Policy Number: 701	Subject: Client Service Record		Page 1 of 10
Relates to: Clinical Records Management	**Written By:** Amy Kobold	**Technical Review/Accountability:** Shelby Shidler, Quality Improvement Manager	**Authorized By:** Amy Kobold, VP, Business Operations
Effective Date: August 2, 2021		**Reviewed:** August 2, 2021 **Revised Date:** August 2, 2021 Amy L. Kobold	

UNISON HEALTH

APPLIES TO:

All Staff

PURPOSE:

To establish guidelines for the contents, maintenance, and confidentiality of client Medical 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, whether in paper or electronic format, that comprises the medical record. Client medical information is contained within a paper and an electronic records system in combination with financial and other types of data. This policy defines requirements for those components of information that comprise a client's complete "*Legal Medical Record."*

POLICY:

Unison Health ensures the efficient, effective, accurate, and confidential maintenance and utilization of client medical records and information.

DEFINITIONS:

Medical Record: The collection of information concerning a client and his or her health care that is created and maintained in the regular course of Unison business in accordance with Unison policies, made by a person who has knowledge of the acts, events, opinions or diagnoses relating to the client, and made at or around the time indicated in the documentation.

1. The medical record includes paper-based records, imaged records, and records maintained in an electronic record system
2. The medical record excludes health records that are not official business records of Unison, such as personal health records managed by the client.

Each Medical Record shall contain sufficient, accurate information to identify the client, support the diagnosis, justify the treatment, document the course and outcomes, and promote continuity of care among health care providers.

The Medical Record may also be known as the "*Legal Medical Record*" or *"LMR*" in that it serves as the documentation of the healthcare services provided to a client by a Unison physician or provider and can be certified by the Unison's Health Information Specialist (s) as such.

The Legal Medical Record is a subset of the *Designated Record Set* and is the record that will be released for legal proceedings or in response to a request to release client medical records. The LMR can be certified as such in a court of law.

Documents that require signatures and/or countersignatures are not part of the LMR until the documents are signed and if required, co-signed. Any unsigned document is to be considered a draft

document and is not considered an official medical record document until it has been signed by an authorized signer, thus draft documents are not to be used in making treatment decisions or to be released from the LMR.

Designated Record Set ("DRS"): A group of records that include protected health information (PHI) and that is maintained, collected, used, or disseminated by, or for, Unison for each individual that receives care. The DRS includes:

1. LMR,
2. Billing records,
3. Information about health plan enrollment, payment, claims adjudication, and case or medical management record systems, and
4. Other information used to make health care decisions.
5. Any research activities that create PHI is part of the DRS and are accessible to research participants unless there is a HIPAA Privacy Rule permitted exception.

Protected Health Information ("PHI"): PHI is individually identifiable health information that is transmitted or maintained in any medium, including oral statements, and part of LMR.

Authentication: The process that ensures that users are who they say they are. The aim is to prevent unauthorized people from accessing data or using another person's identity to sign documents.

Signature: A signature identifies the author or the responsible party who takes ownership of, is responsible for the completeness and accuracy of the entry and attests to the information contained in a record entry or document.

PROCEDURE:

1. Maintenance of the LMR

A. A LMR shall be maintained for every individual who is enrolled with Unison.

2. Confidentiality

A. The LMR is confidential and is protected from unauthorized disclosure by law. The circumstances under which Unison may use and disclose confidential medical record information is set forth in Policy 700 Confidentiality-Release of Clinical Record Information, Policy 700A Privacy of Protected Health Information and other related Privacy Policies and Procedures Policies 700A.1 – 700A.5 and in accordance with Federal regulations, CFR Section 42 and Public Law 104-191.

3. Content

A. LMR content shall meet all State and federal legal, regulatory and accreditation requirements.
B. Additionally, all staff must comply with applicable Unison policies requirements for content.
C. All documentation and entries in the LMR must be identified with the client's full name and a

unique Unison Medical Record number.

D. All LMR entries should be made as soon as possible after the service is provided, or an event or observation is made. An entry should never be made in the LMR in advance of the service provided to the client. Pre-dating or backdating an entry is strictly prohibited.
E. If it is necessary to refer to another client to describe an event, the client's name should not be used in the LMR.
F. Only abbreviations approved by Unison may be used in the LMR, refer to Policy 702A- Clinical Abbreviations.

4. Legal Medical Record vs. Designated Record Set

A. Under the HIPAA Privacy Rule, an individual has the right to access and/or amend his or her protected health information that is contained in a "designated record set." The term "designated record set" is defined within the Privacy Rule to include medical and billing records, and any other records used by the provider to make decisions about an individual. In accordance with the HIPAA Privacy Rule, Unison has defined a "designated record set" to mean the group of records maintained for each individual who receives healthcare services delivered by a healthcare provider, which is comprised of the following elements:
    1. The LMR whether in paper or electronic format.
    2. Billing records including claim information; and
    3. All physician or other provider notes, written or dictated, in which medical decision-making is documented, and which are not otherwise included in the Legal Medical Record (e.g., outside records, email when applicable for treatment).
    4. Refer to Policy 700A.1 Staff/Client/Other Access to Record and Policy 700A.3 Client's Right to Request an Amendment of Record
B. The LMR generally excludes records from non-Unison providers (i.e., health information that was not documented during the normal course of business at Unison or by a Unison provider). However, if information from another provider or healthcare facility, or personal health record, is used in providing client care or making medical decisions, it may be considered part of Unison's Designated Record Set and may be subject to disclosure under subpoena. Disclosures from LMRs in response to subpoenas will be made in accordance with applicable Unison policies related to confidentiality and Policy 708 Subpoena of Clinical Records.

5. Who May Document Entries in the Legal Medical Record

A. Only authorized Unison clinical employees, employees of Unison's contracted medical/clinical services providers, others designated by Unison policies and/or upon a Clinical Director's approval may document in the LMR:

6. Completion, Timeliness and Authentication of Medical Records

A. All staff must comply with applicable Unison policies requirements for timely completion.
B. All LMR entries should be made as soon as possible after the service is provided, or an event or observation is made.

1. Diagnostic Assessments are due within 48 business hours.
2. Comprehensive Assessments are due by the end of the second session.
   a) Case Management– should be completed within two sessions, due prior to the initial ITP and must be updated at least annually.
   b) AOD CM - due for each client that receives case management services and must be completed prior to a client receiving case management services. Re-assessment must be done at least 90 days from the completion of the initial CM Assessment and at least once every 90 days following each reassessment.
3. Mental Health Individual Treatment Plans (ITP) are due by the end of the second session or 1 month of admission, whichever is shorter.
4. Mental Health ITP Reviews for therapy are due at least annually or reviewed at the client's request, when clinically indicated, when there is a level of care change, and/or when a recommended service is terminated, denied, or no longer available to the client.
5. Medical ITPs are to be reviewed and updated on an annual basis.
6. AOD Individual Service Plans (ITP) are due within 7 days of completion of the assessment or at the time of the first face-to-face contact following assessment.
7. AOD ITP Reviews are due every 90 days.
8. AOD Level of Care is due at the time of admission, change in level of care during treatment, and discharge.
9. All community service providers, therapists, prescribers, and nurses should complete progress notes in the Electronic Health Record (EHR) collaboratively with the client at the time of service. They are due within two business days following the service.
10. Case Conferences are documented in Progress Notes and due at the time of case conference.
11. Mental Health Discharge/Termination Summaries are due at the time of discharge.
12. AOD Mental Health Discharge/Termination Summaries are due within 30 calendar days after treatment has been terminated in accordance with the client's individualized treatment plan. Treatment is defined as terminated when no treatment services have been provided or upon documentation of last communication or attempted communication with the client. Services must be documented in the client's chart in order to establish the timeline governing the due date of the termination summary.

C. All LMR entries are to be dated and signed. Entries for the provision of services are to have start and end times. An entry should never be made in the Medical Record in advance of the service provided to the client. Pre-dating or backdating an entry is strictly prohibited.
D. All Unison employees making entries into the LMR are to be in compliance with the Password Maintenance Policy #541A.
E. Fax signatures are acceptable on documents that Unison considers to be originals and part of the LMR.

7. Ownership, Responsibility and Security of Medical Records

A. All Medical Records of Unison clients, regardless of whether they are created at, or received by, Unison, and client lists and billing information, are the property of Unison Health. The

information contained within the LMR must be accessible to the client and thus made available to the client and/or his or her legal representative upon appropriate request and authorization by the client or his or her legal representative – See Policy 700A.1.

B. Responsibility for the LMR. The Quality Improvement Manager is designated as responsible for assuring that there is a complete and accurate medical record for every client. 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 client care.

C. **Original records may not be removed from Unison's facilities and/or offices except by court order, subpoena, or as otherwise required by law.** If an employed physician or provider separates from or is terminated by Unison for any reason, he or she may not remove any original or copy of the LMR, client lists, and/or billing information from Unison's facilities. For continuity of care purposes, and in accordance with applicable laws and regulations, clients may request a copy of their records be forwarded to another provider upon written request to Unison. Paper medical records shall be maintained in the medical records room and are not to be removed from this area. Any individual identified as willingly, intentionally, improperly removing, releasing documents without authorization, destroying, and falsifying client medical information shall be disciplined per Unison policy.
   1. Only authorized staffs are permitted to pull and file charts in the Medical Records room.
   2. The record room is locked when authorized staff is not in attendance. Keys to the room are assigned by Administration. Security should be contacted to open the room in emergency situations.

D. Access to the LMR is limited to staff involved in the care and treatment of the client. EHR access control and validation procedures are in place to validate a staff's access based on role and function. Upon supervisor approval, access to information for emergency situations and client coverage will be granted.

E. Excluding Medical Records personnel, staff may not make copies of documents maintained in the paper Medical Record without prior written Director's approval.

F. With the exception of the following documents, only Medical Records personnel may print EHR documents:
   1. Clinicians are authorized to print the Individual Treatment Plan/Integrated Care Plan for the client and/or significant other (with a valid release).
   2. Psychiatrists and nursing are also authorized to print Medication/Lab Orders and Medication Education forms.
   3. Other documents with written Director approval.

8. Retention and Destruction of Legal Medical Records

All LMR are retained for at least as long as required by State and federal law and regulations, refer to Policy 703 Client Record Storage. Scanned documents are considered an original document after verification of the image, see section X, and are destroyed in accordance with Policy 703.

The electronic LMR is backed up to protect against unintended deletion or modification of a record and computer hardware failure. The Electronic LMR is backed up on a continual basis through logging of changes to the data. Data will be retained for the following time periods:

a. Backups
    i. Nightly backups for up to 30 days
b. Storage
    i. Minimum of one (1) full backup per month are stored securely in a geographically redundant storage for twelve (12) months on encrypted media.
    ii. Minimum of one (1) full backup per year is stored securely in geographically redundant storage for seven (7) years on encrypted media.
c. Recovery
    i. A complete ground up recovery in the case of a catastrophic emergency (where the physical location is no longer available) can be completed in 2 business days.

9. Maintenance, Legibility of Record, and Imaged/Scanned Documents

All Medical Record, regardless of form or format, must be maintained in their entirety, and no document or entry may be deleted from the record, except in accordance with the destruction policy (refer to section IX).

To ensure the quality of electronic scanning, photocopying, and faxing of the document, handwritten entries should be made with permanent blue ink, with medium point pens, and copies of forms are not to be used. All entries in the medical record must be legible to individuals other than the author.

Documents which are scanned will replace paper documents in the medical record and are considered an original document in the imaged form. Thus, it is required that the image maintained in the EHR be identical in every way to its paper source – this includes all writing and text in margins, footnotes, ensuring that the text that runs to the edge of a page does not get cut off or become illegible after the document is scanned, etc. To ensure the images as an exact replication of the paper document and is legible, the following quality assurance process must be followed:

A. Medical Records and designated Support Staff, or as assigned by the Medical Records supervisor, are the only staff authorized to scan documents into the medical record.
B. The Medical Records staff member(s) performing the actual scan will:
    1. Observe that all pages successfully pass through the scanner and that the image displayed on the imaging software preview screen appears accurate.
    2. Enter the date into the EHR for the date the document was scanned when indexing the scanned document.
    3. Stamp the top page of the document scanned using the scan/date stamper, and place on top of a pile of scanned material in a box.

4. The Medical Records member(s) responsible for these records will have 30 days to review the images. If any problem is detected, the paper will be retrieved and rescanned. If the document cannot be scanned to show an exact, legible replica, Medical Records will request another copy of the document for scanning.
5. Thirty days after scanning, the paper documents are sent for storage until destruction according to Policy 703 - Client Record Storage.

C. Any Unison employee that questions if an image is accurately scanned or considers the image illegible must immediately notify Medical Records via email of the image in question.
   1. The Medical Records staff member will pull the stored paper record and compare it to the image within 1 business day of receiving such notice. If any problem is detected, the paper will be rescanned, the image recertified for quality assurance, and the paper document returned to the proper storage box.

10. Addendums to Records

Addendums are significant clinical corrections or changes in a signed report. When an error is made in a medical record entry, the original entry must not be obliterated, and the inaccurate information should still be accessible and readable.

The addendum must be dated and signed by the person making the revision. The contents of LMRs must not otherwise be edited, altered, or removed. Clients may request a medical record amendment and/or a medical record addendum. (*Refer to Policy 700A.3 Client's Right to Request an Amendment of Record.)*

A. The EHR must be corrected, amended, or retracted using Unison's Addendum Policy #713.
B. Addendums made to the LMR must be attached to the original record when released.
C. If the error involves billing (such as time or service billed), staff must fill out the addendum as required and notify the IS Director. The IS Director will work with the Billing Department to correct the error.
D. Preliminary versions of transcribed documents and documents in progress (unsigned) may be edited by the author prior to signing.
E. Documents requiring a countersignature are not part of the LMR until co-signed. Thus, a document may be edited by the author or co-signer until countersigned.
F. Sometimes it may be necessary to re-create a document (e.g., wrong work type) or to move a document, for example, if it was originally posted incorrectly or indexed to the incorrect client record.
G. When a pertinent entry was missed or not written concurrently or within 48 hours of the event, the author must meet the following requirements:
   1. Initiate the Addendum procedure
   2. Enter the current date and time – do not attempt to give the appearance that the entry was made on a previous date or an earlier time. The entry must be signed.
   3. Identify or refer to the date and circumstance for which the addendum is written.
   4. When making a late entry, document as soon as possible. There is no time limit for writing a late entry; however, the longer the time lapse, the less reliable the entry becomes.

H. Errors in Scanning Documents
If a document is scanned with wrong encounter date or to the wrong client, the following must be done:
1. Reprint the scanned document.
2. Rescan the document to the correct date or client.
3. For documents scanned to wrong client, delete the scanned image from the wrong client
4. Store the reprinted scanned document according to section X, 2(d) above.

11. Authentication of Entries

A. Electronic signatures must meet standards for:
1. 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);
2. Authentication to validate the correctness of the information and confirm the identity of the signer (for example requiring signer to authenticate with password);
3. Non-repudiation to prevent the signer from denying that he or she signed the document (for example, public/private key architecture).

At a minimum, the electronic signature must include the full name and either the credentials of the author or a unique identifier, and the date and time signed.

B. Electronic signatures must be affixed only by that individual whose name is being affixed to the document and no other individual.
C. Countersignatures or dual signatures must meet the same requirements.
D. Countersignatures are to be used as required by state licensing or certification statues related to professional scope of practice. Once countersigned, the entry is final and is legally adopted by the supervising professional as his or her own entry.
E. No individual shall share passwords with any other individual.
F. No individual shall make an entry or sign an entry for someone else or have someone else make or sign an entry for them.
G. Digital ink or digitized signatures (handwritten signatures on a pen pad) are considered an original signature on an electronic document.

12. Designation of Secondary Patient Information

The following three categories of data contain secondary client information and must be afforded the same level of confidentiality as the LMR but are not considered part of the legal medical record.

A. Client-identifiable source data are data from which interpretations, summaries, notes, etc. are derived. They often are maintained at the department level in a **separate location or database and** are retrievable only upon request. Examples:
1. Photographs for identification purposes
2. Communication tools (i.e., client lists, ITP lists, missing signature reports, transportation schedule)

3. A client's personal health record provided by the client to his or her care provider.
4. Alerts, reminders, similar tools used as aides in the clinical decision-making process. The tools themselves are not considered part of the legal medical record. However, the associated documentation of subsequent actions taken by the provider, including the condition acted upon and the associated notes detailing the service, are considered a component of the legal medical record. Similarly, any annotations, notes and results created by the provider as a result of the alert or reminder are also considered part of the legal medical record.

B. Administrative Data is client-identifiable data used for administrative, regulatory, healthcare operations and payment purposes. Examples include but are not limited to:
   1. Birth and death certificates.
   2. Event history/audit trails.
   3. Client-identifiable abstracts in coding system.
   4. Client identifiable data reviewed for quality assurance or utilization management.
   5. Administrative reports.

C. Derived Data consists of information aggregated or summarized from client records so that there are no means to identify patients. Examples:
   1. Accreditation reports
   2. Best practice guidelines created from aggregate client data.
   3. Statistical reports.

D. Draft Documents/Work in Progress: Electronic processes and workflow management require methods to manage work in progress. These work-in-progress documents often are available in the system as "draft documents". Draft documents are not considered an official medical record document until it has been signed by an authorized signer and are not to be used in treatment decisions nor released from the Medical Record.

13. ENFORCEMENT, CORRECTIVE & DISCIPLINARY ACTIONS

Compliance with the above policy is monitored by Unison's Information System and Performance Improvement/Quality Assurance Departments. Violations of any of the above policy will be reported to the appropriate supervising authority for potential disciplinary action, up to and including termination and/or restriction of privileges in accordance with Unison's Human Resource/Personnel Policies and Policy 700B – Sanctions for breach of Privacy & Security of Client Protected health Information.

RELATED POLICIES

700 Confidentiality - Release of Clinical Record
700A Privacy of Protected Health Information
700A.1 Staff/Client/Other Access to Record
700A.2 Request for Restrictions on Use/Disclosure of Information
700A.3 Client's Right to Request an Amendment of Record
700A.4 Accounting of Disclosure
700A.5 Confidential Communication/Alternate Delivery
700B Sanctions for Breach of Privacy & Security of Client Protected Health Information

702A Clinical Abbreviations
703 Client Record Storage
708 Subpoena of Clinical Records
709 Facsimile Transmission of Medical Information
711 Observation
713 Addendum to Medical Record