A. POLICY STATEMENT:

Medical records of Office of Mental Health (OMH) State operated facilities are hybrid records, consisting of both paper and electronic documents and utilizing both manual and electronic processes. The term “medical record” is broadly defined to refer to a collection of information about a patient, and includes comprehensive information about clinical, administrative and legal aspects of a patient's care and treatment.

The medical record serves a number of functions related to the provision of care and treatment. The primary function is to facilitate the planning and delivery of integrated quality care and treatment. It provides a comprehensive base of information about a patient's prior history, current functioning and the provision of care and treatment to the full range of staff involved with the treatment of the patient.

The medical record is also used to evaluate and make determinations about the quality of care and treatment provided. Since many reviews are carried out retrospectively, information contained in the medical record is a primary source of assessing the adequacy of the care and treatment provided to individual patients, within a unit, program, facility or throughout the state facility system.

The medical record can also provide a source of information which may be useful in resolving legal issues concerning the patient, staff or the Office, and to implement patient related activities such as quality assurance monitoring, planning, budgeting and activities necessary for payment to be made to or on behalf of patients.

The medical record is comprised of two distinct components: (1) the Legal Medical Record; and (2) the Designated Record Set. The Legal Medical Record is the compilation of information that is released for legal proceedings or in response to authorized requests for medical records (pursuant to HIPAA and Mental Hygiene Law Section 33.13). The Designated Record Set represents a greater scope of information that is available to a patient under the right to access records established in HIPAA and Mental Hygiene Law Section 33.16. Quality assurance information and a patient's Education Record are excluded from both the Legal Medical Record and the Designated Record Set.

This policy directive establishes general requirements pertaining to medical records of OMH State operated facilities. It also specifically identifies the information that comprises both components of a patient’s medical record. It is intended to establish standards for the contents, maintenance, and confidentiality of patient medical records that meet the requirements set forth in both federal and New York State laws and regulations. It fully supersedes the former QA-400, Uniform Case Record.

B. RELEVANT STATUTES AND STANDARDS:

NYS Mental Hygiene Law §33.13
NYS Mental Hygiene Law §33.16  
NYS Technology Law §§103, 104, 105 and 107  
NYS Executive Law §206-a  
9 NYCRR Part 540  
OMH Official Policy directive OM-740 Records Retention Periods  
OMH Privacy Policy  
OMH Information Security Policy  
42 CFR § 482.24  
45 CFR Parts 160, 164  
Joint Commission Standards

C. **DEFINITIONS**  For purposes of this policy directive:

(a) **Authentication**: The process that ensures that users are who they say they are, in order to prevent unauthorized people from accessing data or using another person's identity to sign documents.

(b) **Copy Functionality**: This term refers to the ability to electronically move documentation from one part of a record to another part of the same or a different record, and shall include any of the following techniques: copy and paste, cloning, copy forward, re-use, carry forward, or save note as a template.

(c) **Data Integrity**: The overall completeness, accuracy and consistency of data.

(d) **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, a covered entity for each individual that receives care from a covered entity but excluding quality assurance information (i.e., the incident report and all supporting investigation documents) and the Education Record. The DRS includes:

1. The legal medical record and billing records about individuals maintained by or for a covered health care provider;
2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
3. The information used, in part or in whole, to make decisions about individuals.

(e) **Legal Medical Record**: The collection of information, regardless of format, concerning a patient and his or her health and/or behavioral health care that is created and maintained in the regular course of OMH facility business, in accordance with OMH policies, made by a person who has knowledge of the acts, events, opinion or diagnoses relating to the patient, and made at or around the time indicated in the documentation but excluding quality assurance information (i.e., the incident report and all supporting investigation documents) and the Education Record.

(f) **Medical Record**: The collection of information, regardless of form or format, on all
matters relating to the admission, legal status, care, and treatment of a patient, including all pertinent documents relating to the patient, but excluding quality assurance information (i.e., the incident report and all supporting investigation documents) and the Education Record. The term “medical record” shall mean and include the term “clinical record,” as such term is used and defined in New York State Mental Hygiene Law Sections 33.13 and 33.16.

(g) **Protected Health Information (“PHI”):** PHI is individually identifiable health information that is transmitted or maintained in any medium, including verbal statements.

(h) **Signature:** A signature which, regardless of format, identifies the author or the responsible party who takes ownership of and attests to the information contained in a record entry or document.

(i) **Source information or data:** Data, reports or findings upon which clinical interpretations or decision making are based (e.g., clinical assessments or tests; or written results of a test such as an X-ray, an ECG, or other similar procedures).

(j) **Workforce Members** means employees, volunteers, trainees, clinicians serving under contracts with facilities, and other persons whose conduct, in the performance of work for the Office, including its programs or facilities, is under the direct control of the Office of Mental Health, regardless of whether or not they are paid by the Office.

D. BODY OF THE DIRECTIVE:

(a) **Maintenance of the Medical Record**

(1) A medical record shall be maintained for every individual who is evaluated or treated as an inpatient, outpatient, or residential patient of an OMH hospital, clinic, or program.

(2) The medical record may be a hybrid record, consisting of both electronic and paper documentation.

(3) The medical record contents can be maintained in either paper (hardcopy) or electronic formats, including digital images, and can include patient identifiable source information, such as photographs, films, digital images, and/or a written or dictated summary or interpretation of findings.

(4) The current electronic components of the medical record consist of patient information from multiple electronic medical record source systems. The intent of OMH is to integrate all electronic documents into an electronic repository.

(5) Original medical record documentation must be sent to the designated medical records department. Whenever possible, the paper chart shall contain original reports.
(b) **Confidentiality and Security**

1. The medical record is confidential and is protected from unauthorized disclosure by law, including but not limited to Mental Hygiene Law Section 33.13 and 45 CFR Parts 160, 164 (HIPAA Privacy and Security Regulations).

2. The circumstances and methods under which OMH may use and disclose confidential information from the medical record is set forth in the OMH Privacy Policy and the OMH Information Security Policy.

3. Any disclosures of the medical record shall be limited to that information necessary in light of the reason for the disclosure (i.e., the “minimum necessary rule”).

4. Information disclosed from the medical record shall be kept confidential by the party receiving such information, and the limitations on disclosure (as set forth in Mental Hygiene Law Section 33.13 and the OMH Privacy Policy) shall apply to such party.

(c) **Content Standards**

1. Medical record content shall meet all State and Federal legal, regulatory and accreditation requirements including but not limited to the Medicare Conditions of Participation 42 CFR Section 482.24\(^1\) and standards of the Joint Commission.

2. Each medical record shall contain sufficient, accurate information to identify the patient; support the diagnosis/condition; justify the care; treatment, and services; document the course and results of care, treatment, and services; and promote continuity of care among health and behavioral health care providers. The information may be from any source and in any format, including, but not limited to print medium, audio/visual recording, and/or electronic display.

3. The medical records of all OMH programs must comply with applicable facility policies and procedures, as well as Medical Staff Bylaws, for content and timely completion. Such medical records must also be consistent with any applicable OMH guidelines.

4. All documentation and entries in the medical record, both paper and electronic, must be identified with the patient’s full name and a unique facility medical record number. Each page of double-sided or multi-page forms must

---

\(^1\) Appendix A contains a listing of required medical record documentation content, and current electronic or paper format status.
be marked with both the patient’s full name and the unique medical record number, since single pages may be photocopied, faxed or imaged and separated from the whole.

(5) All medical 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 medical record in advance of the service provided to the patient. Pre-dating or backdating an entry is prohibited.

(d) **Legal Medical Record vs. Designated Record Set**

(1) **Legal Medical Record**: 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 patient medical records under HIPAA and Mental Hygiene Law Section 33.13. The Legal Medical Record includes information pertaining to screening and admission; legal status; assessment and diagnosis; treatment planning, physical and medical data; treatment progress; and discharge.\(^2\)

(2) **Designated Record Set**: 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.\(^3\) In accordance with the HIPAA Privacy Rule, OMH 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:

(i) The Legal Medical Record, whether in paper or electronic format;

(ii) Billing records including claim information; and

(iii) Other information contained in the medical record (whether in paper or electronic format), if such information was used to make treatment decisions about the patient and has not otherwise been incorporated in the Legal Medical Record.

(3) The Legal Medical Record can reference or summarize information obtained from records of non-OMH providers (e.g., health information that was not

\(^2\) The Legal Medical Record includes all information that would formerly be considered the “active” section of the Uniform Case Record.

\(^3\) The Designated Record Set includes all information that would formerly be considered the “active and ‘inactive” sections of the Uniform Case Record.
(4) If information from another provider or healthcare facility, or personal medical record, is used in providing patient care or making medical decisions, it is considered part of the Designated Record Set.

(e) **Completion, Timeliness and Authentication of Medical Records**

(1) All inpatient medical records must be completed within 30 days from the date of discharge. Additional requirements may be included in applicable facility policy/procedures and Medical Staff By-Laws.

(2) All medical record entries are to be authenticated with a signature, date and time.

(3) Certain electronic methods of authenticating the medical record, including methods such as passwords, access codes, tokens, or key cards may be allowed provided certain requirements are met. The methodology for authenticating the document electronically must comply with New York State Electronic Signatures and Records Act (NYS Technology Law §§103, 104, 105 and 107; Executive Law §206-a) and implementing regulations at 9 NYCRR Part 540, and applicable OMH policy (OMH Official Policy Directive QA-400 Medical Records, including Appendix A, Use of Electronic Signature - Electronic Medical Record, [http://inside.omh.state.ny.us/policies/qa400.rtf](http://inside.omh.state.ny.us/policies/qa400.rtf)).

(4) Fax signatures are acceptable, for release of information authorization purposes, but are not acceptable for original chart documents. Efforts should be made to verify signature whenever possible.

(5) No document intended for retention in a medical record should be stored electronically in an unprotected readable/writable format (e.g., MS Word) that permits alteration after the document has been printed, signed, and filed.

(f) **Routine Requests for Medical Records for Purposes of Treatment, Payment and Healthcare Operations**

(1) Facility Health Information Management staff will process routine requests for medical records. All charts physically removed from the medical record storage areas will be logged, including the date and location where they are forwarded (e.g., using a card file or computerized tracking system).

(2) Only authorized OMH Workforce members may directly access medical records in accordance with the OMH Privacy and Security Policies. Workforce
members, who access medical records for payment or healthcare operations are responsible for accessing only the amount of information which is necessary to complete job responsibilities.

(3) Access to medical records by OMH Workforce members shall be in accordance with the following:

(i) Treatment Purposes: Facility clinical staff responsible for providing direct care to a patient may access the full medical record, as necessary to provide care.

(ii) Payment Purposes: Authorized facility workforce members may access the patient’s medical record for purposes of obtaining payment for services, including the following uses:

A. coding and abstracting;
B. billing including claims preparation, claims adjudication and substantiation of services;
C. utilization review; and
D. third party payer reviews (including quality improvement organization reviews).

(iii) Healthcare Operations: Patient medical records may be accessed for routine healthcare operation purposes, including, but not limited to:

A. peer review activities;
B. quality management reviews and investigations;
C. clinical and legal documentation reviews;
D. auditing activities;
E. credentialing and certification activities; and
F. teaching.

(4) Whenever a court requests the Legal Medical Record pursuant to a court order, a copy of the record shall be sent, except when the order specifically states that the original is required.

(g) Requests for Electronic Components of the Medical Record

Personnel who access the electronic medical record are required to have a unique User ID and access code. Access to information is limited according to the minimum necessary rule and managed by role (i.e., “need to know”), as approved by designated management personnel.

(h) Ownership, Responsibility and Security of Medical Records

(1) All medical records of OMH patients, regardless of whether they are created at, or received by, OMH, and patient lists and billing information, are the
property of OMH and the State of New York. However, the information contained within the Designated Record Set must be accessible to the patient and thus made available to the patient or his or her personal representative in accordance with Mental Hygiene Law Section 33.16, HIPAA, and the OMH Privacy Policy Manual.

(2) Responsibility for the medical record: The facility Director of Health Information Services is designated as the person responsible for monitoring release and access to patient medical records. The clinical staff and other health care professionals are responsible for preparing, completing, and submitting accurate documentation in the medical record within required and appropriate time frames to support patient care.

(3) Original records may not be removed from OMH facilities and/or offices except by court order or as otherwise required by law. If an OMH workforce member separates from or is terminated by OMH for any reason, he or she may not remove any original medical records, patient lists, and/or billing information from OMH facilities and/or offices.

(4) Medical records shall be maintained in a safe and secure area. Safeguards to prevent loss, destruction and tampering will be maintained as appropriate, and in accordance with the OMH Information Security Policy. Records will be released from Health Information Management Services only in accordance with the provisions of this policy directive and other applicable OMH policies and procedures.

(5) Consistent with the OMH Confidentiality Guidebook, special care must be exercised with alcohol and substance abuse records protected by 42 CFR Part 2, HIV/AIDS information protected by Article 27F of the Public Health Law, quality assurance documents, and documents relating to patient and child abuse reporting and investigation.

(6) Chronology is essential and close attention shall be given to assure the integrity of data, that documents are filed properly (in the correct section and date order), and that information is entered in the correct encounter record for the correct patient, including but not limited to when scanning and indexing of imaged documents occurs.

(i) **Retention and Destruction of Medical Records**

All medical records are retained for at least as long as required by State and federal law and regulations, and OMH Official Policy Directive OM-740 (Records Retention). The electronic version of the record must be maintained per the legal retention requirements as specified in OM-740, or as otherwise advised by OMH Counsel’s Office.
(j) **Maintenance and Legibility of Record**

(1) All medical records, regardless of form or format, must be maintained in their entirety, and no document or entry may be deleted or expunged from the record, except in accordance with the destruction policy.

(2) Handwritten entries should be made with permanent black or blue ink, with medium point pens. This is to ensure the quality of electronic scanning, photocopying and faxing of the document. All entries in the medical record must be legible to individuals other than the author.

(k) **Corrections and Amendments to Records**

(1) 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.

(2) General Rules:

(i) Documents created in paper format:

   (A) Labels shall not be placed over entries for correction of information.

   (B) If information in a paper record must be corrected or revised, a line shall be drawn through the incorrect entry and the record shall be annotated with the date, time, and the reason for the revision noted, as well as the signature of the person making the revision, provided, however in instances in which the wrong patient's name is in the entry, but the information is correct with respect to the patient of record, the document should be retracted, and a correct copy without the wrong patient's name should be placed in the record, to protect the privacy of the wrong patient. If action has been taken on the wrong patient before the retraction is made, such information must be documented in the record belonging to the wrong patient.

   (C) If the document was originally created in a paper format, and then scanned electronically, the electronic version must be corrected by printing the documentation, correcting as required for paper records, and rescanning the document in its original location.

(ii) Documents created electronically:

   (A) In general, correcting an error in an electronic/computerized medical record should follow the same basic principles as corrections to the paper record.
(B) The system must have the ability to track corrections or changes to any documentation once it has been entered or authenticated.

(C) When correcting or making a change to a signed entry, the original entry must be viewable, the current date and time entered, and the person making the change identified.

(D) Alternatively, if an electronic medical record is not equipped to track corrections or changes, than a user may enter an addendum consistent with paragraph 6 of this subdivision for a late entry (i.e., add the addendum, document the date and time of the entry, and state the reason for the correction); provided, however in instances in which the wrong patient’s name is in the entry, but, the information is correct with respect to the patient of record, the electronic document should be retracted, and a correct copy without the wrong patient’s name should be entered in the record, to protect the privacy of the wrong patient.

(E) Preliminary versions of transcribed documents may be edited by the author prior to signing.

(F) Once a transcribed document is final, it can only be corrected in the form of an addendum affixed to the final copy. The amended version must be reviewed and signed by the author.

(3) Late Entry: When a pertinent entry was missed or not written in a timely manner, the author must:

(i) Identify the new entry as a “late entry”;

(ii) Enter the current date and time, without giving an appearance that the entry was made on a previous date or an earlier time. The entry must be signed;

(iii) Identify or refer to the date and circumstance for which the late entry or addendum is written;

(iv) Document the late entry 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.

(4) Addendum: An addendum is another type of late entry that is used to provide additional information in conjunction with a previous entry. An addendum is also the method used to document corrections submitted by patients or their personal representatives in the exercise of the right to request corrections to their medical records. When entering an addendum the author shall:
(i) Document the date and time on which the addendum was made;

(ii) Write “addendum” and state the reason for creating the addendum, referring back to the original entry;

(iii) Complete the addendum as soon as possible after the original note;

(iv) Sign the addendum and attach it to the associated document, provided, however, that in the event the addendum was submitted by the patient or his/her personal representative, it shall be identified as such.

(5) Errors in Scanning Documents: If a document is scanned with wrong encounter date or to the wrong patient, the scanned document must be reprinted, and then rescanned to the correct episode/encounter date or patient. The incorrectly scanned document must be voided in the permanent document repository.

(I) **Use of Copy Functionality for Documentation within the Medical Record**

(1) The use of copy functionality eliminates duplication of effort and saves time, but should not become routine; it shall be carefully and judiciously used to ensure accurate documentation. Clinicians engaging in electronic documentation must avoid indiscriminately copying and pasting another provider’s progress note, discharge summary, electronic mail communication, or redundant information provided in other parts of the medical record.

(2) Regardless of the method of entry, all clinicians making an entry are responsible for clearly identifying who performed each service documented within the entry. When entering patient data into the medical record that the clinician did not personally take or test, the clinician must attribute the information to the person who did.

(3) Copying from another clinician’s entry: Clinicians remain responsible for the total content of their documentation, whether the content is original, copied, pasted, imported, or reused.

(4) Copying for re-use of data: A clinician may use copy functionality to copy and paste entries made in a patient’s record during a previous encounter into a current record as long as care is taken to ensure that the information actually applies to the current visit, that applicable changes are made to variable data, and that any new information is recorded.

(5) Errors in the source entry that are discovered when using copy functionality must be immediately brought to the attention of Health Information Management. All entries from the original source that contain errors must be corrected in accordance with this policy directive.
(6) Clinicians using copy functionality must attend training offered or recommended by OMH prior to his or her initial use of such technology.

(m) **The following are considered to be part of the Legal Medical Record:**

(1) Administrative records related to patient care, identified in facility guidelines, including but not limited to Admission and Discharge Documents; Acknowledgment of Receipt of Notice of Privacy Practices, Use/Disclosure of PHI Logs, and Patient Movement History;

(2) Advance directives;

(3) Allergy records;

(4) Alerts and reminders;

(5) Assessments, screenings, and evaluations, including:
   (i) Psychiatric, nursing, psychological, social work, vocational, rehabilitation, nutrition, choking, falls
   (ii) Substance Use and Abuse Assessments
   (iii) Suicide and Risk Screenings/Assessments

(6) Care/treatment plans

(7) Consent forms for care, treatment, and research;

(8) Consultation reports;

(9) Diagnostic images;

(10) Discharge plans and summaries;

(11) Graphic records;

(12) History and physical examination records;

(13) Immunization records;

(14) Intake and output records;

(15) Legal papers related to a patient’s care and treatment or legal status, including Legal papers including applications and orders for court retainements, involuntary admission papers, and Criminal Procedure Law 330.20 or 730 examinations;

(16) Medication administration records;

(17) Orders for care and treatment, including medication, laboratory tests, and PRN or STAT orders;

(18) Orders for restraint or seclusion;

(19) Orders restricting patient rights, as required pursuant to Mental Hygiene Law Section 33.02;

(20) Medication profiles;

(21) Monitoring forms required by a specific condition (e.g., diabetes, menses, etc.);

(22) Patient-submitted documentation (including artwork if referenced in the medical record);

(23) Photographs (digital and analog);

(24) Progress notes and documentation;

(25) Records received from another provider directly operated by the Office of Mental Health, if they were relied on to provide care to the patient;

(26) Speech/occupational therapy records;

(27) Vital statistics, including temperature, height, weight, and blood pressure
monitoring;
(28) Any other information required by the Medicare Conditions of Participation, New York State statutes or rules, OMH policy, or by any third-party payer as a condition of reimbursement.

(n) The following are not considered to be part of the Legal Medical Record:

(1) Abbreviation and do-not-use abbreviation lists;
(2) Accreditation reports;
(3) Audit trails related to the electronic record;
(4) Best practice guidelines created from aggregate patient data;
(5) Birth and death certificate worksheets;
(6) Committee minutes (e.g., forensic, case management, or treatment over objection);
(7) Correspondence, including:
   (i) correspondence relating to requests for records;
   (ii) interagency correspondence;
   (iii) oversight agency correspondence;
   (iv) patient complaints.
(8) Databases containing patient information;
(9) Draft documents and work in progress;
(10) Education records;
(11) Event history and audit trails;
(12) Employment indicators located in MHARS;
(13) Financial and insurance forms, including patient resource records;
(14) Incident/investigative reports;
(15) IRB lists;
(16) List of victims of crimes committed by individuals receiving services from OMH;
(17) Lists of known individuals that are identified as potential victims of individuals receiving services from OMH;
(18) Logs;
(19) ORYX, Quality Indicator, Quality Measure, or other reports;
(20) Patient-identifiable claims;
(21) Patient appointment or program schedules;
(22) Protocols and clinical pathways, practice guidelines, and other knowledge sources that do not imbed patient data;
(23) Raw data for testing (e.g., psychiatric or psychological evaluations);
(24) Records from other providers not directly operated by the Office of Mental Health;
(25) Registries;
(26) Research records;
(27) Staff roles and access rights;
(28) SHAPEMEDs;
(29) Statistical Reports.
Use of Electronic Signature - Electronic Medical Record

All MHARS (or its successor electronic records system) patient forms that require confirmation can be electronically signed. It is a facility decision whether or not to enable a form for electronic signature. This can be done on a form by form basis. Once a form is enabled for electronic signature it must be electronically signed. In making the decision to use electronic signature, a facility must conform to the following guidelines:


- The person completing the form must sign into the electronic medical record (EMR) under his/her own name and not under the name of the person who is responsible for electronically signing the form. No one may sign into the (EMR) using someone else's identification.

- If a form is completed by an individual other than the signatory, the person actually signing it must subsequently sign into the application, access it and electronically sign it.

- During active treatment, forms that are electronically signed can be stored electronically in the EMR database (i.e., not printed and placed in the paper chart). Alternatively they can be electronically signed, printed and placed in the chart.

- Although it is acceptable during active treatment to not print, when an individual is no longer receiving services from OMH, it must be ensured that all forms electronically stored are printed and filed in the paper medical record.

- The facility can decide to electronically sign and print some forms while other forms can be electronically signed and stored in the database. Under no circumstances can any single form (e.g., progress notes) be maintained both ways. All copies of an electronically signed form must either be printed and placed in the chart or stored in the database so that anyone seeking one of them will only have one place to go and look for it. A facility cannot elect to have people choose to have the form in electronic format for some patients (or providers) and have the form printed for other patients (or providers). A given form must be either all printed or all electronic.

- If an electronically signed form is not going to be printed, but instead is being stored in the database, then the facility must have a mechanism for ensuring that all persons using the chart are accessing the electronic version of that form.

- The facility’s disaster plan must address the recovery of any form which is being electronically signed and stored in the EMR database in the event of a system failure.
Central Office has a mechanism in place for ensuring that critical clinical information is available to all facilities in the event of a power or network failure. This information will enable facilities to treat patients should the failure last anywhere from several hours to several days.

Any questions concerning the electronic signature standard should be addressed to OMH Information Security Officer. Questions concerning areas of the medical record should be addressed to OMH Chief Medical Informatics Officer. Questions concerning the Information Technology aspects of the EMR should be addressed to HelpDesk. Questions concerning EMR policy should be addressed to the EMR Business Owner.

If a facility has selected to store forms electronically signed in the EMR database without printing them, then upon discharge all stored database forms are to be printed. This requirement shall continue until such time that there is an official EMR electronic medical record.