I. **DEFINITIONS**

A. **Individually identifiable (protected) health information (PHI)**: Information that is a subset of health information, including demographic information collected from an individual and;

1. Is created or received by a health care provider, health plan, employer, or health care clearing house; 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 for the provision of health care to an individual; and
   a. That identifies the individual; or
   b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

B. The patient's **right of privacy** is the right to be free from intrusion upon the patient's physical solitude or seclusion; and the right to keep secret some or all details of his or her personal life and health status.

C. **Confidentiality** is the right of the patient to expect that the information he or she chooses to reveal will not be inappropriately shared with others. Patients have a right not to have sensitive, private information made public despite the fact that it may be true information.

D. A **breach of confidentiality** is concerned with the *re*disclosure of previously revealed private matters, usually to others who have no legitimate or pressing need to know the information. HIPAA compliant collaboration platforms allow employees to share documents within their organization and with partners and clinicians outside their organization. To avoid breaches, hospitals and EMS agencies need Business Associate agreements with their healthcare customers that offer the following product and security features:

1. Data encryption at transit and rest
2. Full audit trail for users and content
3. Strict access to files and seven levels of permissions
4. State-of-the-art practices for identity management
5. Mobile device management

II. Patient privacy information is protected under the Department of Health and Human Services standards for privacy of individually identifiable health information; Final Rule for the Health Insurance Portability and Accountability Act (**HIPAA**) (Effective April 14, 2003).

III. **POLICY**

A. "Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed to the patient, the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, those parties directly involved with providing treatment to the patient or processing the payment for that treatment, those parties responsible for peer review, utilization review and quality assurance, and those parties required to be notified under the Abused and Neglected Child Reporting Act, the Illinois Sexually Transmissible Disease Control Act or where otherwise required by law"[1].

B. Medical records in the NWC EMSS shall be confidential, secure, current, authenticated, legible and complete. The information contained in an EMS patient care report (PCR) or Communications Log is privileged from disclosure (Illinois Code of Civil Procedure, Section 8-802). Any written or electronic copy of the PCR kept at the provider agency is considered a copy of the hospital's record of communications given by the patient to EMS personnel that are acting as agents of the EMS MD. Patients have a reasonable expectation of privacy in communications made to health care professionals, including EMS personnel. A patient has a right to expect that all communications and records pertaining to his or her care should be treated as confidential.

C. Unless otherwise permitted or required by HIPAA, a covered entity may not use or disclose PHI without an authorization that is valid. The patient privilege outlined above can only be waived if one of the listed exemptions applies.

1. Upon **written request,** the following may be given information about the evaluation and/or treatment of a patient by EMS personnel:
   a. Any competent patient.
   b. The parents or guardian of a minor.
   c. The administrator or executor of the estate of a deceased patient.
   d. The committee for an incompetent patient.

2. Upon **written authorization** from the patient, the following may request information about the evaluation and/or treatment of a patient by EMS personnel:
   a. The patient's attorney.
   b. The patient's spouse or other relatives.
   c. The patient's third party payor.

3. Uses and disclosures to carry out treatment, payment, or health care operations
   a. A covered entity may use or disclose protected health information for treatment, payment, or health care operations provided that such use or disclosure is consistent with other applicable requirements (Section 165.506)
      (1) A covered entity may use or disclose protected health information for its own treatment, payment or health care operations.
      (2) A covered entity may disclose protected health information for treatment activities of a health care provider.
      (3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.
      (4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is for the purpose listed above or for the purpose of health care fraud and abuse detection or compliance.

4. Patient records and information about their evaluation and/or treatment may be revealed to other health-care providers involved in the care of the patient without the patient's consent. However, the information **must** be needed to insure proper treatment for the patient in later stages of care.

5. The EMT/PHRN/ECRN shall exercise discrete clinical judgment in discussing patient information over the radio enroute to the hospital. Unprofessional communications are never appropriate over the radio.

6. In the case of third-party payment plans (insurance, Medicaid or Medicare), EMS providers who charge for services may release the medical information about a patient when it is necessary for billing purposes.

7. In certain incidents, the law may demand the release of information about a patient without the patient’s approval. Examples: gunshot wounds, dog bites, certain communicable diseases and child abuse. See System Policies I-2 relative to Communicable Disease reporting and V-2 Violence: Child Abuse and Neglect.

8. **Release of PHI to law enforcement officials**: When considering the release of medical information about the evaluation and/or treatment of a patient to the police or other law enforcement agents, it is recommended that an EMS provider or ECRN check with their local government, risk manager, or attorney to seek legal advice before disclosing any information gathered from a patient in the course of treatment. The Privacy Rule permits covered entities to disclose PHI to law enforcement officials without the individual's written authorization, under specific circumstances summarized below.

   a. To comply with a court order or court-ordered warrant, a subpoena or summons issued by a judicial officer, or a grand jury subpoena. The Rule recognizes that the legal process in obtaining a court order and the secrecy of the grand jury process provides protections for the individual's private information (45 CFR 164.512 (f)(1)(ii)(A)-(B)).

   b. To respond to an administrative request, such as an administrative subpoena or investigative demand or other written request from a law enforcement official. Because an administrative request may be made without judicial involvement, the Rule requires all administrative requests to include or be accompanied by a written statement that the information is requested is relevant and material, specific and limited in scope, and de-identified information cannot be used (45 CFR 164.512 (f)(1)(ii)(C)).

   c. To respond to a request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person; but the covered entity must limit disclosures or PHI to name and address, date and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics. Other information related to the individual's DNA, dental records, body fluid or tissue typing, samples, or analysis cannot be disclosed under this provision, but may be disclosed in response to a court order, warrant, or written administrative request (45 CFR 164.512 (f)(2)).

   d. This same limited information may be reported to law enforcement

      (1) About a suspected perpetrator of a crime when the report is made by the victim who is a member of the covered entity's workforce (45 CFR 164.502 (j)(2));

      (2) To identify or apprehend an individual who has admitted participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to a victim, provided that the admission was not made in the course of or based on the individuals' request for therapy, counseling, or treatment related to the propensity to commit this type of violent act (45 CFR 164.512 (j)(1)(ii)(A), (j)(2)-(3)).

   e. To respond to a request for PHI about a victim of a crime, and the victim agrees. If, because of an emergency or the person's incapacity, the individual cannot agree, the covered entity may disclose the PHI if law enforcement officials represent that the PHI is not intended to be used against the victim, is needed to determine whether another person broke the law, the investigation would be materially and adversely affected by waiting until the victim could agree, and the covered entity believes in its professional judgment that doing so is in the best interests of the individual whose information is requested (45 CFR 164.512 (f)(3)).

f. Where child abuse victims or adult victims of abuse, neglect or domestic violence are concerned, other provisions of the Rule apply:

(1) Child abuse or neglect may be reported to any law enforcement official authorized by law to receive such reports and the agreement of the individual is not required (45 CFR 164.512 (b)(1)(ii)).

(2) Adult abuse, neglect, or domestic violence may be reported to a law enforcement official authorized by law to receive such reports (45 CFR.512 (c)):

(a) If the individual agrees;

(b) If the report is required by law; or

(c) If expressly authorized by law, and based on the exercise of professional judgment, the report is necessary to prevent serious harm to the individual or others, or in certain other emergency situations (see 45 CFR 164.512(c)(1)(iii)(B)).

(d) Notice to the individual of the report may be required (see 45 CFR 164.512(c)(2)).

(3) To report PHI to law enforcement when required by law to do so (45 CFR 164.512(f)(1)(i)). For example, state laws commonly require health care providers to report incidents of gunshot or stab wounds, or other violent injuries; and the Rule permits disclosures of PHI as necessary to comply with these laws.

(4) To alert law enforcement to the death of the individual, when there is suspicion that death resulted from criminal conduct (45 CFR 164.512(f)(4)).

Information about a decedent may also be shared with medical examiners or coroners to assist them in identifying the decedent, determining the cause of death, or to carry out their other authorized duties (45 CFR 164l.512 (g)(1)).

(5) To report PHI that the covered entity in good faith believes to be evidence of a crime that occurred on the covered entity's premises (45 CFR 164.512(f)(5)).

(6) When responding to an off-site medical emergency, as necessary to alert law enforcement about criminal activity, specifically, the commission and nature of the crime, the location of the crime or any victims, and the identity, description, and the location of the perpetrator of the crime (45 CFR 164.512(f)(6)). This provision does not apply if the covered health care provider believes that the individual in need of the emergency medical care is the victim of abuse, neglect or domestic violence; see above Adult abuse, neglect or domestic violence for when reports to law enforcement are allowed under 45 CFR 164.512(c).

(7) When consistent with applicable law and ethical standards:

(a) To a law enforcement official reasonably able to prevent of lessen a serious and imminent threat to the health or safety of an individual or the public (45 CFR 164.512(j)(1)(i); or

(b) To identify or apprehend an individual who appears to have escaped from lawful custody (45 CFR 164.512(j)(1)(ii)(B)).

(8) For certain other specialized governmental law enforcement purposes, such as:

(a) To federal officials authorized to conduct intelligence, counter-intelligence, and other national security activities under the National Security Act (45 CFR 164.512(k)(2)) or to provide protective services to the President and others and conduct related investigations (45 CFR 164.512(k)(3));

(b) To respond to a request for PHI by a correctional institution or a law enforcement official having lawful custody of an inmate or others if they represent such PHI is needed to provide health care to the individual; for the heath and safety of the individual, other inmates, officers or employees of or others at a correctional institution, or responsible for the transporting or transferring inmates; or for the administration and maintenance of the safety, security, and good order of the correctional facility, including law enforcement on the premises of the facility (45 CFR 164.512(k)(5)).

(9) Except when required by law, the disclosures to law enforcement summarized above are subject to minimum necessary determination by the covered entity (45 CFR 164.502(b), 164.514(d)). When reasonable to do so, the covered entity may rely upon the representations of the law enforcement official (as a public officer) as to what information is the minimum necessary for their lawful purpose (45 CFR 164.514(d)(3)(iii)(A)). Moreover, if the law enforcement officer making the request for information is not known to the covered entity, the covered entity must verify the identity and authority of such person prior to disclosing the information (45 CFR 164.514(h)). [HHS, 7/26/04]

9. **Release of information to the news media**: The term “public record” is used to justify the review of the run sheets by the press. While the Freedom of Information Act’s definition of public records would apply to EMS patient care reports, section 207(b)(i) of the Act specifically exempts information obtained by public bodies concerning medical care given by the public body from inspection and copying. Many EMS agencies allow the press to review patient care reports after the names and addresses of the patients have been concealed. According to one legal opinion, this is not proper in light of a ruling in the case of Parkinson, 435 N.E. 2d at 142. In light of this ruling, EMS providers are obligated by law to refuse requests by the press to examine EMS patient care reports. Providers should consult their own legal counsel for direction.

IV. **General guidelines:** When considering releasing information about the evaluation and/or treatment of a patient by an EMS provider, the safe path to follow is not to voluntarily provide the records, or any information from the records without either the patient's written consent or a valid subpoena. If a person could not properly obtain a copy of their medical record, including the run sheet, from the hospital's medical records department, the provider should not provide a copy.

V. **Privacy practices under HIPAA**

A. **Protecting privacy**

1. No PHI shall be placed on countertops or left out on workers' desks in public access areas where an unauthorized person could easily read or see the information.
2. Patients must sign in when they arrive at an agency to seek copies of medical reports.
3. Recycling bins containing PHI must not be kept in a public area like a copy room or open office.
4. When documents containing PHI that is no longer needed are destroyed, they must be shredded or disposed of in a secure manner.
5. Fax machines that receive or send PHI must be located in a secure area so that others workers and visitors will not have access to the PHI that is being communicated.
6. The filing system for written copies of medical records must be secure.

B. **Modes of communication**

1. Faxes containing PHI must include a cover sheet with a confidentiality statement.
2. All pre-set numbers on a fax machine to which PHI is sent must be validated as accurate.
3. All EMS agencies must have a confidentiality policy and concrete procedures addressing privacy related to oral (spoken) conversations or discussions about PHI.
4. E-mails containing PHI must contain a confidentiality statement.

C. **Use and disclosure of PHI**

1. All copies of patient care reports that are sent out must be logged or tracked.
2. No PHI is to be given over the phone unless the identity of the caller can be verified.
3. Before any PHI can be released, the agency must obtain the patient's consent or authorization.
4. Releases that do not require authorization
    a. Public health activities
    b. Victims of abuse, neglect, or domestic violence
    c. Health oversight activities
    d. Judicial and administrative proceedings
    e. Law enforcement purposes (see above)
    f. Information about decedents
    g. Cadaveric organ, eye or tissue donations
    h. Disclosure to avert a serious threat to health or safety
    i. Specialized government functions
    j. Worker's compensation
    k. Disaster relief efforts

5. Disclosure of any PHI must be limited to the amount of information necessary to accomplish the goal of the request. Each request for disclosure must be reviewed on an individual basis in accordance with disclosure criteria.
6. If possible, de-identify information prior to disclosing it. Example: PBPI screens.
7. If patient care reports are faxed, you must verify that the correct person received it.
8. Reports containing confidential information may not be put in the regular trash. They must be shredded or disposed of in a secure waste container.

D. **Disclosure of PHI during OLMC reports**

1. **There is no prohibition against EMS personnel conveying PHI over the radio**. The fundamental principle of the HIPAA Privacy Rule is that PHI cannot be disclosed unless there is an exception in the Rule which permits the disclosure. **Disclosure by EMS personnel communicating over the radio falls under the "Treatment" exception,** under which one treating provider is permitted to disclose PHI to another treating provider (including the name of a patient's personal physician if that is important to expediting patient care).
2. The "Incidental Disclosures" exception applies to unrelated persons intercepting the radio communications (usually with scanners). Incidental Disclosures occur when otherwise legitimate disclosures of PHI are disclosed in such a way that a disclosure which would otherwise NOT be permitted happens just an incidental occurrence to the otherwise legitimate disclosure.
    a. In the event that incidental disclosures are unavoidable, only the "minimum necessary" amount of PHI should be disclosed.
    b. A paramedic should legitimately convey the patient's name and clinical information if it would reasonably facilitate treatment of a time-sensitive condition upon arrival in the ED. It would not be acceptable to transmit information (such as an address or social security number) if that information would not be of any use in facilitating and expediting treatment on arrival.
    c. Covered entities are required to take reasonable (but not unreasonable!) measures to prevent incidental disclosures. The section of the law on Incidental Disclosures gives examples. "Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners" is NOT required by HIPAA.
    d. PHI should not be routinely transmitted when it is not needed. If a handset is available at the telemetry console in the ED, it would not be unreasonable to require its use to prevent incidental disclosures. If no handset is available, the volume should be turned down to minimize the number of people who might be able to hear the transmission.
    e. Other possible "reasonable measure" include the use cell phones instead of radios to restrict scanner interception. .
    f. Under the Treatment exception to the Privacy Rule, a treating provider is entitled to have access to all PHI, and the "minimum necessary" concept does not apply. It is only because of the possibility of incidental disclosures that the "minimum necessary" concept comes into play. If communications were to be by cell phone, in which case incidental disclosures would not be occurring, there would be no restriction on the PHI that the paramedics might convey to hospital. (Mike Frank, MD, JD, FACEP, FCLM EMP)

E. **Privacy education and training**

1. All persons who handle PHI must receive privacy training.
2. There must be measures in place to safeguard PHI when an EMT leaves the system (removal from the CARS database, frequent changes of pass codes etc.).

F. **Physical security** (Final security rules published 2/20/03 address procedural security, personal security, disaster recovery, business resumption planning, physical security, environmental security, media security, software security, networks and hospital (system) security. The compliance deadline for these rules was April 2005.)

1. All PCRs containing PHI must always be kept in a secure, locked area to prevent the information from being accessed/viewed by unauthorized persons.
2. All areas that have PHI-containing electronic databases must have policies in place to keep PHI out of view at work stations and on computer screens, such as having the computers set to automatically log off users after a few minutes of inactivity.
3. All work stations for staff that handle PHI must be set up so passers by cannot easily view computer monitors.
4. There must be a log for how computer equipment, backup tapes and storage devices containing PHI are accounted for when they are removed from the department (i.e., when they are out for repairs or when backup tapes are taken to off-site repositories).
5. Precautions must be taken so it is difficult for people passing by to view documents containing PHI that are being faxed, printed or copied.

G. **Technical security**

1. Computers containing PHI must require log-ins.
2. Screen savers should kick in if there is even a short period of inactivity.
3. Program managers must be able to tell if an unauthorized user has accessed PHI through a computer or network. Safeguards must be in place to prevent unauthorized access.
4. Technology should be in place to verify the true identity of users.
5. Passwords and/or IDs should be used to access PHI.
6. Safeguards must be in place to prevent interception or unauthorized access of PHI by use of wide area networks or the internet.

H. **Administrative requirements:** A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure (Section 164.530).

I. **Penalties:** New penalties (2015) for willful neglect of compliance begin at $10,000.

John M. Ortinau, M.D., FACEP
EMS Medical Director

Connie J. Mattera, M.S., R.N.
EMS Administrative Director

References: P.A. 86-902 Privacy and Confidentiality in Health Care Act, effective September 11, 1989. HIPAA Final Privacy Rule