**Management of Health Data**
**South Metro Human Services, ReEntry House, TMS Treatment Center**
**Effective 9/1/15**

## I. INTRODUCTION:

Client data will be created, maintained and disclosed in accordance with all applicable state and federal laws. Health information will be maintained for a minimum of 8 years.

Relationship between State Law and HIPAA and other federal regulations: (160.203(b)). Federal law preempts state law except if the provision of state law, as it relates to the privacy of Protected Health Information (PHI), is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 (Security and Privacy). There are additional requirements for substance use disorders, minors, family or group therapy and psychotherapy notes. There may be instances where a disclosure permitted under HIPAA is not allowed under another federal or state law. To the extent possible, the following policy and procedure manual has combined the various rules and regulations that apply to protected health information. Staff should direct their questions to the agency's HIPAA Compliance Officer. Staff may also refer to the federal or state law referenced in this manual that applies to these situations for additional detail. The source documents are available on the agency's intranet.

The following are source documents used in the preparation of this policy and procedure manual and can be referred to for more detail on a given matter.

- Minnesota Government Data Practices (MS chapter 13)
- Minnesota Health Record (MS 144.291- 144.34)
- Minnesota Health Care Bill of Rights (MS 144.651)
- Quality of Services (MS 245.467, Sub.6)
- Federal Health Insurance Portability and Accountability Act of 1996, Code of Federal Regulations (42 CFR sections 2.1 – 2.67) and (45 CFR Part 160, Part 162, Part 164
- Health Information Technology for Economic Clinical Health (HITECH) Act (45 CFR Part 170)
- Part 2 regulations relating to confidentiality of alcohol and drug abuse patients records (42 CFR sections 2.1 – 2.67)
- Information to parents of minor patients (MS 144.346)
- Duty to Warn (MS 148.975)
- Psychologists – Protecting the Privacy of clients (Minn.Admin.R.7200.4700) and accessing and releasing private information (Minn.Admin.R.7200.4710)
- Social Workers – Confidentiality and Records (MS 148E.230)
- Licensed Professional Counselors: Disclosure of information (MS148B.593), Protecting the privacy of Clients (Minn.Admin.R.2150.7515), Accessing and Releasing Private Information (Minn.Admin.R2150.7520)
- Licensed Marriage and Family Therapists: Privileged Communications, Exceptions (MS148B.39), code of ethics (Minn.Adminn.R.5300.0350, subp.6)
- Licensed Drug and Alcohol Counselors: Protecting Client Privacy (MS 148.13), Private Information, Access and Release (MS 148F.135), Protecting the Privacy of Clients (Minn.R.2150.7515), Accessing and Releasing Private Information (Minn.Admin.R.2150.7520)

- Rule 31 Chemical Dependency Treatment Clinic: Client Records (Minn.Admin.R.9530.6530)

## II. ABBREVIATIONS AND DEFINITIONS:

- Access – the ability to read, write, modify, or communicate data information or otherwise use any system resource.
- ACT – Social Security Act
- Administrative Safeguards – administrative actions, policies, or procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information, and to manage the conduct of the covered entity's business associate's workforce in relation to the protection of that information.
- Affiliated Entities: 45 CFR Part 164 and MS 144.6521 permit legally separate entities that are affiliated to designate themselves as a single covered entity for purposes of compliance with the Privacy Regulations if all of the entities designated are under common ownership, controlled by another entity, or under common control of another entity. South Metro Human Services, ReEntry House and TMS Treatment Center, Inc., are designated as an Affiliated Entities under this provision.
- ALJ – Administrative Law Judge
- ANSI – American National Standards Institute
- ARRA – subtitle D of the Health information Technology for Economic and Clinical Health provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. 1791-17954
- Authentication – corroboration that a person is the one claimed
- Availability – property or data is accessible and useable upon demand by an authorized person
- BA – Business Associate – another legal entity or a person that is not part of the workforce that performs a function or activity involving individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. It does not include a health care provider concerning the treatment of the individual, a plan sponsor to disclosures by a group health plan.
- Breach of protected health information – unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of 45 CFR 164.402 which compromises the security or privacy of PHI as defined, subject to the exceptions set forth in 45 CFR 164.402.
- CE – Covered entity
  1. A health plan
  2. A health care clearinghouse
  3. A health care provider who transmits any health information in electronic form in connection with a transaction.
- CMS – Centers for Medicare and Medicaid Services within the Department of Health and Human Services.
- Common Ownership or Control – if an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity.

- Confidentiality – means the property that data or information is not made available or disclosed to unauthorized persons or processes.
- Data Classification in Minnesota:
  1. Confidential – data on an individual, not public, inaccessible to the subject of the data
  2. Private – data on an individual, not public, accessible to the subject of the data
  3. Nonpublic – data not on an individual, not public, accessible to the subject of data, if any. Becomes public after 10 years, unless security issues.
  4. Protected nonpublic – data not on an individual, not public, not accessible to the subject of the data. Becomes public 10 years after, unless security issues.
  5. Protected Health Information (PHI) under HIPAA
- De-Identified Information – de-identified information is not consider individually identified health information and is not subject to protection from either the federal or state regulations. It is more comprehensive than a limited data set. The following data elements must be removed from a health record
  1. Names
  2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and equivalent codes
  3. All element dates (except year) that relate to an individual, including DOB, and all ages over 89
  4. Telephone numbers
  5. Fax numbers
  6. E-mail
  7. Social Security numbers
  8. Medical record numbers
  9. Health plan beneficiary numbers
  10. Account numbers
  11. Certificate/license numbers
  12. Vehicle identifiers and serial numbers, license plates
  13. Device identifiers
  14. Web addresses – Universal Resource Locators (URLS)
  15. Internet Protocol (IP) address numbers
  16. Biometric identifiers, including finger and voice prints
  17. Full face photographic images and any comparable images
  18. Any other identifying number, characteristic, or code.
- Disclosure – means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
- DVA – Department of Veterans Affairs
- DRS – Designated Record Set

  Includes:
  1. Medical records, billing records
  2. Enrollment, payment, claims adjudication, and case or medical management records
  3. Other information, in whole or in part, used to make decisions about the individual. This includes any item, collection, used, or disseminated by or for a covered entity and includes Protected Health Information.

  Excludes:
  1. psychotherapy notes
  2. information compiled in anticipation of civil, criminal or administrative action or proceeding.

3. information in clinical laboratory where access is prohibited by the Clinical Laboratory Improvements Amendments of 1988 (CLIA).

- EIN – Employer Identification Number assigned by the Internal Revenue Service.
- Electronic Media – Electronic storage media including memory devices in computers, any removable/transportable digital memory medium, magnetic tape or disk, optical disk or digital memory card, or transmission media used to exchange information already in electronic storage media, including the internet, extranet, leased lines, dial-up lines, private networks.
- Encryption – use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
- Facility – physical premises and the interior and exterior of a building.
- Health Care Operations:
  1. For the treatment of the individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.
  2. To describe a health-related product.
  3. For case management or care coordination, contacting of individuals with information about the treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.
  4. For payment.
  5. Conducting quality assessments, improvement activities, development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies or patient safety activities. Population based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care providers and patients with information about treatment alternatives and related functions that do not include treatment.
  6. Reviewing competence or qualifications of staff, conducting training
  7. Conducting or arranging for medical reviews, legal services, auditing functions, compliance functions.
  8. Business planning and development
  9. General management activities
- Health Information – means any information, whether oral, or recorded in any form or medium that:
  1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and
  2. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment of the provision of health care to an individual.
- HCPCS – Health Care Financing Administration Common Procedure Coding System.
- Individually identifiable health information – is a subset of health information, including demographic information collected from an individual and relates to past, present, or future physical or mental health or condition, that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.
- Information System – an interconnected set of information resources under the same direct management control that shares common functionality. System includes hardware, software, information, data, applications, communications, and people.

- "Informed consent" under Minnesota Law and "Authorization" under federal law shall have the same meaning for this agency.
- Integrity – data or information have not been altered or destroyed in an unauthorized manner.
- Law enforcement officer – an officer or an employee of any agency or authority of the united states, a state, a territory, a political subdivision of any state or territory, or an Indian tribe who is empower to 1) investigate a potential violation, 2) prosecute a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- Limited Data Set: A Limited Data Set may be released only for research, public health or health care operations purposes. A limited Data Set requires the removal of the following: names, postal address, telephone, fax, email, social security number, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers, device identifiers; URLs, Internet Protocol address numbers, biometric identifiers, full face photographs.
- Malicious software – software designed to damage a system
- Minor – means a person who has not attained the age of 18.
- NPI – National Provider Identifier
- OCR – Office of Civil Rights
- Organized Health Care Arrangement – an organized system of health care where more than one agency participates and engages in certain joint activities, including utilization review, quality assessment and improvement, or payment activities.
- Password – confidential authentication information composed of a string of characters
- Patient (or client) identifying information: means the name, address, social security number, fingerprints photograph, or similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information
- PHI – Protected health information, means individually identifiable health information that is created, received, maintained or transmitted
  1. Transmitted by electronic media.
  2. Maintained in any medium described in the definition of electronic media at 162.103.
  3. Transmitted or maintained in any other from or medium.

  It excludes individually identifiable health information in employment records held by a covered entity in its role as employer.
- Physical Safeguards – physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion
- Psychotherapy Notes: includes notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. It does not include medication monitoring, start and stop times, modalities and frequencies of treatment furnished, results of clinical tests and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.
- Related Health Care Entities – MS 144.291 defines a related health care entity as an affiliated health care entity under MS 144.291. South Metro Human Services, ReEntry House and TMS Treatment Center, Inc., are identified as a Related Health Care Entity under this provision for the purpose of PHI data.

- Required by law – a disclosure of PHI due to court order, court-ordered warrants, subpoenas, summons issued by a court, grand jury, tribal government, or an administrative body authorized to investigate, or Medicaid or Medicare or a government program providing public benefits.
- Security – encompasses all administrative, physical, and technical safeguards in a system.
- Security incident – the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system.
- Secretary – means the Secretary of Health and Human Services (HSS) or any other officer or employee of HSS to whom authority has been delegated.
- Technical Safeguards – technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
- Tennessen warning. An individual asked to supply private or confidential data concerning the individual shall be informed of: (a) the purpose and intended use of the requested data within the collecting government entity; (b) whether the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from supplying or refusing to supply private or confidential data; and (d) the identity of other persons or entities authorized by state or federal law to receive the data. This requirement shall not apply when an individual is asked to supply investigative data, pursuant to section 13.82, subdivision 7, to a law enforcement officer.
- Transaction: transmission of information between two parties to carry out financial or administrative activities related to health care:
  1. Health care claims
  2. Health care payment and remittance advice
  3. Coordination of benefits
  4. Health care claim status
  5. Enrollment and disenrollment in a health plan
  6. Eligibility in a health plan
  7. Health plan premium payments
  8. Referral certification an authorization
  9. First report of injury
  10. Health claims attachments
- TPA – Trading Partner Agreement, an agreement related to the exchange of information in electronic transactions.
- TP – Trading Partner.
- Unsecured protected health information – data that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary.
- User – a person or entity with authorized access.
- Workforce members – employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency is under the direct control of such entity, whether or not they are paid by the agency.
- Workstation – an electronic computing device, for example a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

## III. GENERAL ADMINISTRATIVE RESPONSIBILITIES: Part 160

- The agency will cooperate and provide access, records and compliance reports to the Secretary if requested.
- Development of policies and procedures: to accommodate privacy requirements of federal and state rules for the production, storage and management of health care data. The management of the agency is responsible for developing policies and procedures that meet federal and state requirements. Management may revise these policies and procedures from time to time to meet the needs of agency or changing regulations. Policies will be reviewed by August 31st of each calendar year.
- Staff training: all employees will be trained on the management of health care data prior to the effective date of changes in policy or procedure, or at the point of hire, and as regulations or policies/procedures change thereafter.
- Designated Privacy **C**ompliance Officer (HIPAA): The Compliance Officer for this agency is Terry M. Schneider, MA, Licensed Psychologist, 166 4th Street E, Saint Paul, MN 55101, or e-mail: terry@south-metro.org, or another employee whom he has delegated.
- Designated Responsible Authority for Minnesota compliance – for this agency the person is Terry M. Schneider, MA, Licensed Psychologist, 166 4th Street E, Saint Paul, MN 55101 or e-mail: terry@south-metro.org, or another employee whom he has delegated.
- Complaint Process: An individual who believes the agency is not complying with state or federal requirements may file a complaint with the agency's Compliance Officer or Responsible Authority, or with the Secretary.
  1. Complaints filed with the agency must be submitted in writing to the Compliance Officer. The Compliance Officer will respond in writing to the individual within 15 business days or receiving the complaint.
  2. The agency will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provider for filing a complaint.
  3. The agency may not require individuals to waive their rights under 45 CFR Part 160.306
  4. Complaints filed with the Secretary of Health and Human Services:
     - Complaints must be in writing, either on paper or electronically
     - Must name the agency, and describe the acts or omissions believed to be in violation of the applicable requirements
     - Be filed within 180 days of when the complainant knew or should have known that the act or omission occurred.
     - The agency will cooperate and provide access, records and compliance reports to the Secretary if requested.
     - The agency will refrain from intimidation or retaliation for any person testifying, assisting, or participating in an investigation.
     - The Secretary may impose civil money penalties if noncompliance is determined. The Secretary will take into consideration reasonable cause, reasonable diligence, or willful neglect:
       - For a violation where the agency did not know, and by exercising reasonable diligence would not have known: a) an amount of less than $100, or more than $50,000 for each violation, or b) in excess of $1,500,000 for identical violations in a calendar year.

    - For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect: a) an amount of less than $1,000 or more than $50,000 for each violation, or b) in excess of $1,500,000 for identical violations in a calendar year.
    - For a violation due to willful neglect and is corrected within a 30 day period beginning on the first date the agency knew, or by exercising reasonable diligence, would have known the violation occurred: a) an amount of less than $10,000 or more than $50,000 for each violation, or b) in excess of $1,500,000 for identical violations in a calendar year (January 1 through December 31).
    - For a violation due to willful neglect and is not corrected within a 30 day period beginning on the first date the agency knew, or by exercising reasonable diligence, would have known the violation occurred: a) an amount of less than $50,000 for each violation, or b) in excess of $1,500,000 for identical violations in a calendar year (January 1 through December 31).
- <u>Procedure for clients to access, and when appropriate, amend their health data</u>:
  1. Clients have the right to inspect and request a copy of their Protected Health Information in either a paper or electronic format. The agency may not charge the client (including a representative or guardian) for a copy of their record. If the copy is for another provider, the agency may charge 75 cents per page and $10.00for time spent making the copy.
  2. The agency will allow timely access for the client. The agency will respond as quickly as possible, but must comply within 30 days.
  3. If the record is large, and the client agrees, a summary of the Protected Health Information may be provided instead of the complete record.
  4. The agency may deny access, subject to an appeal, if the request is for information that the agency believes to be reasonably likely to endanger the life or physical safety of the individual or another person, or to cause substantial harm to the individual or another person. Denials are subject to a review by a licensed health professional who did not participate in the original decision to deny access. The denial must be timely and in writing, must state the reason for denial, the individual's appeal rights, a description of the complaint process, and contact information. The agency must, to the extent possible, provide access to other protected health information that is requested.
  5. The client has the right to request an amendment to their record if they believe the information is incorrect. The request must be made in writing and include the changes being requested. A copy of the request will be maintained in the record. If the agency accepts the amendment, it will inform others of the changes at the client's request if the information has been previously disclosed to them. The agency may deny the request if the record was not created by them, or if they believe the record is correct. The agency will provide written notice of the denial indicating the basis for the denial, the client's right to submit a "Statement of Disagreement" for the record, and the complaint process and contact information. If a statement of Disagreement is submitted, it along with the agency's letter of denial will be included in the record and included in future disclosures. The agency will let the client know in writing within 60 days of receiving the request for an amendment if the amendment was accepted or denied.
  6. Electronic access with the Credible Client Portal: Clients are able to access their health care record, which can include contacts, schedule, treatment plans, and medications. Clients will also be able to send a message to their treatment team or primary staff if the client needs a medication refill, has a question about a scheduled appointment, or would like to send a general message. Staff will provide and assist the

client in filling out a "Client Portal Registration Form." After the client completes the form and receives their login information, they can create their own password and have immediate access to their record by logging into: www.credibleportal.com.

- Accounting of disclosures of protected health information – the agency will maintain a tracking system to allow clients to receive an accounting of disclosures of protected health information. Clients have the right to request an accounting of the disclosures of their Protected Health Information for the past 8 years. The agency must act on the request within 60 days. The accounting must be in writing and include the date of the disclosure, name of recipient (and address, if known), a brief description of the PHI, and a statement of the purpose for the disclosure. The agency maintains a copy of the written accounting given to an individual. All clinical staff (mental health Rehabilitation workers, mental health practitioners, mental health professionals, registered nurses, clinical supervisors, and program directors, are responsible for receiving and processing requests for an accounting of disclosures by an individual.

  If the agency has made multiple disclosures of PHI to the same person or entity for a single purpose, the agency may provide the information required under this section by giving a summary of the frequency, periodicity, or number of the disclosures made during the accounting period, and the date of the last such disclosure during the accounting period.

  The following are not subject to an accounting of disclosures:
  1. To carry out payment and health care operations as provided in 164.506
  2. To the individual of the PHI
  3. Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in 164.502
  4. Pursuant to an authorization
  5. For a facility Directory, or incidental information to family members
  6. For national security
  7. To correctional institutions or law enforcement

  The agency must temporarily suspend an individual's right to receive an accounting of their PHI disclosure if a health oversight agency or law enforcement official, as provided in 164.512(d) provides a written statement stating the disclosure would impede an investigation and specifying the time for which such a suspension is required. If the request is verbal, the agency must document the identity of the official making the request and limit the suspension to 30 days, unless a written statement is provided.

  Credible is the electronic health record the agency uses. The software tracks and creates a log of every employee who accesses the client's chart. Employees shall document in the individual's chart any time they make a disclosure to an outside party, and any HIPAA breach.

- Staff access to health data: the agency will determine:
  1. Those persons or classes of persons in its workforce who need access to protected health information.
  2. For each person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

3. The agency will make reasonable efforts to limit the access of such person or classes of persons to PHI

- Business Associates: The agency will maintain proper Business Associate contracts that include the following:
  1. Establish the permitted and required use of the information. Information cannot be further disclosed in a manner that would violate state or federal law.
  2. The BA will use appropriate safeguards to prevent use or disclosure of the information other than provided by its contract
  3. The BA will report to the agency any disclosure not covered by the agreement when it becomes aware of it.
  4. The BA will ensure that any subcontractor it uses will comply with the same standards in the contract.
  5. The BA agrees to amend protected health information as required in 164.526.
  6. The BA agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created by the BA, available to Secretary for purposes of determining compliance.
  7. At the termination of the contract, if feasible, return or destroy all PHI.
  8. Authorize termination of the contract if the agency determines that the business associate has violated a material term of the contract.
  9. If the agency believes the BA is not in compliance with the contract, the agency will attempt to resolve the matter informally with the BA. If resolution is not achieved, the agency will bring the matter to the Secretary.
  10. Violation and civil money penalties:
      - The agency is liable for a civil money penalty for a violation by a business associate acting within the scope of the agency.
      - The business associate is liable for a civil penalty for a violation by a member of its workforce or subcontractor acting within the scope of the agency. .
- Trading Partners Agreements: The agency will maintain Trading Partners agreements with those agencies where there is an exchange of electronic information that is not otherwise addressed through a Business Associate Agreement, or is an affiliated entity.
  - Due Process protections and sanctions for non-compliance:

  The agency will establish Business Agreement contracts where necessary and monitor compliance. Supervisory staff will monitor compliance of their employees. The federal and state government has established penalties for failing to comply with these standards.
    - Federal government: The federal monetary penalties were described earlier.
    - State government– MN AGO is authorized to bring civil action in federal court against persons who violate protected health information if AGO has reason to believe that violation threatens or adversely affects resident of MN. MN can fine $100 per violation with a cap of $25,000 for violations within a calendar year, plus costs and attorneys' fees. A willful violation can be fined an additional amount of $1,000 to $15,000.
- Providing information to clients about their rights regarding health information:
  1. The agency will develop and maintain a Notice of Privacy Practices that it will post at each site of service delivery and be given to the client at the time of the first service delivery.
  2. Clients have the right to access their records to review or copy. Clients may request a copy of their record in either a paper or electronic format

3. Clients may request amendments to their records if they believe there is an error in the information, pursuant to 45 CFR Part 164.526.
4. Clients may request restrictions on the release of protected health information.
5. Clients can restrict disclosure of their PHI to a health plan, if the disclosure is for payment or health care operations purposes and it pertains solely to services for which the agency was paid in full by the client.
6. Clients may request an accounting of disclosures.
7. Clients may file a complaint with the agency and the Secretary if they believe the agency has not complied with federal and state regulations regarding the management of health information.

- Duty to mitigate, refrain from retaliatory acts:
  1. The agency has a responsibility to mitigate, to the extent possible, any harmful effect known to have occurred due to the disclosure of PHI in violation of its policies and procedures, or the requirements of the Privacy Regulations, or an agency's Business Associate.
  2. The agency may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of any right, or the participation in any process established by the Privacy Regulations in regard to their PHI. This includes filing a complaint with DHSS against the agency, testifying, assisting or participating in an investigation, compliance review, proceeding, or hearing under the HIPAA, opposing any act or practice made unlawful by HIPAA, provided the person has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and doe not involve a disclosure of PHI in violation of the Privacy Regulations.
- "Minimum Necessary assumption": In disclosing or requesting PHI, staff must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, ore request. The minimum necessary requirement does not apply to:
  1. Disclosure to or requests by a health care provider for treatment.
  2. Uses or disclosures made to the individual, as permitted for treatment, payment or healthcare operations.
  3. Uses or disclosures pursuant to an authorization.
  4. Disclosures made with respect to compliance and enforcement.
  5. Disclosures that are required by law, as described by victims of abuse, neglect, or domestic violence, judicial or administrative proceeding, and law enforcement purposes.

## IV: ELECTRONIC DATA INTERCHANGE (EDI):

The agency's Information and Technology (IT) Department is tasked with the development and maintenance of an electronic clinical record and electronic billing system. The agency's hardware and software meet or exceed the published requirements under HIPAA.

## V: SECURITY AND PRIVACY 45 CFR 164.000

The Security Standards in this section define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. These standards are intended, to the best of our ability, to secure electronic protected health information from unauthorized access, alteration, deletion, and transmission.

When a standard adopted in 164.308, 164.310, 164.312, 164.314, or 164.316 includes a required change the agency and business associates will implement the changes. If a standard adopted in 164.308, 164.310, 164.312, 164.314, or 164.316 includes addressable changes the agency and business associate will consider the change if it is a reasonable and appropriate safeguard in our environment and will contribute to protecting PHI. If implementing the changes are not reasonable and appropriate, the agency and business associate will document the reason and implement an equivalent alterative measure if reasonable and appropriate

**General Rules:**

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the entity creates, receives maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
- Ensure compliance with the workforce.
- Ensure compliance with our Business Associates. The agency considers the size and capabilities of BA's, their technical infrastructure, hardware and software, costs of security measures, and the probability of potential risks to unauthorized PHI disclosures.
- The agency will continue to review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection.

**Administrative Safeguards:**

- <u>The agency will maintain policies and procedures to prevent, detect, contain, and correct security violations</u>.
    1. Risk Analysis – The agency maintains electronic protected health information (PHI) that some employees need to create, modify, or access. Staff may access data over the internet or from a workstation. PHI is electronically transmitted for billing and clinical purposes. Electronic PHI data is maintained by the electronic health record provider (Credible) that is accessible to employees by the internet. PHI is also maintained on a network that is managed by employees and business associates. Data is backed up and the backup media is stored.
    2. Risk Management – The agency has policies and procedures consistent with 45 CFR Part 164.306(a), to reduce risks and vulnerabilities to a reasonable and appropriate level. The agency provides initial and ongoing training to employees, maintains proper business associates agreements, monitors and incorporates new hardware and software applications that ensure security of PHI. The agency regularly reviews its information system as business activity and technology evolve.
    3. Information System activity review – management will regularly review records of their Information System activity, such as audit logs, access reports, and security incident tracking reports.
- <u>Assigned security respon</u>sibility – Terry Schneider is the security official who is responsible for the development and implementation of the policies and procedures required by HIPAA.
- <u>Workforce security</u>:
    1. Authorization and supervision: Management will identify those positions that require access to PHI based on the duties the employee will be involved in and assign the position a security level. There are multiple levels, including; "no access," "read only" and "create and edit" rights for specific programs. Staff will be instructed not to look at

client PHI unless they have a clinical need for the provision of service or other work related reason (e.g., supervision, training). Program managers and clinical supervisors will periodically use the "Log" feature of the electronic chart that indicates all of the charts that their employees have looked in to make sure they are not accessing PHI for non work related reasons.

2. Workforce clearance procedure: Management will periodically review security level assignments for the employees to determine their appropriateness.
3. Training – the agency will train all members on its workforce on the policies and procedures with respect to PHI no later than the compliance date for the agency or when a material change in the policies and procedures occurs. All new employees will be trained within a reasonable period of time after the person joins the work force. The agency will maintain documentation of the training in the employee's personnel file.
4. Termination Procedures – Human Resources will notify the Network Administrator the date and time when an employee terminates their employment. The Network Administrator will disable the individual's ability to access the agency's network.
5. The agency will apply appropriate sanctions against workforce members who fail to comply with the security policies and procedure which may include termination. The agency will maintain documentation of sanctions to employees who violate the policy and procedures.

- <u>Information access management</u>:
  1. Isolating health care clearing house functions – The agency may engage in billing activity for other individuals or agencies. The agency will adopt procedures to protect PHI received from other providers from unauthorized access by employees of the agency. The agency will develop and maintain Business Associate Agreements and limit the access of that data to the agency's employees directly involved in the billing process.
  2. Access Authorization – Human Resources will notify the Network Administrator of a new hire, or when an existing employee changes to a new job within the agency. The Network Administrator will set up a log in and a unique password for the employee and provide access to the network based on the security level assigned to the job position.
  3. Access establishment and modification – Management will periodically review job descriptions and security levels. The agency's security official will notify the Network Administrator if a change is needed in access, or security level for a job position or an individual employee.
- <u>Security awareness and training</u>:
  1. Security reminders – All new employees who have access to PHI will receive initial and recurrent training on the management of PHI. Management will notify employees of security threats as they become aware of them.
  2. Protection from malicious software – the Network Administrator will monitor threats and notify the security official and other employees of potential threats. The Network Administrator is responsible for recommending additional software or hardware to guard against such threats.
  3. Log in monitoring – The Network Administrator is responsible for monitoring log attempts and reporting discrepancies to the security official.
  4. Password management – The Network Administrator is responsible for assigning a temporary password to an employee. Employees must then create a new password that is 8 characters long and must contain letters, numbers and a special character. If an employee becomes concerned about the security of their password they must create a new password and notify the Network Administrator.

- Security incident procedures – All staff are required to report to their supervisor, the Network Administrator or the Privacy and Security Officer any known or suspected security incidents within the agency or business associates. The agency will attempt to mitigate any harmful effects of security incidents and document security incidents and their outcomes.
- Contingency plan:
  1. Data backup plan – The EHR provider (Credible) maintains the data at a secured site with multiple back up storage systems. Information maintained by the agency is stored on a network designed with redundant systems and is backed up daily with an encrypted system. The backup data media is stored off site in case of substantial damage to the site. There is an emergency power supply at the facility to allow the network to save the data and automatically shut down in the event of a power outage.
  2. Disaster recovery plans – The redundant systems in Credible and the agency network are fairly robust and individual components can fail without interrupting the operations of the network. The agency system has successfully recovered from power failures and data has been successfully restored from the backup media.
  3. Emergency mode operation plan – PHI maintained by Credible is accessible to staff through the internet. The vast majority of current agency activity is now managed by Credible. PHI maintained by the agency network would only be down for a few hours unless there was substantial damage to the site. Significant site damage could have the network system down for a day or more. During this time the electronic data itself would be secure, but not necessarily accessible. There may be a paper backup for some of the data, but it may not survive significant site damage as well. The amount of capacity the agency has to operate under these emergency situations is appropriate given the nature of the health care the agency provides.
  4. Testing and revision procedures – The Network Administrator is responsible for checking and maintaining the backup systems and monitoring new technology that would provide greater capacity to operate in an emergency mode.
  5. Applications and data criticality analysis – The agency uses a combination of an EHR provided and maintained by Credible, retail software and propriety software. All software applications and data are backed up with sufficient redundancy to prevent loss. The hardware could be destroyed if there was significant site damage. Although this does not impact the data, it could be some time before the hardware could be replaced and the applications and data restored. Credible and remote sites rely on phone lines to access the client chart and agency network data, damage to the phone system (internal or from the phone company) would limited access for remote sites until the phone damage could be repaired.
- Evaluation
  1. Management will perform periodic technical and non-technical evaluations based on this rule, and subsequent revisions of the rule, to environmental or operational changes affecting the security of electronically PHI.
  2. Management will periodically review its Business Associate Agreements to ensure compliance with 45 CFR Part 164.314(a).
- Business Associates:
  1. The agency will permit a business associate to create, receive, maintain or transmit electronic protected health information on the agency's behalf only it the agency receives satisfactory assurances that the business associate will safe guard the information.

2. The business associate may permit a subcontractor to create, receive, maintain, or transmit only if they receive satisfactory assurances that the subcontractor will safe guard the information.
3. The agency will maintain written business associate agreements with their business associates that meet the requirements of 164.314(a).

**Physical Safeguards:**

- Facility access controls:
  1. Contingency operations – Network administrative staff have access to the facility and the computer room 24 hours a day, 365 days per year to allow restoration of lost data.
  2. Facility security plan – The agency network system is stored at the facility in a locked room, only employees engaged in Network Administration have access to the room.
  3. Facility access control and validation procedures – employees are given either a key or an access code to enter the building. Access codes are changed periodically.
  4. Physical maintenance records – management will review repairs and modifications to hardware, walls, doors, and locks that might impact security.
- Workstation use – supervisory employees will receive training from the network administrator on the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation. Supervisory staff will train their staff on the proper use of the workstation with backup support from the Network Administrative staff.
- Workstation security – all workstations require a proper log in and password to access PHI.
- Device and media controls:
  1. Final disposition of hardware, or electronic media – Electronic PHI will be maintained as long as required by federal and state rules, and indefinitely in some cases. Electronic PHI that is to be destroyed will be done in a manner consistent with the software application. Hardware will be destroyed in a manner that will prevent its use or recovery of data.
  2. Media re-use – Due to the difficulty of removing PHI from an electronic media, media that has been used for PHI will not be re-used and will be destroyed in the manner described above.
  3. Accountability of hardware, electronic media – the agency will maintain a list of hardware and electronic media; any person assigned to it; and notes the destruction date.
  4. Data backup prior to movement of network – the Network Administrator will create an exact copy of electronic PHI before the network is moved to any other site.

**Technical Safeguards:**

- Access control:
  1. Unique user identification – all employees using electronic PHI will be assigned a unique login name and they then must create a unique password to access PYI. The EHR has built in audit functions to identify and track the user identity.
  2. Emergency access procedures – the agency uses a web accessed electronic chart. If the employee has access to the internet they have access to the chart
  3. Automatic log off – all workstations that are not located in a private office will have an automatic log off after 15 minutes of inactivity.
  4. Encryption and decryption – data that is electronically transmitted is encrypted. The agency internal information system also uses encryption for emails that contains PHI.

- Audit controls – The network administrator will implement hardware, software and/or procedural mechanisms that record and examine activity in the information system that contain PHI.
- Integrity – the agency will utilize a variety of methods to protect electronic PHI from improper alteration or destruction. These methods include access controls, data backup, and may include other electronic mechanisms to corroborate the electronic PHI has not been altered or destroyed in an unauthorized manner. The Credible EHR tracks the person, time and any change that was made to the record. Supervisors and IT staff can view the log activity to ensure that only appropriate staff members are accessing the files.
- Person or entity authentication – the primary control to verify the identity of the person seeking access to PHI is through the built in tracking function in Credible. The agency's network has a similar tracking capacity to monitor access and use by employees
- Transmission security – the agency uses the following steps to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.
    1. Integrity controls – the Network Administrator will evaluate hardware, software and procedures to ensure that electronic PHI is not improperly modified without detection until disposed of.
    2. Encryption – The Network Administrator will use hardware and software to properly encrypt data when they deem it is appropriate.

**Organizational requirements:**

- Business associate contracts or other arrangements – The contract between the agency and a business associate (BA) must provide that the BA will:
    1. Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirement of 45 CFR Part 164.504, except that the business associate may use and disclose protected health information for the proper management and administration of the business associate.
    2. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI it creates, receives, maintains, or transmits on behalf of the agency.
    3. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safe guards
    4. Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with 45 CFR Part 164.526
    5. Make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528
    6. Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of the agency, available to the Secretary for purposes of determining the agency's compliance with rule.
    7. Report to the agency any security incidents of which it becomes aware
    8. At termination of contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of the agency, that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the

contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

9. Authorize termination of the contract by the agency if the agency determines that the BA has violated a material term of the contract. If termination is not feasible, the agency will report the problem to the Secretary.
10. The agency may comply with this section by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of this section.
11. The agency may comply with this section if other law or regulations adopted by the agency or its business associate contains requirements applicable to the business associate that accomplish the objective of the section.
12. That agency may omit from its other arrangements the termination authorization required by this section if such authorization is inconsistent with the statutory obligations of the agency or its business associate.

**Policies, procedures and documentation requirements:**

- Policies and procedures – The agency agrees to implement reasonable and appropriate policies and procedures to comply with HIPAA standards, implementation specifications or other requirements of HIPAA. The agency may change it policies and procedures at any time, provided the changes are documented and implemented in accordance with HIPAA standards.
- Documentation:
  1. The agency will maintain these procedures in a written (which may be electronic) form.
  2. If any action, activity or assessment is required by HIPPA to be documented, the agency will maintain a written (which may be electronic) record.
  3. Time limit – the agency will retain the documentation required by HIPPA for 6 years of its creation or the date when it last was in effect, whichever is later.
  4. Availability – the documentation will be available to those persons responsible for implementing the procedures to which the documentation pertains.
  5. Updates – the management will review documentation periodically and update as needed, in response to environmental or operational changes affecting the security of the electronic PHI.

**VI: PRIVACY: 45 CFR 164.000, Minnesota Statutes**

**Standards for Privacy of Individually Identifiable Health Information:**

Data on Individuals maintained by this agency:
Information that is collected on individuals by this agency may be defined in different terms by applicable federal and state regulations. The terms for both federal and state regulations are included in this section although there may be significant overlap.

- Confidential data (is not available to the subject of the data)
  1. Raw test scores
  2. Information that would be harmful to the client, or likely to cause the client to act in a harmful manner to someone else.
  3. Adult protection, child protection, information complied in reasonable anticipation of or, for use in, a civil, criminal or administrative action or proceeding.
- Health information

- Individually identified health information
- Private data, including
    1. All medical data
    2. Mental health data
    3. data on the individual produced by the agency
    4. data or information obtain from other sources
- Protected Health Information

Services to multiple clients: When services are provided to multiple clients, the provider shall initially inform each client of the provider's responsibility to treat any information gained in the course or rendering the services as private information, including any limitation to each client's right to privacy.

Multiple client records: when services are provided at the same time to dual or multiple clients, each client has a right to access only that part of the records that includes information provided directly by the client, unless otherwise directed by law or court order.

Obtaining collateral information: prior to obtaining collateral information about a client from other individuals, the provider shall inform the other individuals that the information obtained may become part of the client's records, and may be accessed or released by the client unless prohibited by law. A provider is not required to give prior informed consent to other individuals when those individuals are credentialed health care providers acting in their professional capacities.

Family or marriage therapy:
The therapist must define who the client is (individual, couple, family as a whole) for the purposes of safeguarding client information. The therapist must maintain an accurate record for each client that contains at least the following:

- A client personal data record and presenting problem
- A treatment plan with a diagnosis and justification for it and treatment goals
- An accurate chronological listing of all client contracts and a summary of each
- Records of any consultation or supervision received in relation to the client.
- A termination statement or case summary indicating date and reason for termination, the client's condition at the time, and any recommendations made to the client.
- Copies of client authorization for release of information and any legal forms pertaining to the client.
- Chronological listing of all fees, separate from the clinical record

Information obtained during the course of family or marriage therapy may not be disclosed unless

- each person or family member grants written consent
- Disclosure is required by law
- Failure would create a clear and present danger to the health safety on an individual
- The agency is a defendant in civil, criminal, or disciplinary action arising from the therapy proceeding and the use of the privilege would violate the agency's right to defend itself.

Minors:

- At the beginning or a professional relationship, the staff person shall inform a minor client, to the extent that the client can understand, that the law imposes limitations on the right of the privacy of the minor with respect to the monitor's communication with the staff person.
- A minor does not need parental approval to seek treatment for a substance use disorder.
- Minor living apart from parents and managing financial affairs: regardless of the source or extent of income, a minor may give effective consent to personal medical, dental, mental and other health services and the consent of no other person is required.
- Staff may inform the parent or legal guardian of the minor patient of any treatment given or needed where, in the judgment of the professional, failure to inform the parent or guardian would seriously jeopardize the health of the minor patient

Observation and recording: Diagnostic interviews or treatment sessions with a client may be observed or electronically recorded only with the written informed consent, except as otherwise provided by law or court order.

Continued privacy of client information: the provider shall continue to maintain the privacy of client information, including the records of a client, after the professional relationship between the provider and the client has ceased.

Record retention**:** Records shall be maintained for a minimum of 8 years after the date of the last professional service to the client, except as otherwise provided by law. If the client is a minor, the records retention period shall not commence until the client reaches the age of 18, except as otherwise provided by law.

**Uses and disclosures of protected health information and Private data: 45 CFR Part 164.504**

Permitted uses and disclosures of PHI include**:**

- Uses and disclosures to carry out treatment, payment, or health care operations. 45 CFR part 164.506.
- To a Business Associate with a Business Associate Agreement in place.
- Disclosures to the Secretary in accordance with subpart C of 160
- Uses and disclosures that are required by law.
- De-identified health information
- Deceased individual: 50 years after the death of the individual
- Disclosure of PHI by a workforce member who is a victim of a crime to law enforcement, the PHI disclosed must be about the suspected perpetrator of the criminal act and be the minimum necessary.
- Use or disclosure by the agency to defend itself in a legal action or other proceeding brought by the individual.
- Disclosure to the parents or guardian of un-emancipated minor
- Disclosed to the individual**: (**adult or emancipated minor)
    1. The individual has rights to access their PHI. They can request a copy of their health record in a paper or electronic format. Rights and limitations are described further under "General Responsibilities." A personal representative with proper legal authority has the same rights as the individual

2. A Representative of the decedent has the same rights as the individual. A representative of the decedent means (in order) the personal representative of the estate, the surviving spouse, any child of the decedent, or if there is no surviving spouse or child, the parents of the decedent.
3. The agency may elect not to treat a person as the personal representative of an patient if the agency has reasonable belief that the patient may be subjected to abuse, neglect or domestic abuse or if treating the person as the personal representative could endanger the individual and the agency exercises professional judgment that it is not in the patient's best interest to treat a person as the personal representative.

- Access denied to the individual:
  1. Clients do not have access to data classified as confidential. Confidential data includes Child Protection, Adult Protection, Ombudsman's Office.
  2. An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
  3. The agency may deny access if the treating professional has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse or neglect by such person.
  4. To the parent, guardian, or other person acting in *loco parentis* on behalf of the minor, a licensed health care professional in the exercise of professional judgment may provide or deny access consistent with state or other applicable law.
  5. A licensed health care professional has determined, in the exercise of professional judgment, the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
  6. The PHI makes reference to another person (unless the other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
  7. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
  8. Review of a denial of access – if access is denied on a ground permitted under this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the agency to act as a reviewing official and who did not participate in the original decision to deny. The agency must provide or deny access in accordance with the determination of the reviewing official under this section.
- Pursuant to an Authorization**:** 45 CFR Part 164.508
  1. General Provision – This agency may not use or disclose identifiable private, confidential, or protected health information on an individual, unless there is an authorization (informed consent) from the individual, or if the disclosure is to carry out the administration of a program authorized by rule or state or federal law, or otherwise allowed for by state or federal law.
  2. Psychotherapy notes – require an authorization, except if used or disclosed to carry out the following treatment, payment, or health care operations
     - Used by the originator of the information for treatment
     - Use or disclosure by the agency for its own training programs

- Use or disclosure by the agency to defend itself in a legal action or other proceeding brought by the individual.

3. Marketing – any marketing activity requires an authorization except for the following
   - If the information was conveyed in a face to face communication
   - Is limited to a promotional gift of nominal value
   - If the marketing involves direct or indirect remuneration from a third party, the authorization must state that such remuneration is involved.
4. Criminal Mental Health Court – information may be provided in advance of receiving a copy of consent if
   - The client is a defendant in a criminal case pending in the district court
   - The data is necessary to determine the client's eligibility to participate in Criminal Mental Health Court
   - The client has consented to the release of mental health data and a copy of the consent will be provided in 72 hours.
5. An authorization must include:
   - A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion
   - The name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure. Staff must verify the identity and the authority of the person requesting PHI.
   - The name or other specific identification of the person(s) or class of persons, to whom the agency may make the requested use or disclosure.
   - A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is sufficient if the individual initiates the authorization.
   - An expiration date, which cannot exceed one year.
   - Signature of the individual and date. If the authorization is signed by a personal representative, a description of the representative's authority to act for the individual must also be provided.
   - The individual's right to revoke the authorization
   - The individual must be offered a signed copy of the authorization.
   - Notice that treatment, payment, enrollment, or eligibility is not conditioned on whether the individual signs the authorization.
   - The potential for information disclosed to be re-disclosed by the recipient and no longer protected.
   - Written in plain language.
   - Chemical dependency records are governed by the Code of Federal Regulations, Title 42, sections 2.1 – 2.67. They must contain this statement:
     "This information has been disclosed to you from records protected by Federal Confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of information is not sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."
   - Compound authorizations are not allowed except for: a research study may be combined with another research study.

6. Timely action by the agency: the agency must act on a request for access no later than 30 days after receipt of the request as follows:
   - If the agency grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested.
   - If the agency denies the request, in whole or in part, it must provide the individual with a written denial.
   - The agency must provide the PHI in the form or format requested by the individual, if it is readily producible in such form or format
   - The agency may provide the individual with a summary of the PHI if the individual agrees in advance to such a summary.

- **Permitted use or disclosure of PHI without authorization, provided the individual has the opportunity to object: 45 CFR Part 164.510**
  1. The agency may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure.
  2. Facility directory – limited to name, location in facility, a general statement of condition that does not communicate specific medication information about the individual. If the individual is unable to agree or object due to an incapacity or an emergency, the directory information may be disclosed if the provider determines it is consistent with a prior expressed preference, or if the disclosure is in the individual's best interest
  3. Disclosure to family members and other responsible person – provider may disclose if the person is directly involved, and the PHI is directly relevant to the involvement. If the individual is unable to agree or object, the provider may use professional judgment in determining whether to disclose PHI. Examples include individual's location, general condition or death.
  4. The agency may use or disclose protected health information to notify, or assist in the notification of a family member, personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.
  5. Uses and disclosures with the individual present - the agency may disclose PHI if the individual is present and gives consent, has the opportunity to object and does not express an objection, or the agency reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.
  6. In an emergency if the individual is incapacitated, the agency may disclose information that is in the best interest of the client. The agency will notify of the individual of the disclosure when their condition allows.
  7. Disaster relief efforts – the agency may disclose PHI to a public or private entity authorized by law or charter to assist in disaster relief.

- **Permitted use or disclosure of PHI without authorization, or opportunity to object: 45-CFR – Part 164.512**
  1. For treatment, payment, or health care operations, as permitted by and in compliance with 45 CRF 164.506. The individual may restrict this disclosure if the individual, and not the health plan has paid for the service in full and the disclosure is not otherwise required by law.
     - The agency may use or disclose PHI for its own treatment, payment, or health care operations.

- May disclose PHI for treatment activities of a health care provider
- May disclose PHI to another covered entity or a health care provider for the payment activities of the entity that receives the information
- May disclose to another covered entity for health care operations or fraud and abuse activities if the entity that receives the information, has or had a relationship with the individual who is the subject of the PHI.
- For the purpose of health care fraud and abuse detection or compliance

2. As described in 164.508 (exceptions to authorization required)
3. As described in 164.510 (uses and disclosures where the individual can object)
4. Pursuant to an agreement under, or as otherwise permitted, by 164.510
5. To a Business Associate if the agency obtains satisfactory assurance that the business associate will appropriately safeguard the information
6. When required by the Secretary
7. Specifically authorized agencies by state, local, or federal law. This includes the Minnesota Department of Human Services and the Minnesota Department of Health, Board of Psychology, Board of Social Work, Board of nursing, Behavior Health Board, MN Medical Board.
8. To a health oversight agency authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the agency, or to appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the agency.
9. To collect or report adverse events, product defects or problems with labeling, to enable product recalls.
10. To track FDA regulated products, to enable product recalls
11. To a person who may have been exposed to communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if authorized by law.
12. To an agent of the welfare system, including law enforcement person, attorney, or investigator in the investigation or prosecution of a criminal or civil proceeding relating to the administration of a program.
13. To personnel of the welfare system who require the data to determine eligibility, amount of assistance, and the need to provide services of additional programs to the individual.
14. To administer federal funds or programs
15. Between personnel of the welfare system working in same program
16. The amounts of cash public assistance and relief paid to welfare recipients in this state, including their names, social security number, income, addresses, and other data as requested to administer the property tax refund law, supplemental housing allowance, early refund of refundable tax credits, and income tax
17. Between DHS and department of economic security
18. Government contracts – to satisfy regulatory and contractual compliance and program efficiency.
19. To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, an individual patient in any report of such research, audit, or evaluation, or otherwise disclose patient identities in any manner.
20. Institutional Review Board – pursuant to 164.512 restrictions
21. The agency may use or disclose protected health information to defend itself in a legal action or other proceeding brought by the individual and that use or disclosure is required by 164.502 or permitted by 164.512.

22. Judicial and administrative proceedings
    - In response to a court order, subpoena
    - Commitment proceeding under MS 253B
23. Law enforcement
    - Court ordered warrant, subpoena or summons by a judicial officer, a grand jury subpoena
    - May disclose PHI of a deceased person for the purpose of alerting law enforcement of the death of the individual if the agency has a suspicion that such death may have resulted from criminal activity.
    - for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that only the following information be given:
        1. Name and address
        2. Date and place of birth
        3. Social security number
        4. ABO blood type and rh factor
        5. Type of injury
        6. Date and time of treatment
        7. Date and time of death
        8. A description of distinguishing physical characteristics, including height, weight, gender, race hair and eye color, facial hair, scars, and tattoos, photograph
        9. The agency may not disclose DNA, or dental records, or samples of body fluids.
    - Victims of a crime, if:
        1. An authorization is obtained from the individual, or if unable due to incapacity
        2. The law enforcement official represents that immediate law enforcement activity would be materially and adversely affected by waiting until the individual is able to agree, and
        3. The disclosure is in the best interests of the individual, as determined by the agency's professional judgment.
    - Commission of a crime on premises of the program, or against program personnel, or to a threat to commit such a crime. Information that may be released includes circumstances of the incident, including the patient status of the individual committing or threatening to commit the crime, that individual's name and address, and that individual's last know whereabouts.
    - Reporting a crime
    - Reporting the individual's death
    - Client is involved in an emergency interaction with a law enforcement agency and the data is necessary to protect the health and safety of the client or another person – the mental health provider <u>must</u> disclose the minimum necessary for law enforcement to respond to the emergency. Disclosure may include, but is not limited to, the name and telephone number of the psychiatrist, psychologist, therapist, mental health professional, practitioner, or case manager.
    - Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.
    - To a correctional institutions and other law enforcement custodial situations for the health care of the individual, safety of the individual or other, to law enforcement who may be transporting inmates from one location to another.

24. Emergency situations: the individual should be notified if a disclosure has been made, unless in the professional judgment of the agency, it would in some manner harm the individual.
    - To appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the individual or other individuals or persons
    - For a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency
19. Activities under MS 253B (civil commitment)
20. Duty to warn – a duty exists when a client (or other person who knows the client) has made a serious, specific threat of harm to an identifiable victim and the provider believes the client is capable and has the means to carry out the threat. The provider must make reasonable efforts to warn the potential victim and failing that, the provider must notify law enforcement.
21. To avert a serious threat to health or safety of a person or the public, to a person or persons reasonably able to prevent or lessen the threat, including the target of a threat, or as necessary, to law enforcement to apprehend an individual.
22. Adult or child protection – the agency may disclose PHI to an agency authorized by law to receive reports of abuse, neglect, financial exploitation, domestic violence.
23. To other providers within related health care entities when necessary for the current treatment of the patient.
24. Ombudsman's office to report a serious injury or death
25. Notice of Privacy Practices statement (Tennessen Warning) 45 CFR Part 164.520: this statement informs the individual, either orally or in writing, why the agency is collecting the data, and who will have access to the data. The following items must be included:
    - HIPAA requirements:
        1. The notice must contain the following language as a header "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATON. PLEASE REVIEW IT CAREFULLY."
        2. Uses and Disclosures must contain:
            - Notice that uses and disclosures are permitted without authorization for treatment, payment, health care operations
            - Describe disclosures that are permitted or required by law without an authorization
            - Statement that if a use or disclosure is prohibited or materially limited by other applicable law, the more stringent law applies
            - A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke the authorization at any time.
        3. Individual Rights:
            - Right to request restrictions on certain uses and disclosures of Protected Health Information (PHI). The client may request that this agency restrict uses or disclosures to carry out treatment, payment, health care operations, or other disclosures required or permitted by state or federal law. The agency is not required to agree to a specific restriction if it determines a disclosure is in the client's best interests.
            - The right to receive confidential communications of their PHI

    - The right to inspect and copy PHI
    - The right to amend PHI
    - The right to receive an accounting of disclosures of PHI
    - The right of an individual who has agreed to receive notice electronically of this privacy statement to receive a paper copy.
  4. Agency's Duties: The agency is required by federal and state laws to maintain the privacy of protected health information and to provide individuals with a notice of its legal duties and privacy practices. This notice will be posted at each facility and offered to the client at the time of their first visit. The agency must abide by the notice in effect, but maintains the right to revise the terms of this notice. Clients will be provided with a copy of revised notices at the time of their next appointment.
  5. Complaints: The client may file a complaint with this agency or the Secretary of Health and Human Services if they believe their privacy rights have been violated. The complaint must be written and filed within 180 days of the date they knew, or should have known their rights were violated.
  6. Contact: If you have questions about this information you may contact Terry M. Schneider, MA, Licensed Psychologist, 166 4Street E, Saint Paul, Minnesota 55101 or 651-256-1211.
- Minnesota requirements (Tennessen Warning)
  1. Why the data is being collected
  2. How the agency intends to use the information
  3. Whether the individual may refuse or is legally required to furnish the information
  4. What know consequences may result from either providing or refusing to disclose the information
  5. With whom the collecting agency is authorized by law to share the data

24. County medical examiner, Coroner, funeral director
25. Disclosure for cadaveric organ, eye, or tissue donation
26. A public health authority authorized by law to collect information for the purpose of preventing or controlling disease, injury, or disability.
27. Food and Drug Administration (FDA) to report adverse events, track FDA regulated products, exposure to a communicable disease.
28. Armed Forces Personnel – if authority is published in the Federal Register
29. National Security and Intelligence – federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act.
30. For an employer to comply with workers compensation laws or OSHA
31. Uses and disclosures for specialized government functions
    - PHI may be released to Armed Forces personnel for activities deemed necessary by military authorities
    - PHI may be disclosed to federal authorities for National Security and intelligence activities.
    - PHI may be released to the Department of State to determine medical suitability.
    - For purpose of a required security clearance conducted pursuant to Executive Orders 10450.
32. Protective services for the President and others authorized by 18 U.S.C. 3056
33. To corrections
    1. For the provision of health care

2. Health and safety of individual or other inmates
3. Health and safety of the officers or others at the facility
4. For law enforcement officers transporting the inmates

- **Breaches of protected health information under HIPAA:**
  Breach of protected health information – acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of 45 CFR 164.402.
  - A breach excludes:
    1. Any unintended acquisition, access, or use of PHI by an employee, business associate or person acting under the authority of the agency, if the acquisition, access, or use was made in good faith and within the scope of their authority and does not result in further use or disclosure in a manner not permitted.
    2. Any inadvertent disclosure by an employee, business associate or person acting under the authority of the agency to another person at the agency who is authorized to access PHI, if the disclosure is not further used or disclosed in a manner not permitted.
    3. An unauthorized disclosure of PHI where the workforce member has a good faith belief that the party receiving the disclosure would not reasonably have been able to retain such information.
    4. An acquisition, access, or disclosure where it can be demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following:
       a. Nature and extent of the PHI and the likelihood of re-identification.
       b. The unauthorized person who used the PHI or to whom the disclosure was made
       c. Whether the PHI was actually acquired or viewed
       d. The extent to which the risk to the PHI has been mitigated
  - Notification to individuals:
    1. the agency will notify each individual whose unsecured protected health information has been, or is reasonably believed by the agency to have been accessed, acquired, used, or disclosed as a result of such breach
    2. Breaches treated as discovered – the first day on which the agency knows, or by exercising due diligence would have known a breach occurred.
    3. the agency shall notify the person without unreasonable delay and in no case later than 60 calendar days after a discovery of a breach

  The notification to the person shall include:
  1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
  2. A description of the types of unsecured protected health information involved in the breach (such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
  3. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
  4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate the harm to individuals, and to protect against any further breaches; and
  5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, web site, or postal address.

6. The notification shall be written in plain language.

Methods of notification:

1. Written notification by first-class mail to the individual at the last know address of the individual, or if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.
2. If the individual is deceased and the agency has the address of the next of kin or personal representative of the individual, the agency shall notify that person.
3. Substitute notice – in the case where there is insufficient or out-of-date contact information that precludes written notification to the notification to the individual, a substitute form of notice that is reasonably calculated reach the individual shall be provided. In the case of fewer than 10 individuals, than an alternative form of written notice, telephone, or other means can be used. In the case of out-of-date information for 10 or more individuals, the notice shall
   - Be in the form of a conspicuous posting for a period of 90 days on the home page of the we site of the agency or conspicuous notice in a major broadcast media in geographic areas where the individuals affected by the breach likely reside
   - Include a toll free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
4. Additional notice in urgent situations – in case where the agency deems urgent action is required to prevent imminent misuse of unsecured protected health information, the agency may provide information to individuals by phone or other mean, as appropriate, in addition to notice provided this section.

Notification to the media: 500 or more individuals

1. For a breach of unsecured protected health information involving more than 500 hundred individuals of a state jurisdiction, the agency shall notify prominent media outlets serving the State or jurisdiction.
2. The notification shall be made without reasonably delay, and in no case later than 60 calendar days after discovery of a breach

Notification to the Secretary:

1. For breaches involving 500 or more individuals, the agency shall make notification contemporaneously with the notice required by 45 CFR Part 164.404(a) to the Secretary in the manner specified by the HHS web site.
2. For breaches involving fewer than 500 individuals, the agency shall maintain a log or other such breaches and not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) 164.408 that occurred in the preceding year to the to Secretary in the manner prescribed by the HHS web site.

Notification by a business associate:

1. A business associate shall notify the agency of a breach of unsecured protected health information. A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate by an employee, officer, or agent of the business associate.

2. A business associate shall provide the notification required by this section without unreasonable delay and in no case later than 60 days after the discovery of a breach.

Law enforcement delay: if a law enforcement official states to the agency or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, the agency shall:

1. If the statement is made in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posing temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as is described above is submitted during that time.

Health care clearing houses - operating as a business associate for the agency must comply with all standards, requirements and implementation specifications, including 45 CFR:

1. Section 164.500 related to applicability
2. Section 164.501 related to definitions
3. Section 164.502 related to uses and disclosures of protected health information
4. Section 164.504 related to uses and disclosures organizational requirements
5. Section 164.512 related to uses and disclosures not required
6. Section 164.532 transition provisions
7. Section 164.534 compliance dates

## VII: Health Information Technology for Economic and Clinical Health: "HITECH" 45 CFR Part 170

Introduction:

This section combines both the required capabilities of a certified Electronic Health Record and the manner the provider uses the record. CMS provides financial incentives through the Medicare and Medicaid Incentive Program to providers using an approved EHR in meaningful ways to improve patient care. Obtaining financial incentives for this agency is therefore contingent on the federal approval of Credible as a certified Electronic Health Record in the Behavioral Health Module and then our use of Credible to meet the defined CMS objectives. Regardless of the incentives, it is important for this agency to adopt, to the extent possible, both the functional capability and meaningful use of Credible in order to participate in the current health care provider market.

To receive an EHR incentive payment, providers have to show that they are "meaningfully using" their EHRs by meeting thresholds for a number of objectives. CMS has established the objectives for "meaningful use" that eligible professionals, eligible hospitals, and critical access hospitals (CAHs) must meet in order to receive an incentive payment.

The Medicare and Medicaid EHR Incentive Programs are staged in three steps with increasing requirements for participation. All providers begin participating by meeting the Stage 1 requirements for a 90-day period in their first year of meaningful use and a full year in their second year of meaningful use. After meeting the Stage 1 requirements, providers will then have to meet Stage 2 requirements for two full years. Eligible professionals participate in the program

on the calendar years, while eligible hospitals and CAHs participate according to the federal fiscal year.

Clinical quality measures, or CQMs, are tools that measure and track the quality of healthcare services provided by eligible professionals (EPs), eligible hospitals (EHs) and critical access hospitals (CAHs) within the health care system. These measures use a wide variety of data that are associated with a provider's ability to deliver high-quality care or relate to long term goals for health care quality. CQMs measure many aspects of patient care and are classified under the following 6 categories: clinical processes/effectiveness, patient safety, efficient use of healthcare resources, care coordination, patient and family engagements, population and public health.

Continuously measuring and reporting these CQMs helps to ensure that our health care system can deliver effective, safe, efficient, patient-centered, equitable, and timely care.
Currently, in Stage 1 of Meaningful Use for the Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs, CQMs are required as a core meaningful use objective. EPs, EHs and CAHs who wish to participate in the EHR Incentive Program must submit data from certified EHR Technology CQMs in order to receive an incentive payment in the EHR Incentive Program. In Stage 2, CQMs are no longer a core meaningful use objective; however, EPs, EHs and CAHs are still required to submit CQMs in order to successfully participate in the program.

Beginning in 2014, all providers, regardless of whether they are in Stage 1 or Stage 2 of meaningful use, will be required to report on the 2014 CQM. CMS has also provided information on what to report in 2013 to begin the transition for reporting in 2014. In addition, beginning in 2014, all EPs and EHs beyond their first year of meaningful use will be required to submit CQMs electronically.

Definitions and acronyms:

- CAH – Critical Care Hospital
- CEHRT – Certified EHR Technology, uses 2014 meaningful use standards
- Common MU Data Set –
    - Patient name
    - Sex
    - DOB
    - Race
    - Ethnicity
    - Preferred language
    - Smoking status
    - Problems
    - Medications
    - Medication allergies
    - Laboratory tests
    - Laboratory values, results
    - Vital signs
    - Care plan fields, goals and instructions
    - Procedures
    - Care team members
- CQM – Clinical Quality Measures – includes defined set of data and measuring tools
- EP – eligible provider

- EH – eligible hospital
- HIT: Health Information Technology.
- ONC HIT Certification Program – certifies HER, new standards adopted for 2014. .
- ONC – Office of the national coordinator of health information technology
- MU – meaningful use
- EHR
    - Complete – includes all of the modules, meets base definition and could be used to meet CEHRT definition
    - Modules
        - Inpatient
        - Ambulatory
        - Behavior Health
- UCD: User Centered Design

<u>Medicare and Medicaid EP Meaningful Use Objectives Stage 1:</u>

Stage 1 of the CMS EHR Incentive Program began in 2011. It sets the basic functionalities for EHRs. The requirements are focused on providers capturing patient data and sharing that data either with the patient or with other healthcare professionals.

A Medicare Eligible Professional must meet all of the Core Set of Objectives to successfully attest to meaningful use. Six meaningful use core objectives have exclusions that can be taken as meeting the objective.

Meaningful Use Core Objectives

1. Use computerized provider order entry for medication orders directly entered by any licensed healthcare provider who can enter orders into the medical record per state, local and provider guidelines
    - *Measure*: more than 30 percent of all unique patients with at least one (1) medication in their medication list seen by the EP have at least one (1) medication order entered using CPOE
    - *Exclusions*: Any EP who writes fewer than one hundred (100) prescriptions during the EHR reporting period
2. Implement drug-drug and drug-allergy interaction checks
    - *Measure*: the EP has enabled this functionality for the entire Electronic Health Record reporting period.
    - *Exclusions*: None
3. Maintain an up-to-date problem list of current and active diagnoses
    - *Measure*: more than 80% of all unique patients seen by the EP have at least one (1) entry or an indication that no problems are known for the patient recorded as structured data
    - *Exclusions*: None
4. Generate and transmit permissible prescriptions electronically (eRx)
    - *Measure*: more than 40% of all permissible prescriptions written by the EP are transmitted electronically using certified Electronic Health Record Technology
    - *Exclusions*: Any EP who writes fewer than one hundred (100) prescriptions during the EHR reporting period
5. Maintain an active medication list

- *Measure*: more than 80% of all unique patients seen by the EP have at least one (1) entry (or an indication that the patient is not currently prescribed any medication) recorded as structured data
  *Exclusions*: None

6. Maintain active medication allergy list
   - *Measure*: More than 80% of all unique patients seen by the EP have at least one (1) entry (or an indication that the patient has no known medication allergies) recorded as structured data
     *Exclusions*: None
7. Record all of the following demographics: Preferred language, Gender, Race, Ethnicity, Date of Birth
   - *Measure*: More than 50% of all unique patients seen by the EP have demographics recorded as structured data
   - *Exclusions*: None
8. Record and chart changes in vital signs: height, weight, blood pressure; calculate and display the Body Mass Index; plot and display growth charts for children 2-20 years, including BMI
   - *Measure*: More than 50% of all unique patients age 2 and over seen by the EP have height, weight and blood pressure are recorded as structured data
     *Exclusions*: Any EP who either sees no patients 2 years or older, or who believes that all three vital signs of height, weight, and blood pressure of their patients have no relevance to their scope of practice
9. Record smoking status for patients 13 years or older
   - *Measure*: more than 50% of all unique patients 13 years or older seen by the EP have smoking status recorded as structured data
   - *Exclusions*: Any EP who sees no patient 13 years or older
10. Report ambulatory clinical quality measures to CMS or, in the case of Medicaid EPs, the States
    - *Measure*: Successfully report to CMS ambulatory clinical quality measures selected by CMS in the manner specified (or in the case of Medicaid, the States)
    - *Exclusions*: None
11. Implement one (1) clinical decision support rule
    - *Measure*: Implement one (1) clinical decision support rule
      *Exclusions*: None
12. Provide patients with an electronic copy of their health information (including diagnostics test results, problem list, medication lists, medication allergies) upon request
    - *Measure*: more than 50% of all patients who request an electronic copy of their health information are provided it within 3 business days
    - *Exclusions*: Any EP than has no requests from patients or their agents for an electronic copy of patient health information during the EHR reporting period
13. Provide clinical summaries for patient for each office visit
    - *Measure*: clinical summaries provided to patients for more than 50% of all office visits within 3 business days
    - *Exclusions*: Any EP who has no office visits during the EHR reporting period
14. Capability to exchange key clinical information (for example, problem list, medication list, allergies and diagnostic test results) among providers of care and patients authorized entities electronically

- *Measure*: Performed at least one (1) test of certified Electronic Health Record technology's capacity to electronically exchange key clinical information
- *Exclusions*: None

15. Protect electronic health information created or maintained by the certified Electronic Health Record technology through the implementation of appropriate technical capabilities
    - *Measure*: Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process
      *Exclusions*: None

<u>Menu Objectives</u>

Eligible Professionals must meet all but 5 of Menu Set Objectives, deferring the selected 5 for later stages. Of the objectives being used, you must include one public health objective either #9 or #10. Eight of the ten objectives have exclusions that can be taken to meet the objective.

1. Implement drug-formulary checks
    - *Measure*: The EP enabled this functionality and has access to at least one (1) internal or external formulary for the entire Electronic Health Record reporting period
    - *Exclusions*: Any EP who writes fewer than 100 prescriptions during the EHR reporting period.
2. Incorporate clinical lab-test results into Electronic Health Record as structured data
    - *Measure*: more than 40% of all clinical lab tests results ordered by the EP during the Electronic Health Record reporting period whose results are either in a positive/negative or numerical format are incorporated in certified Electronic Health Record technology as structured data
      *Exclusions*: An EP who orders no lab tests whose results are either in a positive/negative or numerical format during the EHR reporting period
3. Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, and outreach
    - *Measure*: generate at least one (1) report listing patients of the EP with a specific condition
      *Exclusions*: None
4. Send reminders to patients per patient preference for preventive/follow up care
    - *Measure*: More than 20% of all patients 65 years or older or 5 years old or younger were sent an appropriate reminder during the Electronic Health Record reporting period
    - *Exclusions*: An EP who has no patients 65 years or older or 5 years old or younger with recorded maintained using certified EHR technology
5. Provide patients with timely electronic access to their health information (including lab results, medication lists, allergies) within 4 business days of the information being available to the EP
    - *Measure*: at least 10% of all unique patients seen by the EP are provided timely (available to the patient within 4 business days of the information updated in the certified Electronic Health Record technology) electronic access to their health information, subject to the EP's discretion to withhold certain information
    - *Exclusions*: Any EP that neither orders nor creates any of the information listed at 45 CFR 17-.304(g) during the EHR reporting period
6. Identify patient-specific education resources using certified Electronic Health Record technology and provide those resources to the patient if appropriate

- *Measure*: more than 10% of all unique patients seen by the EP are provided patient-specific resources
- *Exclusions*: None

7. Perform medication reconciliation
   - *Measure*: The EP performs medication reconciliation for more than 50% of all transitions of care in which the patient is transitioned into the care of the EP
   - *Exclusions*: An EP who was not the recipient of any transitions of care during the EHR reporting period
8. Provide a summary care record for each transition of care or referral
   - *Measure*: The EP who transitions or refers their patient to another setting of care or provider of care provides a summary of care record for more than 50% of transitions of care and referrals
   - *Exclusions*: An EP who neither transfers a patient to another setting nor refers a patient to another provider during the EHR reporting period
9. Capability to submit electronic data to immunization registries or immunization information systems and actual submission according to applicable law and practice
   - *Measure*: Performed at least one (1) test of certified Electronic Health Record technology's capacity to submit electronic data to immunization registries and follow up submission if test is successful (unless none of the immunization registries to which the EP submits such information has the capacity to receive the information electronically)
   - *Exclusions*: An EP who administers no immunizations during the EHR reporting period or where no immunization registry has the capacity to receive the information electronically
10. Capacity to submit electronic syndrome surveillance data to public health agencies and actual transmission according to applicable law and practice
    - *Measure*: Performed at least one (1) test of the certified Electronic Health Record technology's capacity to provide electronic syndrome surveillance data to public health agencies and follow up submission if test is successful (unless none of the public health agencies to which an EP or eligible hospital submits such information have the capacity to receive the information electronically)
    - *Exclusions*: An EP does not collect any reportable syndrome information on their patients during the EHR reporting period or does not submit such information to any public health agency that has the capacity to receive the information electronically

<u>Stage 2</u>

Core objectives – a brief description of core objectives follows

1. Computerized provider order entry (COPE)
2. Prescriptions electronically (eRx)
3. Demographics
4. Vital signs
5. Smoking status
6. Clinical decision support on high priority health conditions
7. Provide patients the ability to view online, download and transmit their health information
8. Clinical summaries
9. Protect health information

10. Clinical lab-test results
11. Generate lists of patients by specific conditions
12. Provide reminders for preventive/follow-up care.
13. Use clinical information to identify patient specific education resources
14. Medication reconciliation.
15. Summary care record for each transition of care or referral
16. Electronic data to immunization registries
17. Secure electronic messaging

Summary of 2014 changes or additions

For inpatient and ambulatory records

1. Electronic notes
2. Image results
3. Family health history
4. Record Amendments
5. View, download, and transit to a 3rd party
6. Automated Numerator Recording – includes a percentage based measure
7. Safety Enhanced Design and Quality Management System
8. Data Portability

For Ambulatory care MU

1. Secure messaging
2. Cancer case information and transmission to cancer registries

For Inpatient care MU

1. Electronic medication
2. Electronic prescribing
3. Transmission of electronic laboratory tests and values to ambulatory providers

For ambulatory and inpatient

1. Vital signs, body mass index, and growth charts
2. Drug formulary checks
3. Smoking status
4. Patient list creation – reminders for patients for follow-up, preventive care
5. Drug to drug allergy interaction checks
6. Demographics

**VIII: Summary**

There are many laws that apply to client records – If you have questions, consult your supervisor, Compliance Officer, or the Responsible Authority for the Minnesota Government Data Practices Act for the agency.