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 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**) .

III. **POLICY**

A. (d) No [healthcare worker] shall disclose the nature or details of services provided to patients, except that the information may be disclosed to the patient, persons authorized by 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 or quality assurance, risk management, or defense of claims brought against the hospital arising out of the care, 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 authorized or required by law. (210 ILCS 85/6.17)

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) and 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. EMS personnel shall exercise discrete clinical judgment in discussing patient information during OLMC communications 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.

IV. **Disclosing/Releasing medical records**

A. EMS is required to follow the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule when disclosing or releasing Protected Health Information ("PHI").

The improper release of medical records and the improper spoliation or destruction of records can lead to civil and/or criminal liability. In Illinois, any individual who willfully or wantonly discloses hospital or medical record information is guilty of a Class A misdemeanor. 210 ILCS 85/6.17(i). Protection of and confidential access to medical records and information. HIPAA privacy regulations allow patients the right to collect and view their health information, including medical and billing records, on-demand.

A request for information must be granted within 30 days of the request. If there are extenuating circumstances, the covered entity must provide a reason within that 30-day time frame, and the records must still be provided within 60 days.

Deleting a public record prior to the expiration of the record retention period—or refusing to produce a public record when lawfully ordered to do so—is a criminal offense in many jurisdictions, and a finable civil infraction in the others.

1. **Release of PHI to law enforcement officials**: Check with your local 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]

2. **Release of information to the news media**: The term “public record” is used to justify the review of EMS PCRs by the press. While the Freedom of Information Act’s definition of public records may apply to redacted portions of EMS PCRs, 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.. In Parkinson, 435 N.E. 2d at 142 the court ruled that EMS providers are obligated by law to refuse requests by the press to examine EMS PCRs. Consult your legal counsel for direction.

V. **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 (See template form below). If all requirements are met, the provider should provide a copy of the specific record(s) requested.

VI. **Privacy practices under HIPAA**

A. **Protecting privacy**

1. No PHI shall be placed on countertops or left out on 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 unless they are tamper proof.
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 other 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 releasing PHI, the agency must obtain the patient's consent or authorization except in the following situations that **do not require authorization:**
    a. Public health activities | Disaster relief efforts
    b. Victims of abuse, neglect, or domestic violence
    c. Health oversight activities
    d. Judicial and administrative proceedings | Law enforcement purposes
    e. Information about decedents
    f. Cadaveric organ, eye or tissue donations
    g. Disclosure to avert a serious threat to health or safety
    h. Specialized government functions
    i. Worker's compensation
4. **Disclosure of any PHI must be limited to the minimum necessary information to accomplish the request.** Each request for disclosure must be reviewed on an individual basis in accordance with disclosure criteria.
5. If possible, de-identify information prior to disclosing it. Example: PBPI screens.
6. If patient care reports are faxed, verify that the correct person received it.
7. 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 during OLMC reports**. 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 during OLMC contact 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 OLMC 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 as 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. EMS 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 that can be intercepted by scanners" is NOT required by HIPAA.

    d. PHI should not be routinely transmitted if not needed. If a handset is available at the telemetry console in the ED, it would be reasonable 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. 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. Measures must be in place to safeguard PHI when an EMS clinician leaves the System (Inactivate in the Image*Trend* database), frequently change pass codes.

F. **Physical security:** Final security rules address procedural security, personal security, disaster recovery, business resumption planning, physical security, environmental security, media security, software security, networks and hospital (system) security.

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.

Reference:
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html#:~:text=The%20HIPAA%20Privacy%20Rule%20establishes,care%20providers%20that%20conduct%20certain

Matthew T. Jordan, MD, FACEP
EMS Medical Director

Connie J. Mattera, MS, RN, PM
EMS Administrative Director

HIPAA Checklist Essential elements of an effective HIPAA compliance program	
Required Annual Audits / Assessments: Have you conducted the following 6 annual audits?	
	Security risk assessment
	Privacy standards audit (not required for business associates)
	HITECH Subtitle D privacy audit
	Security standards audit
	Asset and device audit
	Physical site audit
Documentation gaps	
	Have you identified all gaps uncovered in the above audits?
	Have you documented all deficiencies?
Remediation plans	
	Have you created remediation plans to address deficiencies found in all six audits?
	Are these remediation plans fully documented in writing?
	Do you update and review these remediation plans annually?
	Are annually documented remediation plans retained in your records for a minimum of six years?
Staff training	
	Have all staff members undergone annual HIPAA training?
	Do you have documentation of the training?
	Is there a staff member designated as the HIPAA Compliance, Privacy, or Security Officer?
Policies and Procedures	
	Do you have policies and procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification rules?
	Have all staff members read and legally attested to the Policies and Procedures?
	Do you have documentation of their legal attestation?
	Do you have documentation for annual reviews of your Policies and Procedures?
Vendors and Business Associates	
	Have you identified all of your vendors and Business Associates?
	Do you have Business Associate Agreements in place with all Bas?
	Have you performed due diligence on your Bas to assess their HIPAA compliance?
	Are you tracking and reviewing your BA agreements annually?
	Do you have Confidentiality Agreements with non-BA vendors?
Breaches	
	Do you have a defied process for incidents or breaches?
	Do you have the ability to track and manage the investigations of all incidents?
	Are you able to provide the required reporting of minor or meaningful braches or incidents?
	Do your staff members have the ability to anonymously report an incident?
Note: If you are audited, you must provide all documentation for the past six years to auditors	

HIPAA Journal. https://www.hipaajournal.com/wp-content/uploads/2018/08/HIPAA-Journal-HIPAA-Compliance-Checklist.pdf

HIPAA Risk Assessment Checklist Essential elements of an effective HIPAA compliance program	
HIPAA Risk Analysis	
	Identify where PHI is stored, received, maintained or transmitted. This not only includes electronic health records (EHRs) and servers, but also any removable media such as USBs.
	Identify and document potential threats and vulnerabilities. These should include all scenarios in which a HIPAA violation could result in a data breach.
	Assess current security measures used to safeguard PHI – ensuring that they are configured correctly to maximize defenses against threats.
	Assess whether the current security measures are used properly – especially with regards to access and identity measures such as passwords.
	Determine the likelihood of a "reasonably anticipated" threat. The likelihood of a threat occurring may depend on how measures are configured and used.
	Determine the potential impact of a breach of PHI. This includes ransomware attacks that can cripple an organization's operations until resolved.
	Assign risk levels for vulnerability and impact combinations. This process helps organizations prioritize what areas of risk require the most attention.
	Document the assessment and take action where necessary – not forgetting to provide training to members of the workforce when material changes occur.
PRIVACY RISK ASSESSMENT: Identify potential risks and vulnerabilities to PHI that is not created, received, maintained, or transmitted electronically and develop policies and procedures to comply with the Act;	
	Ensure all members of the workforce understand what PHI is - even those who do not use it in day-to-day functions.
	Ensure all members of the workforce with access to PHI are aware of what uses and disclosures are permissible.
	When authorizations are required, ensure procedures exist for obtaining and documenting valid authorizations.
	Review the Notice of Privacy Practices to ensure it provides all the information required by the Privacy Rule.
	Implement procedures for recording, responding to, and managing oral requests for privacy protections.
	Ensure procedures exist to respond to requests for access to PHI, corrections to PHI, and transfers of PHI.
	Adopt procedures for maintaining an accounting of disclosures for each individual patient and/ or plan member.
	Provide general training for all members of the workforce and policy-specific training for those for whom policies are relevant.
Note: If you are audited, you must provide all documentation for the past six years to auditors	

NWC EMSS Sample template: Release of Patient Care Report (PCR)

Patient Name: (Please Print)	
Address	City/State/Zip:
Birth date:	Phone:

I, _____ do hereby authorize:

_____

Agency/Facility/Person

To release the named patient's EMS PCR to:

_____

Agency/Facility/Person

Address:_____City/State/Zip: _____

Phone: _____Fax number: _____

For the purpose(s) of: ☐ Continuity of Care ☐ Attorney/client relationship ☐ Insurance
☐ Request of patient ☐ Other:

Date of EMS Service from _____ to _____

I also authorize the release of the following:
☐ Records of HIV/Aids testing, diagnoses or treatment
☐ Alcohol/Drug abuse diagnoses and treatment records
☐ Mental Health records (Check all that apply)

I acknowledge that I have the right to revoke this authorization. I understand that my revocation must be in writing. I also understand that my revocation will be valid except to the extent that the person(s) or organization(s) authorized to make the requested use/ disclosure have taken action in reliance on this authorization or if this authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest the claim under the policy or the policy itself.

I understand that I have the right to inspect and copy my information that will be used or discussed pursuant to this authorization. I understand I have a right to receive a copy of this authorization.

Patient's Signature: _____ Date: _____

Signature of Minor (12-17): _____ Date: _____
(Mental health or emancipated minor)

Parent/Guardian/
Representative Signature:_____ Date: _____

Relationship to Patient: _____

I attest to the identity of the above signature(s):

Witness: _____ Date: _____

Applicable fees will be charged for patients and attorneys. (735 ILCS 5/8-2006) Under the provisions of HIPAA and under the Illinois Mental Health and Developmental Disabilities Confidentiality Act, authorization for release/disclosure is voluntary. Individuals are not coerced into signing an authorization but provide the information freely. The above-named agency may not limit or restrict services, treatment or care based on the signing of this authorization. Once information is received by the authorized agency/facility or person it may be subject to re-disclosure by the recipient and may no longer be protected by federal privacy laws. Illinois law prohibits re-disclosure of HIV, alcohol, drug abuse and genetic information by the recipient except as otherwise allowed by law. Federal regulations prohibit the recipient from making further disclosure of alcohol and drug abuse patient records except by express written consent of the patient. 42 C.F.R. Part 2. This authorization will automatically expire one year after the date of signing if no prior notice for revocation is received. The above-named individual has requested the above records to be sent to the agency/facility/person named herein and that it not be further disclosed or used for any purpose other than as stated in this authorization. Any person who discloses mental health records and communication without proper consent/authorization may be subject to civil liability or criminal penalty according to 740 ILCS 110.