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

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

**HIM Practice A1**. All documents can be accounted for and the record closed as complete within a specific time period post patient discharge in accordance with State and Federal regulations, accreditation organizations (e.g., Joint Commission, Det Norske Veritas Healthcare - ISO 9000), or organizational policy.[[1]](#footnote-1)

Use Case A1.1. All documents can be accounted for within a specific time period post completion episode of care/encounter.

This Use Case is focused on inpatient encounter. Other types of encounter (outpatient, long-term care and others) will be addressed in the future.

The term "accounted for" is defined as the following:

System shall support all types of medical records (paper and electronic) generated during a specified timeframe of an Episode of care/Encounter.

The time period as well as the type of the record is defined by the type and duration of each specific function/event/step of care within the episode of care/encounter, i.e., workflow steps and sub-steps. This includes completed, incomplete or cancelled documents of the episode of care/encounter (See Use Case A1.2).

The episode of care/encounter may consist of the various functions with the correspondent records/ documents as shown in Table 1.

Table 1. Functions of the Episode of Care and Corresponding Documentation

|  |  |
| --- | --- |
| Episode of Care/Encounter’s Functions | Examples of Records/Documents |
| Visit Registration/Admission  | Patient and Facility Demographics, Billing, Consent for Information Exchange |
| Triage | Triage Notes and Vital Signs |
| Assessment | Medical Summary, Preliminary Diagnosis and Care Plan |
| Laboratory and Diagnostic Testing  | Consent for ProcedureTest Orders and Test Result Reports |
| Diagnosis and Care Plan | Confirmed Diagnosis and Updated Care Plan |
| Prescription  | Medication Order and Dispense Report |
| Discharge/Transfer/Disposition (ADT) | ADT Record |

Please note that relevant paper-based documents provided by patient, caregiver and/or clinicians in the episode of care can be scanned and amended to the Episode of Care/Encounter Record.

Figure 1 presents the examples of the episode of care/encounter’s functions and record components, i.e., individual documents/forms generated at a specific function in the process of care.

a

b

Figure 1. Examples of Episode of Care/Encounter’s Functions and Records/Documents: a – high level view of the episode of care functions and documentation; b – detailed view of episode of care functions and documentation

The decision on the list of the documents that will be accounted for is made by the facility's Form Management Committee[[2]](#footnote-2),[[3]](#footnote-3) comprised of representatives from clinical, business and technology departments. These representatives (policy makers) include:

* patient care providers
	+ clinicians (MDs, PA, RNs, residents, other credentialed providers ) and
	+ staff who supports ancillary services (laboratory, radiology, pharmacy, etc.)
* practice administrators (physician’s assistants, medical group administration)
* medical information services directors/medical informatics (CMIO)
* health information technology department (CIO)
* medical records directors (HIM, CDI, ROI)
* compliance officers (legal and regulatory support) (CLO, Audit)
* purchasing and financial managers (CFO) and
* vendors (scanning, imaging, EHR, laboratory, etc.)
* other.

Organizational policy developed by the Form Management Committee defines who is responsible for documenting information in the medical records - the **business actors** for the episode of care/encounter. They include:

* patient care providers
	+ clinicians (MDs, PA, RNs, residents, other credentialed providers ) and
	+ staff who supports ancillary services (laboratory, radiology, pharmacy, etc.)
* patient for patient-generated data entered via web-portals and mobile/virtual technology (e.g., diabetes monitors).

The custodian of the forms/documents is the health information management (HIM) department (former medical records department).

The list of forms/documents and personnel for defining and maintaining these forms/documents are specified by organizational policies.[[4]](#footnote-4) If other facility is involved in providing services, data sharing agreements between two facilities shall define the policies on how documentation will be accounted for when shared.

**The Start and End of the Episode of Care/Encounter**

The **start and the end** of each function/event/step within the episode of care/encounter are defined by the creation and completion of the correspondent record/document related to the specific function/event/step.

The **start of the episode of care/encounter** is defined by the **initial interaction** of the patient with the healthcare facility (e.g., present at the facility, e-mail, phone or other). This initial interaction sets into motion the chain of functions/events/steps defined by the clinical pathway of activities for a specific episode of care/encounter. This initial interaction acts as a trigger of a specific clinical pathway (Table 1).

Table 1. Relationship between Episode of Care/Encounter’s Flow of Events and Documents

|  |
| --- |
| Episode of Care/Encounter |
| Clinical Pathway for <Function: Registration, Assessment, testing, etc.> |
| Workflow Activities or Flow of Events | Records/Documents |
|  | Initial interaction with healthcare facility (visit, e-mail, phone) |
| Step 1 | Document 1 – output for Step 1 and input /trigger for Step 2 |
| Step 2 | Document 2 – output for Step 2 and input/trigger for Step 3 |
| Step 3 | Document 3 – output for Step 3 |

For patient registration, the start of the registration is triggered by the patient presenting at the facility in person or contacting the facility by phone or e-mail. The registrars’ person activates the command “Register a New Patient” or “Look up for the Existing Patient” in facility’s health information system (HIS) to initiate the specific record/document for Step 1 (Patient Registration Form).

For assessment that follows the registration, the completed Patient Registration Form serves as a trigger of the Medical Summary Form

**States of Interactions**

Patient’s **registration, admission, disposition, discharge/transfer** are the **states of the patient’s interaction** with healthcare facility. HIS must capture change in these states via Open and Closed documentation related to each of the states (see Use Case 2). HIS also must support the document flow across all states within the episode of care (Table 1).

 In the HIS the patient status is typically monitored in the **Patient Status** application**. – NEED TO GET BETTER DESCRIPTION OF THIS APPLICATION**. For example, under disposition when patient is moved to another floor for testing, all previous documents that trigger this new function (input documents) and new documents generated by this new function (output documents) must be captured in the HIS.

Please note that **Patient Status** (data element, field) was traditionally used for billing. Now this field may be used as a trigger to determine the corresponding documentation.

The **end** of the function as well as an episode of care/encounter, in general, is defined by providing capabilities to electronically sign the output document. This action is called “**Verified by Authentication**” and includes the time stamp (date and time) of verification for each output document. The completion of this capability is done by obtaining signature of an authorized person including digital signature on a specific document. Furthermore, within each document there can be multiple authentications as defined by organizational policy.

In this year, we will focus on inpatient facilities only, so the **end of the episode of care/encounter** is defined as **patient discharge** from this episode of care/encounter.

Figure 2 represent example of episode of care/encounter and various HIS (applications (APP)) involved in documenting clinical pathway followed in the episode of care. Specific examples of participating information systems (technical actors) include:

1 – EHR System – Record Originator

2 – Ancillary System (Laboratory, Radiology, etc.) – Record Receiver (order) and Record Originator (result report)

3 – Ancillary System (Laboratory, Radiology, etc.) – Record Receiver (prescription) and Record Originator (prescription dispense report)

Please note that every participating technical actor may also exchange the following documentation:

1 – Notification of Document Availability (Sender to Receiver)

2 – Acknowledgement of Document Receipt (Receiver to Sender

Figure 2. Example of Episode of Care/Encounter and Various Health Information Systems (Technical Actors) Involved in Documenting Clinical Pathway

**Use Case A1.2: Record is closed as complete within a specific time period post completion of the episode of care/encounter.**

There are two states of the record/document - **Open and Closed** - that represent the state of therecord.

**Open Record**

**Open** **record** is the document that is created to begin a new function.

In the paper-based environment, **Open record** can be a synonym to the **incomplete record**. In some cases, **incomplete record** term was used for a **lost record,** i.e., the record that could not be found or record that had not been completed when physician left an organization. In the electronic environment these records can be traced as **Open** records.

An **Open record** has to be completed within defined timeframe for a specific function. The Form Management Committee defines policies on the processes and timeliness of the record completion, e.g., 30 days for discharge summary for US Joint Commission and Medicare Conditions of Participation.

**Delinquent** records are considered as **Open** records**.**

HIS must support capabilities to notify clinician (1) when the record is open; (2) when the record is outside of the time limits set for a specific function; (3) ready to be signed, i.e., verified by authentication; and (4) when the record is closed.

The record remains Open until all its parts are assembled and the appropriate documents are authenticated according to organizational policies. [[5]](#footnote-5)

**Record completion** is the process defined by the organizational policy. This process specifies activities of the authorized personnel to be able to

1. open (initiate the new record),
2. access existing record to contribute new information
3. access existing record to modify/correct existing information and
4. close (verify by authentication) a specific component of the record and/or the full record.[[6]](#footnote-6)

In the paper based environment, term **Retraction (go back)** was used to access the record for correcting information that was inaccurate, invalid, or made in error. Retraction is aimed to modify the Open record. [[7]](#footnote-7)Audit trail must capture all modifications done to the record.

The term **Retraction** is used in HIM to modify existing information in the record through record **amendment** or **addendum,** i.e., modification of the original record entry.

**Closed Record**

**Closed record** is the record that (1) contains all necessary clinical information to substantiate the care rendered, (2) verified by authentication by the authorized clinician, and (3) meets the requirements of the legally defensible health record as defined by organizational policies.

In some cases, the function can be initiated but not completed. For example, the test was ordered but the procedure was never performed because patient did not show up.In this case, in the Open record (test order for this procedure) information about the reason why the procedure was not performed must be captured, so the record can be closed.

HIS must have capabilities to assure the completion of the records by the authorized personnel, as follows:

1. generate the list Open records for all patients of a clinician on a daily basis upon opening the HIS
2. generate notifications about the record for which the timeframe is expiring, so clinician could act upon this notification as follows:
	1. close the record supplying appropriate description for the reason of the record closure
	2. sending reminder
		1. to the patient via phone, e-mail, etc. to follow-up
		2. to the ancillary system to follow-up
	3. providing other explanation why the record cannot be closed at this time and
	4. other
3. generate audit reports on records generation, retraction for modification (amendment or addendums) and completion.

**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)**

This Use Case is focused on the continuous maintenance of the health record necessary to maintain a current and accurate Legal Health Record (LHS) and Designated Records Set by the facility staff under the leadership of the custodian of the health records the health information management department in accordance with organizational policy.

Working with representatives from clinical, business and technology departments, the health information management department is responsible for defining the content of the Legal Health Record (LHS) and Designated Records Set. These representatives (policy makers) include:

* patient care providers
	+ clinicians (MDs, PA, RNs, residents, other credentialed providers ) and
	+ staff who supports ancillary services (laboratory, radiology, pharmacy, etc.)
* practice administrators (physician’s assistants, medical group administration)
* medical information services directors/medical informatics (CMIO)
* health information technology department (CIO)
* medical records directors (HIM, CDI, ROI)
* compliance officers (legal and regulatory support) (CLO, Audit)
* purchasing and financial managers (CFO) and
* vendors (scanning, imaging, EHR, laboratory, etc.)
* other.

 Whenever, changes are made to the health information system, they must be reviewed and approved by the health information system 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 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.[[8]](#footnote-8)

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.[[9]](#footnote-9)

The use and disclosure functions can 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 access, review, or use health information or receives copies of records for specific purposes.

The terms **“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.[[10]](#footnote-10) 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** is 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.”[[11]](#footnote-11) The key word hereis **within** because it addresses how entities covered under HIPAA are allowed to use PHI for internal purposeswithout patient authorization.

**Disclosure** is defined by federal regulations disclosure as “the release, transfer, provision of, access to, or divulging in any othermanner of information outside the entity holding the information.”[[12]](#footnote-12) The key word here is **outside**, such asdisclosing a patient’s medical record to an attorney.

**Management of Release of information function can be organized into four steps:**

1. Enter the release of information request into the ROI database. Capturing patient name, date of birth, record number, name, address, and telephone number of the requestor, purpose of the request, and specific health information requested.
2. Validating the authorization. Validate the completed authorization form signed by the patient against the organization’s requirements for a valid authorization. Requirements must compile with federal and state regulations. If authorization is found to be invalid access will be denied.
3. Verify the patient’s identity by validating patient name, date of birth, social security number, address, and phone number in the master patient index. Patient signature on authorization is compared to patient’s signature on file.
4. Process the request for release of information. Record is retrieved, and the information authorized for release is copied and released.[[13]](#footnote-13)

**Use Case for Release of Information process:**

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[[14]](#footnote-14)

**Requests for disclosure permitted by regulation that may not require a patient’s authorization:**

**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

• Governmental insurers

**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

**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.[[15]](#footnote-15)

**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 appropriate staff use. 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 multiple 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**

The focus of this use case is proper and consistent protected health information disclosure management based on compliance with organizational policies and procedures related to the following:

* Patient Access (very important for OCR desk audits)
* Corrections/Amendments
* Release of Information
* Minimum Necessary (Employee access & Patient transfer, or patient referral)
* Designated Record Set Definition
* Legal Health Record Definition
* HIPAA Complaints
* Mobile Devices
* Encryption of Email

In addition, the review should include policies related to the health information exchange (HIE) environment such as the Data Use and Reciprocal Support Agreement (DURSA) and data sub-sets created through the DURSA, and HIE audits.

**2. Internal Audits**

To the extent practicable, harmful effects of non-compliance with organizational policies and procedures can be identified through internal audit and mitigated. Proactive internal audits have revealed dangerous privacy and security issues practices. The privacy and security officers should develop a checklist and visit various areas of the hospital to review the following:

* Are printers and fax machines secured from public view? Are they shared devices?
* Are waste bins free of PHI?
* Are appropriate recycle/shred bins accessible and secure for staff?
* 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 white boards used and out of public view?
* Are doors locked and access limited to departments housing PHI?
* Is the Notice of Privacy Practices posted? If needed in the necessary languages or according to ADA guidelines?

Also, conduct various tests to determine if staff is protecting PHI (be a secret shopper)::

* 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 report a HIPAA complaint?
* 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.[[16]](#footnote-16)

**A3. A log of all requests and accounting of disclosures is kept as an audit trail and can be referenced as needed (1, p. 40)**

**A3.1 An audit log of all requests for release of information and accounting of disclosures should be maintained for historical purposes.**

This Use Case is focused on the maintenance release of information and accounting of disclosure logs for historical and audit purposes. When organizations are considering new health information system technologies, consideration should be given to systems that provide functionality that allow for the capture of release and disclosure logs and the ability to conduct appropriate ad hoc audits. Working with representatives from clinical, business and technology departments, the health information management department is responsible for the design and implementation of the type and format of logs used to record and monitor request-processing activities. Currently, no specific federal laws govern the type and format of logs maintained. The retention of these logs should be in accordance with state laws and hospital policy.

**Elements of the release of information log:**

1. Patient Name
2. Medical Record Number
3. Requestor Name
4. Requestor Address
5. Request Date
6. Time Period of Request
7. Specific Exclusions
8. Date Request Sent
9. Charges
10. Scan of ROI Request

Release of information logs must be retained for 6 years. (HIPAA Privacy Rule)

**The following disclosures must be accounted for:**

1. Government mandated reporting
2. Research
3. Disclosures by business associates that are not for treatment, payment, and healthcare operations[[17]](#footnote-17)

**Though exceptions apply, disclosures typically included in response to an AOD request include:**

* All disclosures of PHI that are not for treatment, payment, or delivery of healthcare operations
* Suspected domestic and child violence and abuse reporting
* Disclosures made for research unless authorized by the patient or legal representative
* Disclosures made to government agencies (excluding intelligence/national security)
* Disclosures to public health authorities
* Disclosures to the Food and Drug Administration
* Disclosures to employers
* Disclosures to health oversight agencies
* Vital statistics reporting
* Disclosures to law enforcement
* Disclosures regarding deceased persons
* Disclosures for research purposes
* Disclosures for specialized government functions
* Disclosures for workers' compensation purposes[[18]](#footnote-18)

**A4. Full chart management functionality (i.e. Record Lifecycle Management) to verify the identification of location of the source of the release, completeness of the documents being released, and destination for the release or review are available in the release of information software. [1, Page 47]**

A.4.1 Release of Information software must identify the physical location and source of the release of information. (1, p. 47).

ThePurposeof this policy is to establish guidelines for the contents, maintenance, and confidentiality of patient electronic health records that meet the requirements set forth in federal and State laws and regulations, and to define the portion of an individual’s healthcare information that comprises the complete patient health record. Patient health information is contained within multiple electronic health information systems in combination with financial and other types of data. Shadow files are maintained by some clinics or care sites and contain copies of selected material, the originals of which are filed in the patient’s permanent electronic health record. This policy defines requirements for those components of information that comprise a patient’s complete health record.

All patient health records regardless of whether they are created at, or received by the organization, and all related patient lists and billing information are the property of the organization. The information contained within the Medical Record must be accessible to the patient and thus made available to the patient and/or his or her legal representative upon appropriate request and authorization by the patient or his or her legal representative.

Original records may not be removed from organizations’ facilities and/or offices except by court order, subpoena, or as otherwise required by law.

Health records shall be maintained in a safe and secure area. Safeguards to prevent loss, destruction and tampering will be maintained as appropriate. Records will be released under the oversight of Health Information Management Services only in accordance with the provisions of this policy and other organizational Privacy Policies and Procedures.

The release of information system shall:

1. Maintain a health record for every individual who is evaluated or treated as an inpatient, outpatient, or emergency patient, clinic, or physician’s office visit.
2. Track the physical location all electronic health information documentation that comprises the patient’s health record regardless of where it may exist in the separate and multiple locations of the enterprise.
3. Track all formats of electronic health information document contents maintained in the patient’s health record, including structured and unstructured text, photographs, films, digital images, monitor strips, and/or a written or dictated summary or interpretation of findings.
4. Identify all created, captured, or scanned health information with the patient’s full name, unique encounter number, Date and time of origination, Attending physician, principle author, secondary author, and if appropriate the scribe.
5. Identify physical location of health information file(s) within the organization.
6. Log the name and title of health information custodian.
7. Maintain a log of each release of information request in an ROI database. Capturing patient name, date of birth, record number, name, address, and telephone number of the requestor, purpose of the request, and specific health information requested.
8. Provide a means to validate and record the completion of authorization form signed by the patient against the organization’s requirements for a valid authorization. Provide a means to capture the verification of the patient or proxy signature on authorization based on comparison to patient’s signature on file.
9. Provide a means to verify the patient’s identity by validating patient name, date of birth, social security number, address, and phone number in the master patient index.
10. Record the location of the where the information was released from. If direct secure faxing is done from the ROI module fax numbers should be hard coded into the system. If manual faxing is done, there should be a way to review that the fax was sent and received.
11. Provide an historical process log to track; (1) Request for release of information. (2) Validating patient authorization. (3) Patient identification and record retrieve. (4) Itemized record that information authorized for release is copied and released.[[19]](#footnote-19)

A.4.2 Release of Information software must identify completeness of the documents being released. (1, p. 47).

1. Medical Record content shall meet all State and federal legal, regulatory and accreditation requirements
	1. Heath information system shall record compliance with specific regulatory and accreditation requirements.
2. Subsequently, all hospital records and hospital-based clinic records must comply with the applicable hospital’s Medical Staff Rules and Regulations requirements for content and timely completion.
	1. Heath information system shall record compliance with specific Medical Staff Rules and Regulations requirements
3. All documentation and entries in the electronic health record must be identified with the patient’s full name and a unique encounter health record number. Each electronically generated document must be affixed with the patient’s full name, unique encounter health record number, as well as date and time stamp.
	1. Health information system shall record completeness based on approved criteria.
4. Chronology is essential and close attention shall be given to assure that documents are filed properly, and that information is entered in the correct encounter record for the correct patient, including appropriate scanning and indexing of imaged documents.
	1. Health information system shall record allow for accurate patient matching
5. All electronic health record entries should be made as soon as possible after the care is provided, or an event or observation is made. An entry should never be made in the electronic health record in advance of the service provided to the patient. Pre-dating or backdating an entry is prohibited.
	1. Health information systems shall validate compliance with timeliness of data entries by monitoring Consistent Time (CT) objectives through Clock synchronization to a predetermined source[[20]](#footnote-20)
6. The Director of Health Information Management is designated as the person responsible for assuring that there is a complete and accurate electronic health record for every patient. The medical staff and other health care professionals are responsible for the documentation in the medical record within required and appropriate time frames to support patient care.[[21]](#footnote-21)

A.4.3 Release of Information software must identify the destination for the release or review. (1, p. 47).

Electronic health records shall be maintained in a safe and secure area. Safeguards to prevent loss, destruction and tampering will be maintained as appropriate. Records will be released from Health Information Management Services only in accordance with the provisions of this policy and other organizational Privacy Policies and Procedures.

The system must have the ability to track corrections or changes to any documentation once it has been entered or authenticated.

The system must provide for data integrity to protect data from accidental or unauthorized change (for example “locking” of the entry so that once signed no further untracked changes can be made to the entry).

The Health Information Management Services staff will process routine requests for health record access, use, and disclosure. All charts accessed, used, or disclosed from the electronic health record system or peripheral health information systems files will be logged, e.g., using a computerized tracking system

**Completion, Timeliness and Authentication of Medical Records**

1. All inpatient Medical Records must be completed within 14 days from the date of discharge In accordance with State regulations and Medical Staff By-Laws and/or Rules and Regulations.
2. All operative and procedure reports must be completed immediately after surgery.
3. All Medical Record entries are to be dated, the time entered, and signed.
4. Certain electronic methods of authenticating the Medical Record, including methods such as passwords, access codes, or key cards may be allowed provided certain requirements are met. The methodology for authenticating the document electronically must comply with organizational electronic signature standards. The entries may be authenticated by computer key, in lieu of a medical staff member’s signature, only when that medical staff member has placed a signed statement with the Medical Center to the effect that the member is the only person who: 1) has possession of the computer key (or sequence of keys); and 2) will use the computer key (or sequence of keys).
5. Fax signatures are acceptable. [[22]](#footnote-22)

**Definitions**

**Record**

According to HIMSS, **record** is defined as a document stating results achieved or providing evidence of activities preformed.[[23]](#footnote-23)

Our record definition analysis showed the need to further define the relationship between records generated throughout healthcare delivery in the context of record lifecycle for the lifetime record, episode of care record, function record and record entry. We proposed the following record hierarchy and definitions:

1. **Lifetime Record (-9mos, birth-death)** is defined as longitudinal health record, i.e., a permanent, coordinated patient record of information that was acted upon to treat the patient, listed in chronological order and maintained across time from birth to death.[[24]](#footnote-24)
2. **Record of Episode of Care (admission-discharge)** is defined as full medical documentation generated during the episode of care, i.e., in a period of continuous medical care performed by healthcare professionals in relation to a particular clinical problem or situ**ation. This period may include one or more heal**thcare services given by a provider. (For our purposes we are limiting the definition to inpatient status.)
3. **Record at the Function Level or Record Entry** is defined as full medical documentation generated during the activities performed under a function. It is defined as the notation made in a patient's health record, whether paper or electronic, by the responsible healthcare practitioner to document an event or observation associated with healthcare services provided to the patient.[[25]](#footnote-25)For some functions, this can be o**ne document, e.g., registration form; for ot**her functions, several documents can comprise the record entry, e.g., testing: consent for procedure, test order, test result report.

Please note that in the standards development organizations (HL7, ISO), the term Record Entry is used for a single document only.

1. R**ecord at Data Entry Level** is defined asa collection of parts that are related to, or associated with, a record for a specific activity.

Using the terminology of the HL7 Clinical Document Architecture (CDA) standards, these parts follow the following hierarchy: record’s **Sections, Templates** and **Da**ta **Fields**.

Using terminology of HL7 Fast Healthcare Information Resource (FHIR) standard, these parts can be represented as record’s “**resources**.” These parts of the record can be completed by various business actors.

Figure 2 presents the record hierarchy.

Figure 2. Record Hierarchy

**Clinical pathway** is defined as a flow of activities and documentation derived from the clinical guidelines as related to a specific episode of care (Figure 1).

Clinical pathway is a tool designed to coordinate multidisciplinary care planning for specific diagnoses and treatments. [[26]](#footnote-26)

Clinical pathway – also known as a clinical workflow document (specification or checklist) – is developed by physicians (medical informaticians) at the facility. It serves as a **practice management protocol**. This protocol defined information and data requirements (forms, documents) associated with the episode of care. The information and data requirements (forms, documents content) are also called **case definitions**, i.e., specific instructions on how to document specific activity within the function based on the clinical guidelines.[[27]](#footnote-27)

The oversight of the correct recording of information according to the clinical pathway protocol and case definition is conducted by the facility’s **Clinical Documentation Improvement (CDI)** team of the HIM department. CDI team is also involved in developing **templates** (standardized formats) for forms and documents used in the clinical pathway to document the episode of care/encounter.[[28]](#footnote-28)

**Form/Document/Screen**

The terms “**Form**”, “**Document**” and “**Screen**” are used interchangeably in this White Paper. Form/document/screen is the representation of knowledge assembled from data collected during the Episode of care/Encounter or Function/Record Entry. Formal definitions of these terms are the following:

**Forms** are pages that allow users to fill in and submit information[[29]](#footnote-29)

**Document** is any analog or digital, formatted and preserved “container” of data or information[[30]](#footnote-30)

**Screen** prototype is a sketch of the user interface of each screen that is anticipated in a project[[31]](#footnote-31)

Information in the Form/Document/Screen can be delivered as scanned document, .pdf, structured text (based on HL7 CDA or FHIR standards) or message (string of data).

The content for specific forms/documents generated under the episode of care/encounter’s functions such as patients demographic, assessment notes, test orders and results, care plans, medication prescriptions and other (Table 1) is out of scope for this White Paper. It may be developed under the IHE Content Profiles in the future.

**Episode of Care/Encounter**

In this White paper, the **episode of care/encounter** is referred to a visit or multiple visits or interaction(s) between patient and provider and/or ancillary services within the facility. The type of episode of care/encounter is defined by the service type (e.g., inpatient, outpatient, emergency department (ED), long-term care and others). Additional discussions are needed to align the terms for episode of care/encounter/ and visit with terminology used by other countries.

The term “episode of care” is also the unit of payment under the home health prospective payment system (HHPPS)[[32]](#footnote-32)

Term **interaction** includes phone calls, e-mail communication, telemedicine sessions, e-visits and other. Specific states of the interaction (**registration, admission, disposition, discharge/transfer)** are the **states** of the patient’s interaction, as an inpatient, are described under **Start and the End of the Episode of Care/Encounter** below.

**Function, Event, Step**

The episode of care/encounter is comprised of **functions/events/steps**.

The **Function** of the episode of care/encounter is defined as entity or the activity that involve a single healthcare department, service area or discipline, [[33]](#footnote-33) e.g., visit registration/admission; triage; nurse's and physician's assessment; laboratory and diagnostic testing; diagnosis and care plan; prescription; discharge/transfer/disposition and other (Figure 1).

The **Event** is defined as an action or activity that occurs within a system and/or network, inclusive of its boundaries.[[34]](#footnote-34)

The **Step** is defined as a sub-action or sub-activity that occurs within a specific event of care.

**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[[35]](#footnote-35)

**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: The record of what you acted upon to treat the patient.

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”[[36]](#footnote-36)

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.

**Provenance** is a very broad topic that has many meanings in different contexts. The **W3C Provenance Incubator Group** developed a working definition of provenance on the Web:”Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that resource. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance.”[[37]](#footnote-37)

**Out of Scope issues**

1. Outpatient and other types of episodes of care/encounter are out of scope for this White Paper.

The episode of care/encounter for other visits than in-patient may not be completed within the same visit. It may involve multiple visits.

The terms “**Day Hospital**”, “**Day Patient**” or “**Partial Hospital**” are referred as a partial care administered in the mental health institution, rehabilitation facility, surgery and other outpatient settings defined as an episode of care provided during the day of the visit. This is also out of scope for this for this White Paper.

1. The content for specific forms/documents generated under the episode of care/encounter’s functions such as patients demographic, assessment notes, test orders and results, care plans, medication prescriptions and other (Table 1) is out of scope for this White Paper. It may be developed under the IHE Content Profiles in the future.

**Recommendations**

**HIM Professionals**

1. Standardize Policies for Form Management Committees including
2. Harmonize existing policies across healthcare organizations
3. Develop a template organizational policy related to form development and management
4. Define standardized set of forms for the Episode of Care
	* Get samples of all possible forms that HIM have to have for the Episode of Care
5. Define policies on the Open and Closed Records and the processes and timeliness of the record completion. This includes finalizing definitions on
	* Open records - former terms must be harmonized and eliminated, e.g., Incomplete, Lost, Delinquent, Cancelled etc.)
	* Define policy that outlines how clinicians are notified of open and closed records when
		+ Procedures ordered but not performed
		+ Documentation components are missing
		+ Signatures are missing. [[38]](#footnote-38)
	* Define a minimum set of content to be analyzed for timeliness and completeness in the legal record

**Standards Development Organizations (SDOs)**

**Health Level Seven (HL7)**

HL7 CBCC (Community-based Collaborative Care (CBCC)) Workgroup

1. Review Patient Friendly/Plain Language ballot (URL: here)
2. Review CBCC documentation in wiki (URL: <http://wiki.hl7.org/index.php?title=Community-Based_Collaborative_Care>)

HL7 FHIR (Fast Healthcare Information Resources) Workgroup

1. Review EHRS Functional Model - Record Lifecycle Events Implementation Guide Ballot by May 7. (URL: <http://hl7-fhir.github.io/ehrs-rle.html>

Please note that Record Amendment should be replaced with Record Retraction that includes Record Amendment and Record Addendum

EHR Functional Model Workgroup

1. Normalize definitions for records/document lifecycle as follows:

***Record Infrastructure RI. 1.4, Function; Record Completeness, Conformance Criteria****:*

***Statement:*** *Manage Record Completeness.*

***Description:*** *The EHR-S must provide the ability for an organization to define minimum elements and timeframes for completion at the report level and at the record level.*

Define: element, report level, record level

*Provide a report that identifies completion and timeliness status by patient/ health record number or other specified parameters.*

Is this Audit trail report?

*Prior to disclosure for legal proceedings or other official purposes, an organization analyzes the health record for completeness. EHR systems must provide the ability to ~~define~~ to capture a minimum set of content to be analyzed for timeliness and completeness and provide a report of the status.[[39]](#footnote-39)*

EHR system will not define a minimum set of content prior to ROI. The Form Committee will.

1.Change define to capture.

2.Define a report of status?

**Care Provision Support (CPS) (SPELL OUT) 3.3.12:** The system SHOULD provide the ability to render an indicator that a patient record is incomplete (e.g., not finalized or authenticated/signed) when a discharge or transfer order is entered into the system. *[[40]](#footnote-40)*

Harmonize terms for Incomplete with Open and Closed records

**W3C**

**W3C:** Review W3C documents addressing Provenance on the W3C wiki.

Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that resource. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance.

<http://www.w3.org/standards/techs/provenance>

<http://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/>

**Vendors**

**Policy Makers**

**International Community**

International Federation of Health Information Management Associations (IFHIMA)

Harmonize the terms Episode of Care/Encounter/Visit

1. Grzybowski, D. (2014). Strategies for electronic document and health record management. Chicago, IL: AHIMA. p.40 [↑](#footnote-ref-1)
2. Forms Management. Hospital Policy. University of Vanderbilt, Nashville TN. June 12, 2000 [↑](#footnote-ref-2)
3. Quinsey CA. Managing forms and legal electronic health records. JAHIMA, July 2007, p.58-59 [↑](#footnote-ref-3)
4. Forms Management. Hospital Policy. University of Vanderbilt, Nashville TN. June 12, 2000 [↑](#footnote-ref-4)
5. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 32 [↑](#footnote-ref-5)
6. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 126 [↑](#footnote-ref-6)
7. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 130 [↑](#footnote-ref-7)
8. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 128 [↑](#footnote-ref-8)
9. 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-9)
10. HHS. “Permitted Use and Disclosure FAQs.” hhs.gov/hipaafaq/permitted/index.html. [↑](#footnote-ref-10)
11. HHS. “Administrative Data Standards and Related Requirements: Definitions.” [↑](#footnote-ref-11)
12. 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. [↑](#footnote-ref-12)
13. Johns, M. L. (2011). *Health Information Management Technology: An Applied Approach.* Chicago, IL: AHIMA Press. [↑](#footnote-ref-13)
14. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf> [↑](#footnote-ref-14)
15. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf> [↑](#footnote-ref-15)
16. 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-16)
17. , Stuard. S. 2003. Developing a plan of action – How to conduct an accounting of disclosures. *In Confidence* 11(7): 4-5. [↑](#footnote-ref-17)
18. Downing, Kathy; McLendon, Kelly. "Checking In on Accounting of Disclosures." *Journal of AHIMA* 84, no.11 (November–December 2013): 50-52. [↑](#footnote-ref-18)
19. University of California Corporate Compliance Policies and Procedures, Legal Medical Records Standards, Policy # 9420 (05/01/2008) <http://pharmacy.ucsd.edu/faculty/ExperientialEducation/docs/Kenneth_Schell_Legal_Medical_Record_Standards_2_29_12_AMPC.pdf> [↑](#footnote-ref-19)
20. Health Information Technology Standards Panel. “Consistent Time Transaction, T 16” <http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=3&PrefixNumeric=16> [↑](#footnote-ref-20)
21. University of California Corporate Compliance Policies and Procedures, Legal Medical Records Standards, Policy # 9420 (05/01/2008) <http://pharmacy.ucsd.edu/faculty/ExperientialEducation/docs/Kenneth_Schell_Legal_Medical_Record_Standards_2_29_12_AMPC.pdf> [↑](#footnote-ref-21)
22. University of California Corporate Compliance Policies and Procedures, Legal Medical Records Standards, Policy # 9420 (05/01/2008) <http://pharmacy.ucsd.edu/faculty/ExperientialEducation/docs/Kenneth_Schell_Legal_Medical_Record_Standards_2_29_12_AMPC.pdf> [↑](#footnote-ref-22)
23. Health Information Management and Systems Society (HIMSS). Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations. 2010. p. 101 [↑](#footnote-ref-23)
24. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 88 [↑](#footnote-ref-24)
25. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 70 [↑](#footnote-ref-25)
26. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 28 [↑](#footnote-ref-26)
27. Children’s Medical Center. Guide to Clinical Documentation Improvement. 2nd Edition. Dallas TX. 2015. [↑](#footnote-ref-27)
28. Solicit from SMEs the samples of such templates and provide the link to the examples of these templates here. [↑](#footnote-ref-28)
29. McGraw Hill Dictionary of Scientific and Technical Terms. 2003 [↑](#footnote-ref-29)
30. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 49 [↑](#footnote-ref-30)
31. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 133 [↑](#footnote-ref-31)
32. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 55 [↑](#footnote-ref-32)
33. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p. 62 [↑](#footnote-ref-33)
34. Health Information Management and Systems Society (HIMSS). Dictionary of Healthcare Information Technology Terms, Acronyms and Organizations. 2010. p. 49 [↑](#footnote-ref-34)
35. Servais, C.E. 2008. *The Legal Health Record.* Chicago: AHIMA [↑](#footnote-ref-35)
36. AHIMA. “Release of Information Toolkit.” May 2013. <http://library.ahima.org/xpedio/groups/secure/documents/ahima/bok1_050184.pdf>. [↑](#footnote-ref-36)
37. Provenance XG Final Report, W3C Incubator Group Report 08 December 2010, <http://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/> [↑](#footnote-ref-37)
38. AHIMA Pocket Glossary of Health Information Management and Technology. 2014. p.77 [↑](#footnote-ref-38)
39. ISO/HL7 10781 - Electronic Health Record System Functional Model, Release 2. 2014 [↑](#footnote-ref-39)
40. ISO/HL7 10781 - Electronic Health Record System Functional Model, Release 2. 2014 [↑](#footnote-ref-40)