**Appendix 1. Health Information Management (HIM) Practice Use Cases by Information Governance Principle**

1. **Information Governance Principle:** Record Availability

**A2.Single or multiple groups of documents within the electronic medical record can be viewed by or released to the requestor as allowed by Health Insurance Portability and Accountability Act (HIPAA) (1. p.40).**

**A2.1 Single documents within the electronic medical record can be viewed by or released to the requestor (1. p.40)**

To keep a Legal Health Record (LHS) current and accurate requires continuous maintenance by the facility staff under the leadership of the custodian of the health records the health information management department. Whenever, the all changes to the health information system must be reviewed and approved by the forms management committee. Whenever, a new form is added, a current form is revised, documentation tasks are added, deleted, or revised, or other elements of the health information system, the content of the LHS must be updated**.**

The **legal health record (LHR)** is defined as the subset of all patient specific data created or accumulated by a healthcare provider that constitutes the organization’s official business record, and is typically used when responding to formal requests for information for legal and legally permissible purposes[[1]](#footnote-1)

**Distinguishing between the Designated Record Set and the Legal Health Record**

Questions often arise about the difference between the designated record set (DRS) and the legal health record (LHR). The **designated record set** is what an individual has a right to access and request under the HIPAA regulation. According to the ROI Toolkit, “The HIPAA Privacy Rule requires that organizations identify their designated record set, which is defined as a group of records maintained by or for a covered entity that is:

1. The medical records and billing records about individuals maintained by or for a covered healthcare provider
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan
3. Used, in whole or part, by or for the covered entity to make decisions about individuals”[[2]](#footnote-2)

With the definition of the designated record set in mind, the organization must identify the content and data sets specific to their facility. Once the necessary information for the designated record set has been determined, it is required that this information and content be defined and documented within organizational policies.

The **legal health record** is very similar and is considered a subset of the designated record set. It is defined as: “The business record generated at or for a healthcare organization. It is the record that would be released upon receipt of a request. The legal health record is the officially declared record of healthcare services provided to an individual delivered by a provider. The legal health record’s purpose is to serve as the official business record of services performed by the entity for regulatory and disclosure purposes.”[[3]](#footnote-3)

The ability to rapidly gather and assemble all records regardless of format (paper, electronic, or hybrid) and make the documents availability for release electronically is a performance criteria key to the effective delivery of the **release of information (ROI)** workflow process and providing full access on demand to the documents maintained in the enterprise-wide health information system (HIS).

**Release of Information (ROI)** is defined as the process of disclosing patient identifiable information from the health record to another party.[[4]](#footnote-4)

The factors that influence the effectiveness of the release of information process are numerous, multi-faceted, and interrelated. The ideal process should be based upon the implementation of an **electronic document management system (EDMS)**, a multi-component health information technology system designed to serve as a single central platform from which release of information is managed.[[5]](#footnote-5)

The access, use, control, and release of information functions has the potential to be one of the most obscure and confusing business processes owing to the difficulty and capacious nature of state and federal regulations. At a basic level the release of information function consists of a request or authorization from an entity or individual seeking to review, access, or use health information or receive copies of specific records.

**The request and response process typically includes:**

1. Requestor submits a request for ROI. Request may be verbal or written.
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.
3. ROI request content is reviewed against policies and procedures and regulatory criteria.
4. **Decision Point:** Does the request content meet the required policies, procedures and regulatory requirements?

4a. No: Return the request to the originator with a return letter.

1. Yes: **Decision Point:** Does the request provide proof of authority to authorize ROI?
2. Yes: **Decision Point:** Can requestor verify identity?
3. Yes: **Decision Point:** Is requested patient’s admission(s)/ encounter(s) in Master Patient Index (MPI).
4. Pull/retrieve/electronically access record(s) of concern.
5. Produce copies of required record components in the format requested by the requestor.
6. Provide copied record(s) to requestor or designated entity in the format requested by the requestor according to organizational policy.
7. Log completed request in the tracking system
8. End task[[6]](#footnote-6)

**Releasing information to law enforcement:**

1. Release is mandatory to report injuries such as a gunshot or stab wounds
2. Response to judicial officer by subpoena, court order, warrant, summons, or investigative demand
3. For locating a suspect, fugitive, witness, or missing person if the victim cannot consent due to an emergency and when it would affect the investigation
4. If a person has died due to a criminal act
5. If the PHI is evidence of criminal conduct
6. If the release helps avert a serious threat to the health and safety of the public
7. To provide medical care to those in custody at a correctional facility or to protect the health and safety of employees and others[[7]](#footnote-7)

**A2.2 Multiple groups of documents within the electronic medical record can be viewed by or released to the requestor (1. p.40)**

All authorizations for ROI should be visible at the episode-specific level affiliated with a specific encounter number. The business process implemented to review authorizations for release of information for validity and verification against a specific encounter in an electronic health information system can be an extremely time consuming task. Best practice indicates the implementation of 24/7 access via a combination of external patient portal and staff internal viewing application. In such environments, consideration must be give to the release of information staffing and logistics concerns for departments located remotely from the main healthcare facility; that might not be fully staffed to support release of information.

Increased risk mitigation is realized when review of all requests for access, use, and release of information is managed from a single central location. Furthermore, a single centralized processing and storage management location allows for enhanced identification and control of disparate records. Additionally, records maintained to support the billing and collections process could be supported via the **electronic document management system,** or modifications could be made to incorporate the process into apt financial systems. Finally, externally maintained records (digitally or paper –based) could be included in the **EDMS.** Increased record access, control, and security of all requests and accounting of disclosures could be realized through the implementation of a combined centralized logging and audit trail process that could be referenced on demand 24/7.

“With over 40 potential disclosure points in the average healthcare enterprise, it is important for organizations to collaborate on the creation of a single point of oversight and accountability for **personal health information disclosure management**. **Enterprise-wide disclosure management** enables quality control, standardization, and better adherence to policies. It allows for the development of the best possible processes, while also setting the stage for continuous improvement.

Implementing a **centralized PHI disclosure management program** can mitigate opportunities for risk, improve compliance, and better prepare an organization for audits. Below are four key steps to compliance. Ideally, health information management can conduct these steps in a centralized fashion, collaborating with information technology and other departments as appropriate.

**1. Policy and Procedure Review**

A key component of OCR audit preparation—and ensuring proper PHI disclosure management on an ongoing basis—is a comprehensive review of policies and procedures. HIM’s longstanding responsibility as the owner of PHI policies and procedures puts the department in an ideal position to offer this same expertise across the organization.

The review should include policies and procedures related to the following:

* Patient Access (very important for OCR desk audits)
* Accounting of Disclosures
* Restrictions
* Corrections/Amendments
* Breach Notification (very important for OCR desk audits)
* Notice of Privacy Practices
* Sanctions
* Business Associate Agreements
* Release of Information
* Minimum Necessary
* Designated Record Set Definition
* Legal Health Record Definition
* Confidentiality

In addition, the review should include policies related to the HIE environment such as the Data Use and Reciprocal Support Agreement (DURSA) and the sub-data set available through the DURSA, and audits of the HIE environment.

**2. Internal Audits**

Conducting internal audits in a variety of ways (planned, unplanned, or even “mystery” audits, when the staff doesn’t know it’s being audited) can promote better compliance. By going on the offensive, organizations also ensure more thorough preparation for possible OCR audits or state health department reviews. Internal audits at some facilities have revealed dangerous practices—for instance, nursing stations leaving patient information visible on a monitor, and emergency department (ED) clinicians burning CD copies of patient records for unauthorized family members. That said, consider developing an audit program that addresses various privacy and security issues. Develop a checklist and visit various areas of the hospital to review the following:

* Are printers and fax machines secured from public view?
* Are waste bins free of PHI?
* Are computer monitors equipped with privacy screens or kept away from public view?
* Can staff discussing PHI be overheard?
* Are print capabilities limited to only the necessary departments?
* If patient names are used in waiting rooms, do clinicians and staff use only the minimum necessary? (i.e., Ms. Smith)
* If sign-in sheets are used, is the minimal amount of PHI requested?
* Are doors locked and access limited to departments housing PHI?
* Is the Notice of Privacy Practices posted?

Also, conduct various tests to determine if staff is protecting PHI:

* Walk through the nursing station to see if it’s possible to remove a chart or access documents.
* Ask IT to call a staff member to see if he or she will give out password information.
* Call release of information staff to ask how to obtain a medical record.
* Call the facility and attempt to find out verbal information about a patient.
* Call the HIM department to ask for a correction to your patient record.
* Verify the organization has revoked computer rights and badge access for recently terminated employees.

**3. Tools and Technology**

While departmental and enterprise-wide IT systems have advanced, their capability to support proper PHI disclosure may not be keeping up with increasingly stringent requirements. Working with IT and other appropriate departments, HIM can help ensure software is supporting the organization’s enterprise-wide PHI disclosure management goals. Software enhancements such as flagging for minors’ records, computing turnaround times for fulfilling requests, and adding access trails within the platform can facilitate compliance.

It’s also helpful to review departmental processes and see where technology can be improved to support compliance, or where it currently creates risk by being misused. For instance, in the previous example where ED staff burned patients’ records onto CDs for family members, the use of the CD burner led to improper distribution of patient records. In this case, the organization’s replacement workstation didn’t have a CD burner.

**4. Adequate Training**

A sharp increase in PHI disclosure points and a more networked and complex digitized environment are two factors that increase the importance of comprehensive, organization-wide privacy and security training. Clinicians and staff have numerous opportunities each day to disclose PHI, and if they haven’t received full, up-to-date training, they can unknowingly create risk. The HIPAA privacy and security rules require healthcare organizations to formally educate the workforce to ensure ongoing accountability for the handling of PHI, as well as documentation verifying that it was provided.

While there are no set guidelines for how to conduct training, AHIMA’s best practices include the following:

* Provide annual training for all staff
* Include education, training, and ongoing awareness and cover PHI in all its forms (verbal, written, electronic)
* Develop a repository of current policies and procedures
* Test staff on information to ensure that they have completed training before they are able to access PHI

Role-based training is especially important, as it enables trainees to focus on their daily responsibilities and specifically where they will encounter potential compliance risk. In addition to comprehensive employee training, it is important to work closely with BAs to ensure both thorough training and documentation is conducted.”[[8]](#footnote-8)

1. Servais, C.E. 2008. *The Legal Health Record.* Chicago: AHIMA [↑](#footnote-ref-1)
2. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf>. [↑](#footnote-ref-2)
3. AHIMA. “Fundamentals of the Legal Health Record and Designated Record Set.” Journal of AHIMA 82, no. 2 (February 2011): expanded online version. [↑](#footnote-ref-3)
4. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 128 [↑](#footnote-ref-4)
5. Kohn, D. 2009. (March). How information technology supports virtual HIM departments. *Journal of AHIMA 80(3):* web extra. <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_043005.hcsp?dDocName=bok1040035> [↑](#footnote-ref-5)
6. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf> [↑](#footnote-ref-6)
7. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf> [↑](#footnote-ref-7)
8. Hardwick, Don; Twiggs, Mariela; Braden, James H. "Optimizing PHI Disclosure Management in the Age of Compliance." *Journal of AHIMA* 86, no.2 (February 2015): 32-37. [↑](#footnote-ref-8)