STANDARD OPERATING GUIDELINE

Number 103-01

Patient Access to Protected Health Information(PHI)

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 3

PURPOSE: Under the HIPAA Privacy Rule, individuals have the right to access their protected health information (PHI) that is maintained in "designated record sets (DRS)". (See policy on Designated Record Sets).

The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

The intent of this policy is to ensure that Lincoln County Emergency Medical Services (LCEMS) only releases the PHI that is covered under the Privacy Rule, this policy outlines procedures for requests for patient access of PHI.

This policy also establishes the procedure by which patients or appropriate requestors may access PHI.

POLICY: Only information contained in the DRS outlined in this policy is to be provided to patients who request access, amendment and/or restriction on the use of their PHI in accordance with the Privacy Rule and the Privacy Practices of LCEMS.

PROCEDURE: **Patient Access**

Upon presentation to the LCEMS business office, the patient or appropriate representative shall complete a Request for Access Form.

The LCEMS employee receiving the Request for Access Form shall verify the patient's identity, and if the requestor is not the patient, the name of the individual and reason that the request is being made by this individual. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose.

The completed form shall be presented to the Privacy Officer for action.

The Privacy Officer shall act upon the request within 30 days, preferably sooner. Generally, LCEMS shall respond to requests for access to PHI within 10 days of receipt of the access request, unless the designated record set is not maintained on site, in which case the response period may be extended to 30 days.

If LCEMS is unable to respond to the request within these time frames, the requestor shall be given a written notice no later than the initial due date for a response, explaining why LCEMS could not respond within the time frame and in that case LCEMS may extend the response time by an additional 30 days.

Upon approval of access, patient shall have the right to access the PHI contained in the DRS outlined below and may make a copy of the PHI contained in the DRS upon verbal or written request.

LCEMS shall establish a reasonable charge of $10.00 per DRS for copying PHI for the patient or appropriate representative.

Patient access may be denied for the reasons listed below, and in some cases the denial of access may be appealed to the Lincoln County Attorney for review.

The following are reasons to deny access to PHI that are not subject to review and are final and may not be appealed by the patient:

- If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding.
- If the information the patient requested 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.

The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:

a. If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

b. If the protected health information makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person.

c. If the request for access is made by a requestor as a personal representative of the individual about whom the requestor is requesting the information, and a licensed health professional has determined, in the exercise of professional judgment, that access by the requestor is reasonably likely to cause harm to the individual or another person.

d. If the denial of the request for access to PHI is for reasons a, b, or c, then the patient may request a review of the denial of access by sending a written request to the Privacy Officer.

e. LCEMS shall designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. LCEMS shall promptly refer the request to this designated review official. The review official shall determine within a reasonable period of time whether the denial is appropriate. LCEMS shall provide the patient with written notice of the determination of the designated reviewing official.

f. The patient may also file a complaint in accordance with the Procedure for Filing Complaints About Privacy Practices if the patient is not satisfied with the LCEMS's determination.

Access to the actual files or computers that contain the DRS may not be accessed by the patient or requestor. Rather, copies of the records should be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated LCEMS staff member. UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.

If the patient or requestor would like to retain copies of the DRS provided, then LCEMS may charge a reasonable fee for the costs of reproduction.

Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book, electronic or hard copy, indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.

Following a request for access to PHI, a patient or requestor may request an amendment to his or her PHI, and request restriction on its use in some circumstances. Please refer to Request for Amendment to PHI.

STANDARD OPERATING GUIDELINE

Number 103-02

Requests for Amendment to Protected Health Information (PHI)

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 2

PURPOSE: Under HIPAA Privacy Rule, individuals have the right to request amendment to their Protected Health Information (PHI) as it is maintained in the Designated Record Set (DRS).

The intent of this policy is to provide consistent guidelines for Lincoln County Emergency Medical Services (LCEMS) staff so that they may assist a patient in amending the protected health information (PHI) of their patient care record in accordance with their rights under the federal Privacy Regulations.

POLICY: An individual has the right to amend his/her patient care records, as long as his/her protected health information is maintained by LCEMS, except in the following circumstances:

- The originator of the record is no longer available.
- The information the patient is requesting to amend was not created by LCEMS.
- The information is not part of the patient care record.
- The information is accurate and complete.
- The information would not be available for inspection as provided by law, and therefore LCEMS is not required to consider an amendment. This exception applies to information compiled in anticipation of a legal proceeding.
- Information received from someone else under a promise of confidentiality.

PROCEDURE: Confirm the identity of requestor or legal representative. If the requestor is a legal representative, ask for legal proof of their representative status.

The patient must fill out the Request for Amendment of Health Information form completely.

LCEMS, with the assistance of legal counsel, will act on the request for amendment within 60 days of the request.

If LCEMS agrees with the amendment:

- Then the record will be amended.
- LCEMS will then notify the individual of the agreement to amend the record.
- Copies of the amended record will be provided to our business associates, facilities to or from which we have

transported the patient, and others involved in the patient's treatment.

If LCEMS denies the request for amendment:

- Then the individual that requested the amendment will be notified of the denial, and the reason for the denial in writing.
- A statement will be given to the individual that he/she may submit a short written statement disagreeing with the denial, and how the individual may file such a statement.
- A statement will be given to that individual that he/she may, if he/she does not wish to submit a statement of disagreement, that he/she may request that the Request for Amendment and the denial become a permanent part of his/her medical record.
- A statement that the individual may complain to the Privacy Officer of LCEMS, or to the federal agency that oversees enforcement of the federal Privacy Rule, the Department of Health and Human Services.

All documentation pertaining to the request for amendment will be kept in the medical record.

STANDARD OPERATING GUIDELINE

Number 103-03

Request to Restrict Use of Protected Health Information (PHI)

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 1

PURPOSE: Under HIPAA Privacy Rule, individuals have the right to request to restrict the use of their Protected Health Information (PHI) as it is maintained in the Designated Record Set (DRS).

The intent of this policy is to establish a procedure for individuals to request restricted use of their Protected Health Information (PHI) with Lincoln County Emergency Medical Services (LCEMS).

POLICY: The patient may request a restriction on the use and disclosure of his/her PHI.

LCEMS is not required to agree to any restriction, and given the emergent nature of our operation, we generally will not agree to a restriction.

ALL REQUESTS FOR RESTRICTION ON USE AND DISCLOSURE OF PHI MUST BE SUBMITTED IN WRITING ON THE APPROVED COMPANY FORM. ALL REQUESTS SHALL BE REVIEWED AND DENIED OR APPROVED BY THE PRIVACY OFFICER.

If LCEMS agrees to a restriction, we may not use or disclose PHI in violation of the agreed upon restriction, except that if the individual who requested the restriction is in need of emergency service, and the restricted PHI is needed to provide the emergency service, LCEMS may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.

The agreement to restrict PHI will be documented to ensure that the restriction is followed.

A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate restrictions must be documented. A current restriction may also be terminated by LCEMS as long as LCEMS notifies the patient that PHI created or received after the restriction is removed is no longer restriction. PHI that was restricted prior to LCEMS voiding the restriction must continue to be treated as restricted PHI.

STANDARD OPERATING GUIDELINE

Number 103-04

Designated Record Sets (DRS)

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 2

PURPOSE: The intent of this policy is to ensure that Lincoln County Emergency Medical Service (LCEMS) releases Protected Health Information (PHI) in accordance with the Privacy Rule, this policy establishes a definition of what information should be accessible to patients as part of the Designated Record Sets (DRS), and outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

Under the Privacy Rule, the DRS include medical records that are created or used by LCEMS to make decisions about the patient.

POLICY: The DRS should only include HIPAA covered PHI, and should not include information used for the operational purposes of the organization, such as quality assurance data, accident reports, and incident reports. The type of information that should be included in the DRS is medical records and billing records.

PROCEDURE: **The Designated Record Set**

The DRS for any requests for access to PHI include the following records:

- The EPCR created by EMS field personnel (this includes any photographs, monitor strips, Physician Certification Statements, Refusal of Care forms, or other source data that is incorporated and/or attached to the EPCR, except for QA flags and Special Reports.)
- The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.
- Any patient-specific claim information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.
- Medicare Advance Beneficiary Notices, Notices from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance card or policy coverage summary that relate directly to the care of the patient.
- Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not

amended upon request, or an accurate summary of the statement of disagreement.

The DRS also include copies of records created by other service providers and other health care providers such as first responder units, assisting ambulance services, air medical services, nursing homes, hospitals, police departments, coroner's office, etc., that are used by LCEMS as part of treatment and payment purposes related to the patient.

STANDARD OPERATING GUIDELINE

Number 103-05

Security, Levels of Access and Limiting Disclosure and Use of PHI

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 5

PURPOSE: The intent of this policy is to outline levels of access to Protected Health Information (PHI) of various staff members of Lincoln County Emergency Medical Services (LCEMS) and to provide a policy and procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone's responsibility.

POLICY: LCEMS retains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be based on the role of the individual staff member in the organization, and should be only to the extent that the person needs access to PHI to complete necessary job functions.

When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

PROCEDURE: **Role Based Access**

Access to PHI will be limited to those who need access to PHI to carry out their duties. The following describes the specific categories or types of PHI to which such persons need access is defined and the conditions, as appropriate, that would apply to such access.

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
EMT / EMT-I	Intake forms from dispatch, patient care reports,	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Paramedic	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities and only while actually on duty
Administrative Secretary acting as Billing Clerk	Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities	May access only as part of duties to complete patient billing and follow up and only during actual work shift
Logistics Officer	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities, as well as for monitoring equipment and supply usage and repairs

Shift Supervisor	Intake forms from dispatch, patient care reports	May access only as part of completion of a patient event and post-event activities, as well as for quality assurance checks and corrective counseling of staff
Performance Improvement Coordinator/Privacy Officer	ALL	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel
Training Coordinator	ALL	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel
Deputy Director	ALL	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel
Program Director	ALL	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on LCEMS's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.

Access to a patient's entire file **will not be allowed** except when provided for in this and other policies and procedures and the justification for use of the entire medical record is specifically identified and documented.

Disclosures to and Authorizations from the Patient

You are not required to limit to the minimum amount of information necessary required to perform your job function, or the disclosures of PHI to patients who are the subject of the PHI. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by LCEMS.

Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct employees to release PHI to those entities, are not subject to the minimum necessary standards.

For example, if there is a patient's authorization to disclose PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, LCEMS is permitted to disclose the PHI requested without making any minimum necessary determination.

Lincoln County EMS Requests for PHI

If LCEMS needs to request PHI from another health care provider on a routine or recurring basis, we must limit our requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, you must make this determination individually for each request and you should consult your supervisor for guidance. For example, if the request in non-recurring or non-routine, like making a request for documents via a subpoena, we must make sure our request covers only the minimum necessary PHI to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
Skilled Nursing Facilities	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Hospitals	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Mutual Aid Ambulance or Paramedic Services	To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the Company	Patient care reports

For all other requests, determine what information is reasonably necessary for each on an individual basis.

Incidental Disclosures

LCEMS understands that there will be times when there are incidental disclosures about PHI in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to

the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

The fundamental principle is that all staff members need to be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information. Co-workers and other staff members should not have access to information that is not necessary for the staff member to complete his or her job. For example, it is generally not appropriate for field personnel to have access to billing records of the patient.

But all personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. Pay attention to who is within earshot when you make verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures.

Verbal Security

Waiting or Public Areas: If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened area before engaging in discussion.

Garage Areas: Staff members should be sensitive to that fact that members of the public and other agencies may be present in the garage and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. You should be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment

provided, and any of their health information you may have in your possession with others involved in the care of the patient.

Physical Security

Patient Care and Other Patient or Billing Records: Patient care reports should be stored in safe and secure areas. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

Billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individually to whom it is assigned at all times. See the LCEMS Policy on Use of Computer Equipment and Information Systems.

STANDARD OPERATING GUIDELINE

Number 103-06

Use of Computer and Information Systems and Equipment

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 5

PURPOSE: Lincoln County Emergency Medical Service (LCEMS) is committed to protecting our staff members, the patients we serve, LCEMS and Lincoln County from illegal or damaging actions by individuals and the improper release of protected health information and other confidential or proprietary information.

The intent of this policy is to outline the acceptable use of computer equipment at LCEMS. These rules are in place to protect the employee and patients of LCEMS. Inappropriate use exposes Lincoln County Emergency Medical Service to risks including virus attacks, compromise of network systems and services, breach of patient confidentiality and other legal claims.

POLICY: This policy applies to employees, volunteers, contractors, consultants, temporary employees, students, and others at LCEMS who have access to computer equipment, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Lincoln County Emergency Medical Service.

PROCEDURE: **Use and Ownership of Computer Equipment**

All data created or recorded using any computer equipment owned, controlled or used for the benefit of LCEMS is at all times the property of LCEMS. Because of the need to protect the computer network, LCEMS cannot guarantee the confidentiality of information stored on any network device belonging to LCEMS, except that it will take all steps necessary to secure the privacy of all protected health information in accordance with all applicable laws.

Staff members are responsible for exercising good judgment regarding the reasonableness of personal use and must follow operational guidelines for personal use of Internet/Intranet/Extranet systems and any computer equipment.

At no time may any pornographic or sexually offensive materials be viewed, downloaded, saved, or forwarded using any LCEMS computer equipment. Please refer to Lincoln County Management Information Systems Internet and E-Mail Policy for further information.

For security and network maintenance purposes, authorized individuals within LCEMS may monitor equipment, systems and network traffic at any time to ensure compliance with all LCEMS and Lincoln County policies.

Security and Proprietary Information

Confidential information should be protected at all times, regardless of the medium by which it is stored. Examples of confidential information include but are not limited to: individually identifiable health information concerning patients, LCEMS and Lincoln County financial and business information, patient lists and reports, and research data. Staff members should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and User level passwords should be changed in accordance with LCEMS and Lincoln County MIS policies.

All PCs, laptops, workstations and remote devices should be secured with a password-protected screensaver, wherever possible, and set to deactivate after being left unattended for 10 minutes or more, or by logging-off when the equipment will be unattended for an extended period.

Staff members must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

Unacceptable Use

Under no circumstances is a staff member of LCEMS authorized to engage in any activity that is illegal under local, state, or federal law while utilizing LCEMS computer resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by LCEMS or Lincoln County.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources,

copyrighted music, and the installation of any copyrighted software for which LCEMS or the end user does not have an active license is strictly prohibited.

Installation of Hardware, Software or Peripheral devices is strictly prohibited by anyone other than LCEMS System Administrator or Lincoln County MIS.

Exporting system or other computer software is strictly prohibited.

Introduction of malicious programs into the network or server (e.g., viruses, worms, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a LCEMS computer device to actively engage in procuring or transmitting material that is in violation of LCEMS and Lincoln County prohibition on sexual and other harassment.

Making fraudulent statements or transmitting fraudulent information when dealing with patient or billing information and documentation, accounts or other patient information, including the facsimile or electronic transmission of patient care reports and billing reports and claims.

Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the staff member is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

Providing information about, or lists of, LCEMS staff members or patients to parties outside of Lincoln County Emergency Medical Service.

Remove, unplug or alter any wiring and/or devices attached.

E-mail and Communications Activities

Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of e-mail header information.

Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited e-mail originating from within LCEMS's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by LCEMS or connected via LCEMS's network.

Use of Remote Devices

The appropriate use of Laptop Computers, Personal Digital Assistants (PDAs), and remote data entry devices is of utmost concern to Lincoln County Emergency Medical Service. These devices, collectively referred to as "remote devices" pose a unique and significant patient privacy risk because they may contain confidential patient, staff member or company information and these devices can be easily misplaced, lost, stolen or accessed by unauthorized individuals.

Personnel owned devices, including memory sticks, shall not be used to store LCEMS data.

Remote devices containing confidential or patient information must not be left unattended.

If confidential or patient information is stored on a remote device, access controls must be employed to protect improper access. This includes, where possible, the use of passwords and other security mechanisms.

Remote devices should be configured to automatically power off following a maximum of 10 minutes of inactivity.

Remote device users will not permit anyone else, including but not limited to user's family and/or associates, patients, patient families, or unauthorized staff members, to use LCEMS owned remote devices for any purpose.

Remote device users will not install any software onto any computers owned by LCEMS, except as authorized by LCEMS Administration.

- Users of LCEMS owned remote devices will immediately report the loss of a remote device to a supervisor or the Privacy Officer.
- Remove, unplug or alter any wiring and/or devices attached.

Enforcement

Any staff members found to have violated this policy may be subject to disciplinary action, up to and including suspension and termination.

STANDARD OPERATING GUIDELINE

Number 103-07

Policy on Privacy Training

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 2

PURPOSE: The intent of this policy is to ensure that all members of Lincoln County Emergency Medical Service (LCEMS) Staff, including all employees, volunteers, students, trainees and any member of fire departments, rescue squads or other first responder groups assisting or acting on behalf of LCEMS (collectively referred to as "staff members") who have access to patient information understand the organization's concern for the respect of patient privacy and are trained in LCEMS's policies and procedures regarding Protected Health Information (PHI).

POLICY: All current staff will be required to undergo privacy training in accordance with the HIPAA Privacy Rule prior to or within a reasonable time period with the implementation date of the HIPAA Privacy Rule, which is April 14, 2003.

All new staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the organization, as scheduled by the Privacy Officer.

All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time after there is a material change to LCEMS policies and procedures on privacy practices.

PROCEDURE: The Privacy Training will be conducted by the Privacy Officer or his or her designee.

All attendees will receive copies of LCEMS's policies and procedures regarding privacy.

All attendees must attend the training in person and verify attendance and agreement to adhere to all LCEMS policies and procedures on privacy practices.

Initial Training will be conducted in the following manner:

- VIDEOTAPE and CLASSROOM LECTURE.
- Continuing education may be conducted through the above mentioned mediums as well as COMPUTER-BASED EDUCATION.

Topics of the training will include a complete review of Lincoln County Emergency Medical Service's Policy on Privacy Practices and will include other information concerning the HIPAA Privacy Rule, such as, but not limited to the following topic areas:

- Overview of the federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Description of Protected Health Information (PHI).
- Patient rights under the HIPAA Privacy Rule.
- Staff member responsibilities under the Privacy Rule.
- Role of the Privacy Officer and reporting employee and patient concerns regarding privacy issues.
- Importance of and benefits of privacy compliance.
- Consequences of failure to follow established privacy policies.
- Use of LCEMS specific privacy forms.

STANDARD OPERATING GUIDELINE

Number 103-08

Medical Records of Employees

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 2

PURPOSE: The intent of this policy is to provide guidance to management and staff concerning the privacy of medical records which involve staff members of Lincoln County Emergency Medical Service (LCEMS).

PROCEDURE: LCEMS shall, to the extent required by law, protect medical records it receives about employees or other staff in a confidential manner. Generally, only those with a need to know the information shall have access to it, and, even then, they shall only have access to as much information as is minimally necessary for the legitimate use of the medical records.

In accordance laws concerning disability discrimination, all medical records of staff shall be kept in separate files apart from the employee's general employment file. These records shall be secured with limited access by the Privacy Officer.

In accordance with the Privacy Rule of the Health Insurance Portability and Accountabilities Act, medical records that are not considered employment records shall be treated in accordance with the safeguards of the Privacy Rule with respect to their use and disclosure.

Employment records are not considered to be protected health information, or PHI, subject to HIPAA safeguards, including certain medical records of employees that are related to the job. These employment records not covered under HIPAA include, but are not limited to: information obtained to determine suitability to perform the job duties (such as physical examination reports), drug and alcohol tests obtained in the course of employment, doctor's excuses provided in accordance with the attendance policy, work-related injury and occupational exposure reports, and medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers' compensation coverage.

Despite the fact that such records are not considered HIPAA protected, LCEMS shall limit the use and disclosure of these records to only those with a need to have access to them, such as certain management staff, LCEMS's designated physician, and state agencies pursuant to state law.

With respect to staff members of LCEMS, only health information that is obtained about staff in the course of providing ambulance or other medical services directly to them is considered PHI under HIPAA. In other words, if LCEMS provides ambulance service to an employee, the protections typically given to such information

to our ambulance service patients applies to the employee. These protections are subject to HIPAA exceptions, such as in the situation in which the staff member used LCEMS involved in a work-related injury while on duty.

As another example, if we receive a staff member's medical record in the course of providing the employee with treatment and/or transport, it does not matter that LCEMS happens to be the employer – that record is PHI. If, however, the employee submits a doctor's statement to a supervisor to document an absence or tardiness from work, LCEMS does not need to treat that statement as PHI. Other health information that could be treated as employment related, and not PHI, includes medical information that is needed for LCEMS to carry out its obligations under the FMLA, ADA and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, drug screening results, workplace medical surveillance, and fitness-for-duty-tests of employees.

If you have any questions about how medical information about you is used and disclosed by LCEMS, please contact the LCEMS Privacy Officer at (704) 736-9385.

STANDARD OPERATING GUIDELINE

Number 103-09

HIPAA Public / Media Information & Relations

EFFECTIVE DATE:	REVISION DATE:	APPROVED BY:	PAGE:
04/14/2003	09/25/2015	RONALD D. ROMBS	1 OF 2

PURPOSE: The intent of this policy is to provide for proper public and media relations while insuring appropriate compliance with HIPAA requirements.

SCOPE: This procedure applies to all Lincoln County Emergency Medical Service (LCEMS) System providers.

POLICY: It is the position of LCEMS to cooperate with the media and provide excellent public information when possible. LCEMS will seek to achieve and maintain a strong relationship with members of the media and the general community.

Only the on-duty LCEMS Shift Supervisor, Director, Deputy Director and Training Coordinator may issue statements to the media at their own discretion in accordance with Lincoln County Policy.

All LCEMS system providers not serving in one of the above mentioned capacities should direct all issues concerning the media or public information to EMS Administration.

All LCEMS system providers shall refrain from making any comment to media, family or other public interactions regarding matters of an EMS nature. All correspondence and interaction related to an EMS incident shall be coordinated through Lincoln County EMS Administration.

LCEMS shall work in a coordinated process with allied agencies to determine what, if any information can be released about an EMS incident.

Issues that attract a large volume of media attention should be handled by notification of the Director of EMS and the Public Information Officer who shall then issue a press release and coordinate a press conference. No interaction with the media or public shall occur outside of the press conference unless expressly authorized by the Director.

Patient specific information and operational issues concerning LCEMS shall not be discussed with the media or general public by EMS or allied agency personnel not authorized to do so. Solicitation for comments or reactions should be directed to the on-duty Shift Supervisor.

When conducting an authorized interview with the media or general public concerning an incident involving patient care the following may be disclosed:

- Number of patients
- Age of patient/patients
- Sex of Patients
- Location of incident
- Generalized types of injuries, in layman terms
- Mode and destination of transport
- General condition of patient /patients
- Assisting Agencies

Do not discuss calls or specific information that deals with or could easily intrude upon Private Health Information (PHI), placing blame or fault, or any specifics surrounding the circumstances of the incident.

When issuing an authorized statement to the media concerning an operational or personnel issue the following will apply:

- If a personnel issue has occurred no information shall be disclosed concerning the identity of personnel involved;
- While representing LCEMS to the media or public no statement containing opinionated, accusatory, or defensive stances shall be issued;
- If dealing with an operational issue the policy concerning the issue may be quoted to the media;
- Any discussion of operational issues beyond quotation of policy is prohibited unless expressly authorized by the Director.
- Any incident involving a public official or any person/persons drawing abnormal public attention should immediately be brought to the attention of the Director and Public Information Officer prior to issuing a press statement.
- Employees failing to comply with this policy shall be subject to disciplinary action up to and including dismissal.
- Allied agencies failing to comply with this policy shall be in violation of the Business Associate Agreement.