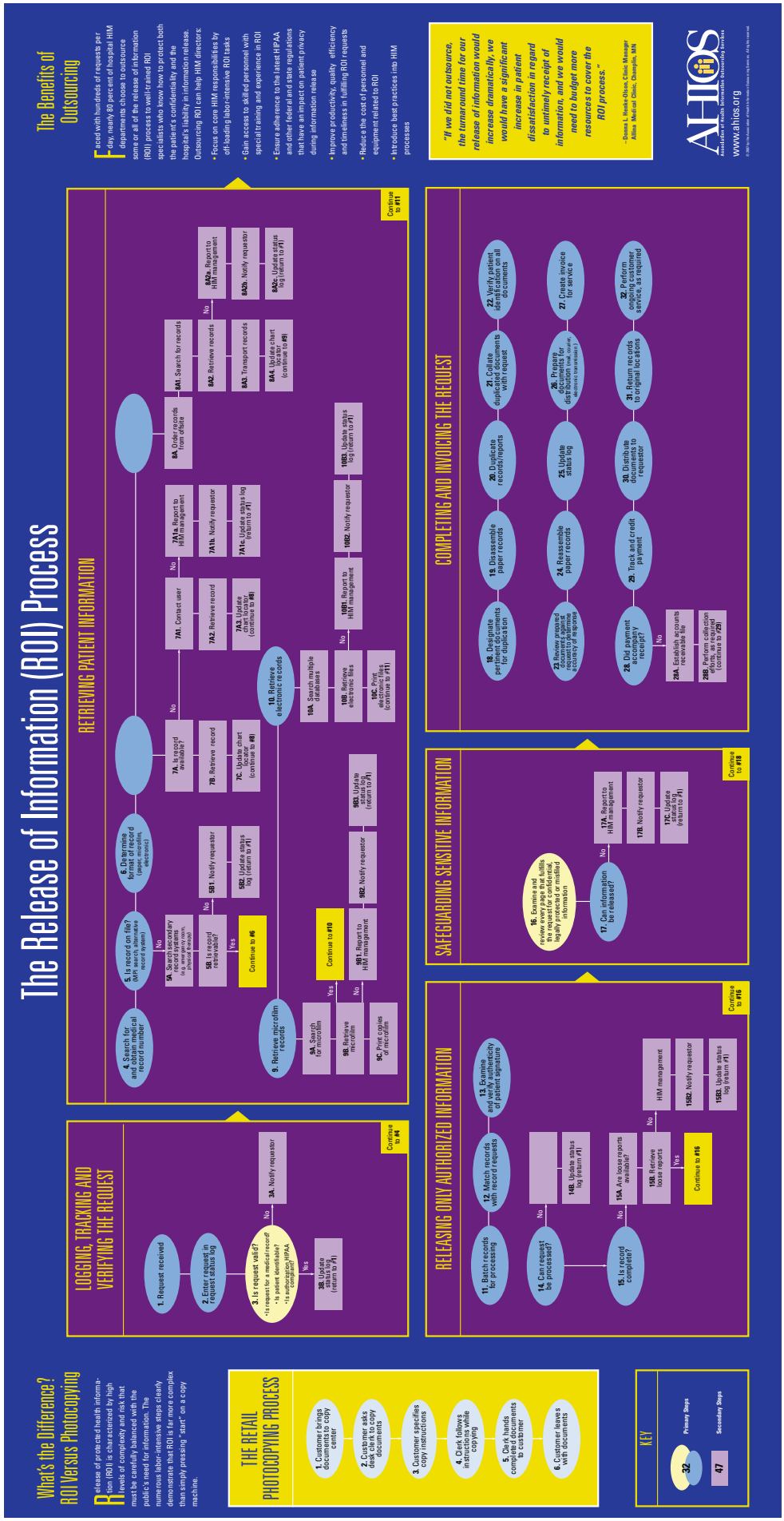
Requestor	Request/Purpose	Disclosures
Patient	Entire record for Continuity of Care (CoC)	Standard Abstract*
Patient	Specific document, (e.g. Test Result)	Specific document requested only.
Physician	Entire record for CoC	Standard Abstract
Physician	Specific document, (e.g. Test Result)	Specific document requested only.
ER to Acute Setting	Provide ER information for purpose of CoC in the acute setting.	ER Record, provider-dictated report, nursing assessments and treatment records, reports of diagnostic studies, transfer documents, any other critical care records and flow sheets.
School Nurse	Verification of required student immunization(s)	Vaccine/Immunization Record: (e.g. type of vaccine, date given, source, site given, Vaccine lot number & manufacturer, VIS information, person giving vaccine, etc.)
School Nurse	Proper administration of child's medications at school	List of medications, dose, frequency, etc. and indications for use.
School Nurse/Counselor	Evaluate child's medical condition for school activities	Letter from physician or discharge summary
Public Health: Primary Care Provider	Obtain health status and medical care information	WIC Record: lab results—hemoglobin, blood lead levels; special formula/diet recommendations; nutrition assessment.
Public Health: Primary Care Provider	Obtain vaccine or treatment information (rabies, community exposure, etc.)	Immunization record: type of vaccine, dose, administration site, date of vaccine, need for additional doses or follow-up. Treatment record: Course of treatment, medication, strength, dosage, need for additional doses or follow-up.
Public Health: Primary Care Provider	Obtain assessment results, status reports	Assessment reports; progress notes.
Public Health: Specialty Care Program providers	Obtain medical, social, or behavioral history for care planning	Letter from physician, physical exam; narrative; Level I behavior documentation.
Public Health: Primary care providers	Obtain assessment reports, care plans, progress notes	Intake/screening assessment, nursing notes, care plan.

Requestor	Request/Purpose	Disclosures
Public Health: Request for Immunization Record could be obtained from parent, school or primary care provider	List of immunizations an individual has received	List of immunizations. This could include immunization lab tests, vaccine, manufacturer, lot number, expiration date, diluents, date and time of administration, clinician administering, and details about the patient response to vaccine, etc.
Public Health: Shelter Records would be requested from hospital, nursing home or primary care records	Medical services and medical evaluation results documented within the shelter environment	Medications, vital signs, and progress notes regarding health and emotional status.
Public Health: Women's, Infant and Children (WIC) Records would be requested by primary provider of hospital at time of delivery	Medical reports to determine the dietary status of the participant and administrative records as required by the program.	Medical evaluation including hemoglobin or hematocrit, medical reports as indicated by request from provider and administrative eligibility record.

*Standard abstract would contain: history and physical, progress notes, procedure notes, consultation reports, medication list, immunization record, and test reports (ECGS, lab, pathology, etc). Special situations may include requests for copies of photographs or films. Original documents, photographs, and films must be retained at the physician practice as part of the legal health record, unless release of original films is required for clinical purposes.

APPENDIX F
THE ROI PROCESS

(Reprinted with the permission of the Association of Health Information Outsourcing Services, www.ahios.org)



APPENDIX G

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:

_____, Medical Record # _____.

The medical records attached are for the following dates of treatment:

INPATIENT DATES:

OUTPATIENT DATES:

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 (ROI company or department).

_____

HIM Director

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.

APPENDIX H

SAMPLE RETURN REQUEST LETTER

HEALTHCARE FACILITY NAME

DATE:_____

REGARDING PATIENT:_____

To Whom It May Concern:

We cannot process your request for copies of health information at the present time because:

_____ We have searched our information system and have found no record of this patient. If you can provide additional information such as date of birth, social security number or account numbers, we will be happy to recheck our index.
Additional Information: _____

_____ Our records indicate that this information was sent to you on _____ and there have been no subsequent visits made to this facility since that date.

_____ The records you have requested have been destroyed as allowed by law.

_____ We have no records on this patient for the time period of _____.

_____ We have no records on this patient for the physician/facility you specified.

_____ Your authorization contains an e-signature that we do not accept because the patient's identity cannot be verified.

_____ The authorization appears to have been altered. Correction fluid is not allowed.

_____ Your authorization form does not meet the requirements of a valid authorization as defined by the HIPAA privacy regulations §164.508(c). Please have the enclosed authorization form *FULLY* completed and return it with this request.

_____ Please provide the following additional document(s): _____ Copy of death certificate

_____ Copy of healthcare power of attorney _____ Letter of Representation

_____ Other:

Please contact Employee Name with Healthcare Facility, at Phone Number with any questions. Please return all correspondence with any additional information.

Sincerely,

Director, Health Information Management

APPENDIX I

RELEASE OF INFORMATION SPECIALIST JOB DESCRIPTION

JOB TITLE: Release of Information Specialist

DEPARTMENT: Medical Records/ Health Information Management Department

SUPERVISOR'S TITLE: Release of Information Manager

GENERAL SUMMARY

PURPOSE: To provide coverage for release of health information functions, including written and verbal requests for health information. Duties include: Opening mail, verification of proper authorization, using Master Patient Index to obtain medical record numbers, using chart location system to locate paper charts, using EHR system to locate electronic health information, copying health information, billing for copies of health information when applicable, entering all releases into Correspondence Tracking system, answering telephone calls related to the ROI function and numerous other small associated duties.

POLICY SETTING RESPONSIBILIES: The person in this job is responsible for providing input into policies and procedures associated with the job's purpose and essential responsibilities.

DECISION-MAKING AUTHORITY: Routine decisions include: verification of appropriate authorization, prioritizing requests, problem solving record locations, problem solving in customer service for internal and external departmental personnel.

SUPERVISORY RESPONSIBILITY: No formal supervisory responsibility.

PATIENT CARE PROVIDER RESPONSIBILITY: None

ESSENTIAL RESPONSIBILITIES

Responsibility A:	Processes incoming requests for the Release of Information area with 98% accuracy.	Time % 15%	Relative Importance 5
Task #1: Opens and date stamps 100% of all requests received each day. Task #2: Screens each request for release of information requirements and verifies proper authorization. Task #3: Utilizes the facility computer system to obtain medical record numbers and dates of service. Task #4: Enters medical record number, name, requestor, requestor type, date received, and other data items into correspondence tracking system.			

Responsibility B:	Identifies locations and retrieves medical records needed to complete ROI request with 98% accuracy.	Time % 20%	Relative Importance 5
Task #1: Locates patient charts, utilizing the chart tracking system. Task #2: Locates older charts on microfilm using the microfilm system. Task #3: Locates and obtains records from other departments not housed in the MR/HIM Dept.			

Responsibility C:	Tracks medical records during ROI request processing with 98% accuracy.	Time % 5%	Relative Importance 4
Task #1: Transfers location of chart in the chart location system. Task #2: Returns all medical records to correct location.			

Responsibility D:	Processes authorizations/subpoenas with 98% accuracy.	Time % 25%	Relative Importance 5
Task #1: Determines information requested on authorization. Task #2: Communicates with requestor regarding possible charges. Task #3: Photocopies requested information. Task #4: Calculates invoice and determines whether prepayment is required. Task #5: Determines disposition/mails out copies (pick-up/ mail/overnight.) Task #6: Completes request in the correspondence tracking system, entering date processed, documents sent, etc.			

Responsibility E:	Processes STAT requests and walk-in requests the same day with 98% accuracy.	Time % 10%	Relative Importance 4
Task #1: Stat requests are completed according to the need of the patient for patient care purposes. Task #2: Assist walk-in requestors in filling out "Authorization for release of confidential Medical information".			

Responsibility F:	Processes problem requests.	Time % 5%	Relative Importance 4
Task #1: Researches request. Task #2: Returns request with letters stating reason for return. Task #3: Sends final notices on requests pending more than two months. Task #4: Cancels unpaid prepayment requests after thee to four months.			

Responsibility G:	Answers phone calls related to release of information.	Time % 20%	Relative Importance 4
Task #1: Assists requestors with verbal continuity of care requests. Task #2: Assists callers concerning status of requests.			

REQUIRED KNOWLEDGE AND SKILLS

COMPONENT	DESCRIPTION
Knowledge	Working knowledge of MR functions to include chart order/assembly, Terminal Digit Order filing and record flow of department. Required for completely satisfactory performance in this job is knowledge of medical record format, computerized registration inquiry process and back-up manual registration system, as well as admissions process. Working knowledge of computerized access systems.
Skills	Required for completely satisfactory performance in this job is the ability to communicate effectively, provide good customer service, problem solve routine medical record issues, prioritize tasks, be punctual and dependable regarding work tasks, work independently, and pay attention to detail. Must utilize well-organized work habits along with good written and verbal communication skills, utilize electronic messaging, and perform accurate data entry/verification/updating. Computer Skills proficiency
Formal Education and Experience	The formal education normally associated with completely satisfactory performance in this job is a high school diploma or the equivalent. A minimum of two years of experience in medical record department or equivalent is required.

WORKING CONDITIONS

Conditions, which differ from the normal work environment, include stress when communicating with parents, patients, physicians, attorneys, telephones constantly ringing, meeting deadlines and frequent distractions.

The above statements are intended to describe the essential responsibilities being performed by people assigned to this job. They are not intended to be an exhaustive list of the responsibilities assigned to these people.

APPROVED BY

NAME:

TITLE:

APPENDIX J

AUTHORIZATION FAQS AND FACTS

1. **What makes an authorization invalid, defective, or unacceptable?**

   The privacy rule declares invalid any authorization with the following defects:
   - The expiration date or event has passed or occurred.
   - The authorization is missing one or more items of content described above.
   - The authorization is known to have been revoked.
   - The authorization violates a privacy rule standard on conditioning or compound authorizations.
   - Material information in the authorization is known to be false.

2. **How can an organization limit the potential for invalid, defective, or unacceptable authorizations?** Perhaps one of the unintended consequences of the privacy rule is that handwritten, patient-generated authorizations may often be invalid under the rule, as most do not contain an expiration date or a statement about the individual's right to revoke the authorization.

   To minimize the number of invalid authorizations received, the covered entity may want to post its authorization form on its website and encourage individuals to use it. Covered entities may also want to provide instructions for obtaining the authorization form on appropriate automated telephone messages. In addition, covered entities may find it beneficial to distribute new authorization forms to organizations that routinely request patient health information, such as local law firms, insurance companies, and law enforcement agencies.

   Another consideration is the development of an authorization checklist to compare those authorizations received from other facilities against the requirements for a valid authorization to disclose (see "Authorization Checklist" below).

3. **Is special wording or information needed for certain types of releases?**

   Yes. These areas are frequently spelled out in state laws or certain federal laws. It is imperative that when setting up your ROI program, a review of federal and state laws be done to ensure compliance with any local state variances for certain high risk areas. These frequently require more protections to the information and additional actions or information prior to release of information of the defined type. The most common of these types of information are discussed

4. **Substance Abuse Records Covered by Federal Law Protections**

   The Confidentiality of Alcohol and Drug Abuse Patient Records Rule applies to federally assisted alcohol and drug abuse programs. The rule establishes the following content requirements for authorizations to disclose individually identifiable patient health information generated by alcohol or drug abuse programs:

   - The specific name or general designation of the program or person permitted to make the disclosure.
   - The name or title of the individual or the name of the organization to which disclosure is to be made.
   - Patient name.
   - Purpose of disclosure.
   - How much and what kind of information is to be disclosed.
   - The signature of the patient or legal representative.
   - The date on which the authorization is signed.
   - A statement that the authorization is subject to revocation at any time except to the extent that the program or person who is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of services in reliance on a valid authorization or consent to disclose information to a third-party payer.
   - The date, event, or condition upon which the authorization will expire if not revoked. This date, event, or condition must ensure that the authorization will last no longer than reasonably necessary to serve the purpose for which it is given.

5. **Other Records Where Authorization Content May Be Impacted by Individual State Laws**

   Individual states may have laws or regulations defining authorization content. As mentioned above, the state of Minnesota has developed its own Universal Consent Form (See Appendix H for sample of form). For example, some state laws require that authorizations to disclose HIV are separate and apart from any other authorizations an individual may sign for release of protected health information. Other examples of special restrictions may cover information pertaining to mental health treatment, child/elder/domestic abuse, genetic testing, etc. When such laws or regulations exist, a determination must be made how to implement the laws in concert with HIPAA regulations. Sometimes state laws are more protective of information than the HIPAA rule. Other times they may be less stringent than HIPAA. This requires a complete understanding of the state laws that apply to your jurisdiction and how they interact. Refer to Section 3 for more information on your state laws. You may also consult section 160 of the HIPAA privacy rule to determine how to apply the preemption requirements.

6. **What can be done to ensure that the organization is using a valid authorization form for the release of health information?**

   - Study both federal and state requirements for authorizations.
   - Investigate recommended formats by the state medical society, hospital association, or the component state health information association.
   - Draft a sample authorization form that complies with federal and state laws and regulations. (See Appendix C "Sample Authorization to Use or Disclose Health Information")
   - Ask the risk manager and legal counsel to review your draft authorization form.
   - Update or generate new policies and procedures relative to the new authorization.
   - Order appropriate quantities of the approved authorization form.
   - Educate and train staff.
   - Replace all supplies of the old authorization forms with new ones.
   - Post the approved authorization form on the organization's website.
   - Distribute new authorization forms to frequent requestors.

APPENDIX K

TO CHARGE OR NOT TO CHARGE?

The reference table below may be used to determine whether charges should be assessed.

REQUESTER/PURPOSE OF REQUEST	BILL?	RATE/REQUEST TYPE
Ambulance Services (Air & Ground)	No	
Armed Services/Department of Veterans Affairs	No	
Attorney	Yes	Review the state regulation to determine what charges are applicable for the attorney requests
Black Lung Benefits Act	Yes	US Department of Labor will pay up to $180.50 maximum ($175 plus $5.50 postage) for Black Lung records requests. Bill at the State standard rates.
Board of Medical Practice/Licensing Boards	Yes/No	Review the state regulations to determine the appropriate charges
CHAMPUS	Yes/No	Review the request letter to determine appropriate amount to charge.
Child Abuse/Neglect Cases/Investigations	No	Requests received from government agencies
Commitment Proceedings Requests	No	
Coroner's & Medical Examiners	No	
Court-Appointed Special Advocate (CASA) Requests	No	
Crime Victims Compensation Boards/Funds	No	
Disability	Yes	Review the request letter to determine appropriate amount to charge. Also, be aware that some state disability allows a charge for "No Record Found"
Durable Medical Equipment Requests	No	Unless request letter indicates requester will pay.
Fire Departments	No	Entitled to records free of charge per the "fire responders law of HIPAA"
Funeral Director	No	
Guardian ad Litem Program Requests	No	Unless request letter or order indicates will reimburse, cannot charge for records when requester provides Order Appointing Guardian ad Litem.

REQUESTER/PURPOSE OF REQUEST	BILL?	RATE/REQUEST TYPE
Hospitals/Clinics/Healthcare	No	
Homeless Advocacy Projects	No	
Immunizations	No	
Insurance Providers—Auto	Yes	With health insurance, you will need to review the contract within your own healthcare organization to determine if a charge is plausible.
Insurance Providers—Health	Yes/No	Dependent on the contractual agreement between Health Care Entity and Insurance Provider
Insurer Quality Initiative Studies	Yes	Dependent on the contractual agreement between Healthcare Entity and Insurance Provider
Internal Facility Use (Risk Management, Quality, Other not included above)	Yes	Per internal charging approach
Marketing	No	Discuss with your healthcare entity's privacy officer
Medicaid	No	
Military Recruiter Requests	No	
Nursing Homes/Home Health Care Agencies/Hospice	No	
Organ, Eye, or Tissue Donation	No	
Patient, Patient Representative, or Next of Kin	Yes	Per HIPAA a covered entity is not allowed to charge a "retrieval" fee. It is recommended that the Health-care Facility revert to the per page fee allowed by their state regulation.
Physicians	No	
Quality Improvement/Management Review Requests from Insurance Companies	Yes	If the request is from or on behalf of CMS, may be able to charge $0.12 per page. For all other requesters, review the request letter to see if charges are indicated
Researchers (e.g. American Cancer Society, American Diabetes Association, etc.)	Yes	Negotiable—Dependent on the grant and what is allowed for copies of medical records
School Districts	No	
Law Enforcement Officials (LEOs)	No	
Subpoenas (issued directly by the court)	Varies	If the order indicates copies to be provided at no charge, no fee. Otherwise there may be a flat fee included in the request or a statement that there will be a payment.
Subpoenas (issued by Attorney)	Yes	Follow state rates
US Department of Health and Human Services	No	

REQUESTER/PURPOSE OF REQUEST	BILL?	RATE/REQUEST TYPE
US Department of Justice	No	
US District Court/US District Court Subpoena's /United States Court of Federal Claims/US Federal Probation	Varies	
United States Equal Employment Opportunity Commission (EEOC)	No	
Vital Events Reporting or Registry Reporting (e.g., death, births, injuries, disease, state-specific reporting, etc.)	No	
Warning/Notification: (e.g., child abuse, adult abuse, patient threat of harm)	No	
Worker's Compensation—Attorney	Yes	Review state regulation to determine the appropriate charges

APPENDIX L

COSTS TO CONSIDER FOR RELEASE OF INFORMATION

Management should consider the following costs when it is assessing the appropriateness of establishing, maintaining in-house, or outsourcing its release of information activities. These costs can then be evaluated against any state or federally permitted fees.

Description	Managed Totally In-House by the Healthcare Entity	Totally Outsourced to an ROI Vendor	Partially Managed by Healthcare Entity and Partially Managed by Outsourced Vendor
Space for the ROI function	Healthcare entity cost	Healthcare entity cost (typically)	Healthcare entity cost
ROI Forms (including authorization and fax cover sheet)	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost
Reference materials (legal manual, physician directory, hospital directory, etc.)	Healthcare entity cost	Directory of physicians that are affiliated with the Hospital-Healthcare entity cost; Legal manual, national or regional directories of hospitals and physicians—Outsource vendor cost	Depends on contract between healthcare entity and vendor
Office supplies (CDs, USB drives, staplers, staples, scotch tape, pens, etc.)	Healthcare entity cost	Outsource vendor cost	Depends on what is being done by vendor vs. healthcare entity
Access to healthcare entity information system	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost
PCs, printers, printer toner, monitors	Healthcare entity cost	Outsource vendor cost	Depends on what is being done by vendor vs. healthcare entity
Scanner, copier, fax machine, CD burner, or MFU	Healthcare entity cost	Outsource vendor cost	Depends on contract between healthcare entity and vendor
Service contracts on copier/fax machine	Healthcare entity	Outsource vendor	Depends on what is being done by vendor vs. healthcare entity
Microfilm reader/ printer	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost
Paper	Healthcare entity cost	Outsource vendor cost	Depends on contract between healthcare entity and vendor
Envelopes, labels, label maker	Healthcare entity cost	Outsource vendor cost	Depends on contract between healthcare entity and vendor
Telephone	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost
Long distance	Healthcare entity cost	Depends on contract between healthcare entity and vendor	Depends on contract between healthcare entity and vendor
Internet access	Healthcare entity cost	Depends on contract between healthcare entity and vendor	Depends on contract between healthcare entity and vendor
Off-site storage fees and record return fees	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost

Description	Managed Totally In-House by the Healthcare Entity	Totally Outsourced to an ROI Vendor	Partially Managed by Healthcare Entity and Partially Managed by Outsourced Vendor
Postage	Healthcare entity cost	Depends on contract between healthcare entity and vendor	Depends on contract between healthcare entity and vendor
Copies for internal use (Risk Management)	Healthcare entity cost	Depends on contract between healthcare entity and vendor	Depends on contract between healthcare entity and vendor
ROI Management Software	Healthcare entity cost	Outsource vendor cost, except when healthcare entity requires vendor to use healthcare entity's product	Depends on contract between healthcare entity and vendor
Staff (including management)	Healthcare entity cost	Outsource vendor cost; healthcare entity ultimate responsibility for over-sight	Depends on what is being done by the vendor vs. healthcare entity
Education of staff	Healthcare entity cost	May be shared depending on healthcare entity's compliance policies	Depends on contract between healthcare entity and vendor
Benefits for staff	Healthcare entity cost	Outsource vendor cost	Depends on what is being done by vendor vs. healthcare entity
Cost to appear in court pursuant to court order	Healthcare entity cost	Depends on contract between healthcare entity and vendor	Depends on contract between healthcare entity and vendor
Responsibility to address amendment requests	Healthcare entity cost	Healthcare entity cost	Healthcare entity cost
Preparation of affidavits	Healthcare entity cost	Shared cost of healthcare entity and vendor	Shared cost of healthcare entity and vendor
Preparation of accounting of disclosures	Healthcare entity cost	Shared cost of healthcare entity and vendor	Shared cost of healthcare entity and vendor
Responsibility to conduct periodic quality and compli-ance reviews of work	Healthcare entity cost	Healthcare entity cost and vendor cost	Healthcare entity cost and vendor cost