

Management Practices for the Release of Information (2012 update)

Save to myBoK

Editor's note: This update replaces the November–December 2008 practice brief "Management Practices for the Release of Information."

Exchange of health information is an essential function for the provision of high-quality, cost-effective, and safe healthcare. The health information released must be complete, appropriate, and timely to fulfill its intended purpose. Although this sounds straightforward, often it is not an easy task in the complex medical and legal environment in which the healthcare community operates. Release of information (ROI) in healthcare is critical to the quality of the continuity of care provided to the patient. It also plays an important role in billing, reporting, research, and other functions.

Many laws and regulations govern how, when, what, and to whom protected health information (PHI) is released. Federal and state regulations contain specific requirements for the management of health information to ensure privacy of the individual. These regulations attempt to balance the need for prompt and informed delivery of healthcare services while protecting the confidentiality of the individual's PHI.

Challenges occur when federal and state laws conflict. There is no standard, uniform state privacy law in use by all 50 states and the territories. State laws vary (e.g., HIV, mental health, or genetic information) in relation to the protection of patient privacy. Some states require that additional patient authorization be obtained before release; some states do not. Because of variations in local, state, and federal laws, healthcare organizations must develop, implement, and maintain thorough policies, processes, and procedures for compliant ROI practices.

Even as adoption of electronic health records (EHRs) increases access to health information and expands the possible uses of health data, it also has added to the complexity of ROI. For example, meaningful use of EHR technology as defined by the American Recovery and Reinvestment Act includes several requirements for ROI such as formats used for provision of information and turnaround times for health information.

The overall management of ROI processes is fundamental to privacy, security, and compliance. It is crucial that the organization's policies and procedures include management practices to support the actual process of disclosure and its oversight including continuous review and maintenance of the authorization form. This practice brief discusses key management principles within HIM for the release of information in areas of quality control, productivity management, turnaround times, and backlog management.

Quality Control Practices

It is imperative that quality control practices are sufficiently comprehensive to cover the release of information for any purpose. These practices should include prioritization of all requests. Quality control practices should address:

- Processing the request in terms of priority and efficiency
- Tracking and monitoring the request from receipt through final disposition, including any billing or charges for reproducing
- Completion of the request, including final review of health information to be released not including another individual's PHI
- Ensuring responsiveness to clinical need and regulatory guidelines in relation to turnaround time
- Routine monitoring of ROI processes when using an outsourced service
- Regular review of any automated requests for access or release from EHR systems
- Regular review of automated fax numbers and e-mail addresses

These functions should be defined in departmental or organizational policies and should include compliance with all state and federal regulations that may apply to disclosure of health information. The following quality control approaches are critical actions that can be audited concurrently with the process flow or retrospectively for a specified time range.

Monitoring Receipt of the Request

Organizations can monitor the receipt of a request for information to determine if staff performed at a minimum the following actions:

- Recorded the date and time the request was received
- Identified the date and time the requested information was needed
- Identified to whom the information was to be sent
- Confirmed that the request included a valid authorization, where applicable (See [appendix A](#) for a checklist of required elements.)
- Identified the delivery format

Additional activities that may assist in the monitoring and tracking of the request include:

- Recording the date and time of receipt on the request and recording in a manual or electronic log so the request can be tracked from its entry into the work queue to its exit as a completed process
- Entering minimum tracking data appropriately—for example, patient legal name, medical record number, date of birth, date and time of receipt, name of requester, due date, date and time of actual completion, method of transmission, and name of employee completing request

Tracking the Request

Many types of logs may be used to record and monitor request-processing activity, from simple spiral or three-ring binders to specialized release of information software. ROI software is designed to facilitate tracking a request through its life cycle. The software can aid management in monitoring staff performance, turnaround times according to type of request, and other measures. Electronic systems provide the ability to analyze data for monitoring purposes; for example, they can calculate turnaround time by subtracting the date of receipt from the date of actual completion.

The tracking log referred to here is for management of the business process, not the accounting of disclosures function. Logs also may be created by using simple database or spreadsheet programs or may be provided as part of an ROI vendor program.

Manual logs are appropriate in facilities that have minimal ROI activity. If manual logs are used, filing dividers assist in finding the request when updating its status. Dividers may be arranged alphabetically according to patient last name or day of the month the request was received.

It is important to ensure that all pertinent information is captured at the time the request is logged. Staff can flag requests for continuing care to distinguish them from other types of requests routinely received, such as third-party payer, legal, and research requests. As requests are received, staff should prioritize requests according to the date and time needed. It is essential to give priority to continuity of care requests to ensure the information will be available for the next patient encounter. Meaningful use, court orders, subpoenas, and audits all have legal and regulatory deadlines that must be met to avoid financial and criminal penalties.

Processing the Request

Key elements of quality control in the processing of requests for ROI include verifying the completeness and accuracy of the request, the authority of the requester, the identity of the patient, and the appropriateness of the information requested.

Review the content. Staff must verify that requests for information contain all data required by internal policy and state and federal regulations. With the exception of medical emergencies, this should include a requirement for a written request for release of medical information. The request must include in complete and clear language the requirements of a valid

authorization according to HIPAA and any applicable state laws. HIPAA requirements can be found in § 164.508 "Uses and disclosures for which an authorization is required." This regulation not only requires certain specific content items but also addresses attributes of a defective authorization such as the expiration date has passed or it is known that the authorization has been revoked. See [appendix B](#) for a sample valid authorization.

Verify the legal authority of the requester. The patient or third party requesting information must have legal standing to receive the information requested. Evidence of legal authority may require verification of the requester's identity, a witness signature or notary public seal on the request form, evidence of the relationship between the requester and the patient (e.g., guardianship, conservatorship), documentation from a court of competent jurisdiction, or other means. Consider your organization's policies for electronic signature and identification of requesters, if your facility allows electronic authorization through a portal. For requests considered routine (rather than emergency), verification of the requester's relationship may require direct contact with the patient if the care provider or requesting entity is not known to the healthcare organization processing the request.

Verify the patient. Before processing the request, staff must verify the patient's identification, as provided in the request for release, against the organization's master patient index to ensure the correct records are retrieved. The patient's legal name, date of birth, sex, address, telephone number, guarantor, subscriber, next of kin, or unique identifier such as Social Security number (if available) are key identifying data elements that assist in establishing the proper individual. When there are multiple individuals whose demographic data are similar, staff should investigate further, such as comparing the patient signature on the consent form with a signature contained in the medical record.

Verify appropriateness of information requested for release. Staff must review the content of the information being released to ensure the following:

- An authorization is not required. For patient care, an authorization is not required by HIPAA, but it may be required by state law.
- It conforms to the information that is requested.
- Only the minimum necessary information required to comply with the request is provided.
- The information complies with regulations, such as meaningful use, and organization policies.

Information that pertains to behavioral health, substance abuse, genetic information, HIV, or adoption are some categories that may be governed by more stringent state and federal regulations and require particular care in the review of the request, authorization for release, and provision of the specified information to the entity designated to receive it.

One of the most common causes of a privacy breach is the release of PHI beyond the scope of the authorization. It is critical to perform a final review of all information being released pursuant to each request before the actual disclosure. EHR systems may package information automatically for release and create media for delivery in a single step; it is vital that HIM staff review the outgoing content, even in electronic format.

Verify accuracy of the recipient's address before release. Verify the recipient's mailing address, e-mail address, and fax number before release.

Completing the Request

The final aspect of the quality control process is evaluating the completion of the request. Critical questions include the following:

- If the content of the request does not meet the organization's required elements, was the request returned to the requester with an explanation of the additional information needed or required?
- If the content of the request meets the requirements, was the request processed in accordance with the organization's policies and procedures?
- Was the information directed only to the individual or entity designated in the authorization for release of the information?
- Was the information that was released recorded for internal auditing?
- If a patient picked up the information in person, was there a process in place to verify that person's identity?

- Was the information delivered to the designated entity in accordance with the organization's policies and procedures (e.g., electronic versus hard copy)?

At this point, the request is complete.

Productivity Management, Turnaround Times, and Backlog Management

Management of the ROI process requires development and application of productivity standards to facilitate timely completion of requests. These include a turnaround time goal and measures to address backlog management. The content of such standards must conform to applicable state and federal law, as well as the organization's policies, procedures, mission, and business strategies.

The measures enumerated here are guidelines that must be viewed as the minimum organizations address in developing their internal policies.

Productivity Management

Although productivity information may be collected manually, electronic systems offer more tools for data manipulation and can provide individual production statistics, departmental request volumes, and information regarding request turnaround times. Some systems sort work queues to emphasize higher priority requests automatically and may even alert staff when requests are in danger of exceeding turnaround limits.

Regardless of method, using statistics to manage productivity requires:

- Capture of accurate volumes of incoming requests according to request type
- Tracking staff members who complete the various ROI functions
- Collecting the date and time of key processes to determine processing and turnaround times
- Making the date and time the information available to the requester
- Media or method used to deliver the information, such as fax, post, courier, picked up in person, or released electronically
- If data are captured electronically, audit trail to monitor the accuracy, integrity, and timeliness of all data entry

Workforce Management

To ensure the release of information process is performed in a manner consistent with organizational policies and procedures, management must monitor, review, and evaluate workforce performance. Performance reviews should be completed annually at a minimum. New staff performance should be monitored concurrently for a time to ensure adherence to all applicable guidelines and rules. Each workforce member will require a different level of monitoring based on performance.

Recommendations for quality control include but are not limited to:

- Providing staff with written organizational policies and procedures for the ROI function to include additional training as revisions occur
- Training and education program for new staff: providing staff an opportunity to attend in-service training and education as appropriate when changes in laws and regulations occur
- Reviewing all requests processed by new staff before delivery to ensure validity, appropriateness, compliance, and completeness
- Providing regular feedback to new staff, citing instances of both good and poor performance; offering examples to clarify performance expectations
- Ongoing review, on a regular basis, of a random sample of releases from all types of requesters to ensure that staff is following policies and procedures; providing feedback as appropriate

Turnaround Times and Backlog Management

To measure the time taken to fulfill requests, each organization must establish acceptable standards for turnaround time. Standards should vary depending on the type of request. A request concerning a patient who is in an emergency room or physician's office requires a much shorter turnaround time than a request for a scheduled appointment the following day or the following month. Organizations must determine internal turnaround time expectations for the release of information process and provide resources to meet those requirements and then measure compliance over time.

Assembling aggregate data according to type of request provides concrete information with which to evaluate compliance. When this parameter routinely is not met, evaluation of processes, request volumes, and staff performance provide the information needed to make adjustments. With government programs such as Recovery Audit Contractors and meaningful use, a single late release can have a significant financial effect, adding another reason to manage turnaround time carefully according to request type.

Appendix A: Authorization Checklist—Required Elements

The following checklist can be used as a tool to assess the validity of the authorization submitted with requests for release of information. The first section contains the required elements of HIPAA's valid authorization. The second section contains the additional requirements of an authorization to disclose sensitive or restricted health information (e.g., HIV, alcohol and drug, etc.). This is not an all-inclusive list because some states may have additional exceptions.

#	Section 1: Requirements for Authorization to Disclose Patient Health Information or Records (45 CFR §164.508(c) - HIPAA)	?
1	Authorization is written in plain language.	
2	Authorization identifies the name of the patient whose PHI is being disclosed.	
3	Authorization identifies the type of information to be disclosed.	
4	Authorization identifies the names or classes of persons or types of healthcare providers authorized to make the disclosure.	
5	Authorization identifies the names or classes of persons or types of healthcare providers authorized to whom the organization may make the disclosure.	
6	Authorization identifies the purpose of the disclosure.	
7	Authorization contains the signature of the patient or patient's authorized legal representative.	
8	If signed by an authorized legal representative, the authorization identifies the relationship of that person to the patient.	
9	Authorization includes the date on which the authorization is signed.	

#	Section 1: Requirements for Authorization to Disclose Patient Health Information or Records (45 CFR §164.508(c) - HIPAA)	?
10	Authorization identifies the time period for which the authorization is effective and expiration date or event.	
11	Authorization contains a statement informing the individual regarding the right to revoke the authorization in writing and a description how to do so.	
12	Authorization contains a statement informing the individual about the organization's ability or inability to condition treatment, payment, enrollment or eligibility for benefits.	
13	Authorization contains a statement informing the individual about the potential for information to be redisclosed and no longer protected by the federal privacy rule.	
14	Authorization contains a statement that if an organization is seeking the authorization, a copy must be provided to the individual signing the authorization.	
15	Authorization contains statement that the individual may inspect or copy the health information disclosed.	
16	Authorization includes a statement regarding assessment of reasonable fees for copy services.	
Section 2: Additional Requirements for Authorization to Disclose Sensitive or Restricted Health Information (Refer to Applicable Federal and State Laws for Categories Below)		
	Mental health or behavioral health patient health information or records	
	Alcohol or other drug abuse patient health information or records	
	Developmental disability patient health information or records	
	HIV test results or patient health information or records	
	Other: sexual abuse, child abuse, elder abuse, etc.	

The Department of Health and Human Services offered the following guidance about authorizations:

"The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire 'one

year from the date the Authorization is signed,' 'upon the minor's age of majority,' or 'upon termination of enrollment in the health plan.'

"An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event."¹

HHS also notes:

"One Authorization form may be used to authorize uses and disclosures by classes or categories of persons or entities, without naming the particular persons or entities. See [45 CFR 164.508\(c\)\(1\)\(ii\)](#). For example, it would be sufficient if an Authorization authorized disclosures by 'any health plan, physician, health care professional, hospital, clinic, laboratory, pharmacy, medical facility, or other health care provider that has provided payment, treatment or services to me or on my behalf' or if an Authorization authorized disclosures by 'all medical sources.' A separate Authorization specifically naming each health care provider from whom protected health information may be sought is not required.

"Similarly, the Rule permits the identification of classes of persons to whom the covered entity is authorized to make a disclosure. See [45 CFR 164.508\(c\)\(1\)\(iii\)](#). Thus, a valid Authorization may authorize disclosures to a particular entity, particular person, or class of persons, such as 'the employees of XYZ division of ABC insurance company.'"²

Notes

1. Department of Health and Human Services. "Must an Authorization Include an Expiration Date?" September 24, 2003. www.hhs.gov/hipaafaq/use/476.html.
2. Department of Health and Human Services. "May a Valid Authorization List Categories of Persons Who May Use or Disclose Protected Health Information, without Naming Specific Individuals or Entities?" September 24, 2003. www.hhs.gov/hipaafaq/use/473.html

Appendix B

Sample Authorization to Disclose Health Information

Patient Last Name: _____ Patient First Name: _____

Address: _____

Phone Number: _____ Date of Birth: _____

Health Record Number: _____

1. I authorize the disclosure of the above named individual's health information as described below. Please specify requested dates of service:

2. The following individual(s) or organization(s) are authorized to make the disclosure:

Name: _____

Address: _____

3. The type of information to be disclosed is as follows (check the appropriate boxes and include other information where indicated)

☐ problem list

- ☐ medication list
- ☐ list of allergies
- ☐ immunization records
- ☐ most recent history
- ☐ most recent discharge summary
- ☐ laboratory test results (please describe the dates or types of test results you would like disclosed):
- ☐ x-ray or imaging report(s) (please specify the date and type of each report requested):

-
- ☐ x-ray or imaging film(s) (please specify the date and type of each film requested):
 - ☐ consultation reports from (please supply doctors' names):

-
- ☐ entire record
 - ☐ other (please describe):

4. I understand that the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental health services and treatment for alcohol and drug abuse.

5. The information identified above may be disclosed to the following individuals or organization(s):

Name: _____

Address: _____

Name: _____

Address: _____

6. This information for which I am authorizing disclosure will be used for the following purpose:

- ☐ my personal records
- ☐ sharing with other healthcare providers as needed
- ☐ other (please describe):

7. I understand that I have a right to revoke this authorization at any time. I understand that if I revoke this authorization, I must do so in writing and present my written revocation to the health information management department. I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy.

8. This authorization will expire (insert date or event): _____

If I fail to specify an expiration date or event, this authorization will expire six months from the date on which it was signed.

9. I understand that once the above information is disclosed, it may be redisclosed by the recipient and the information may not be protected by federal privacy laws or regulations.

10. I understand authorizing the disclosure of the information identified above is voluntary. I need not sign this form to ensure healthcare treatment.

Signature of patient or legal representative: _____

Date: _____

If signed by legal representative, relationship to patient: _____

Signature of witness: _____

Date: _____

Distribution of copies: Original to provider; copy to patient; copy to accompany disclosure

Note: The types of documents listed on the authorization form may need to be modified for the particular healthcare setting. Authorizations for marketing need to disclose whether remuneration was received by the covered entity. This form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with other federal and state laws and regulations.

Prepared By

Barbara Demster, MS, RHIA, CHCQM
 Angela K. Dinh, MHA, RHIA, CHPS
 Steven Emery
 Elisa R. Gorton, RHIA, MAHSM
 James R. Lantis, Jr., MHA, MS, RHIA

Acknowledgments

Jill Clark, MBA, RHIA
 Margaret M. Foley, PhD, RHIA, CCS
 Jennifer McCollum, RHIA, CCS
 Kelly McLendon, RHIA
 Mona Nabers, MBA, RHIA
 John C. Parmigiani
 Daniel J. Pothan, MS, RHIA, CPHIMS
 Mary Poulson, MA, RHIT, CHC, CHPC
 Marion Prichard, MEd, RHIA
 Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
 Margaret Schmidt, RHIA
 Mariela Twigg, MS, RHIA, CHP, FAHIMA
 Allison Viola, MBA, RHIA
 Diana Warner, MS, RHIA, CHPS, FAHIMA
 Lou Ann Wiedemann, MS, RHIA, FAHIMA, CPEHR

Prepared By (Original)

Linda J. Bock, RHIA

Barbara Demster, MS, RHIA, CHCQM

Angela K. Dinh, MHA, RHIA

Elisa R. Gorton, RHIA, MAHSM

James R. Lantis, Jr., MHA, RHIA

Article citation:

AHIMA. "Management Practices for the Release of Information (2012 update)." *Journal of AHIMA* 83, no.2 (February 2012).

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.