	Lower Providence Emergency Medical Service Standard Operating Guidelines	
	Subject: <i>Administration - HIPAA Compliance</i>	SOG #100-005
	Approved: Chief Christopher J. Reynolds	Initiated: July 2023 Revised: N/A

Description: To ensure that Lower Providence Community Center Ambulance (LPCCA) DBA: Lower Providence EMS, releases Protected Health Information (PHI) in accordance with the Privacy Rule. This SOG establishes a definition of what information should be accessible to patients or appropriate requestors 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 the Company to make decisions about the patient.

Under the HIPAA Privacy Rule, individuals have the right to access and to request amendment or restriction on the use of their protected health information, or PHI, and restrictions on its use that is maintained in “designated record sets,” or DRS.

To ensure that Lower Providence Community Center Ambulance only releases the PHI that is covered under the Privacy Rule, this guideline outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

Purpose: 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.

Only information contained in the DRS outlined in this SOG is to be provided to patients who request access, amendment and restriction on the use of their PHI in accordance with the Privacy Rule and the Privacy Practices of LPEMS.

LPEMS maintains levels of access to Protected Health Information (PHI) of our various members and follows the stated procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone’s responsibility.

Procedure:

1. The Designated Record Set

1.1. The DRS for any requests for access to PHI includes the following records:

- 1.1.1. The patient care report or PCR 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 PCR.
- 1.1.2. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.

- 1.1.3. 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.
 - 1.1.4. 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.
 - 1.1.5. 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.
2. 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 the Company as part of treatment and payment purposes related to the patient.
3. Patient Access:
 - 3.1. Upon presentation to the business office, the patient or appropriate representative will complete a Request for Access Form.
 - 3.2. The Company employee must 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.
 - 3.3. The completed form will be presented to the Privacy Officer for action.
 - 3.4. The Privacy Officer will act upon the request within 30 days, preferably sooner. Generally, the Company must respond to requests for access to PHI within 30 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 60 days.
 - 3.5. If the Company is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why the Company could not respond within the time frame and in that case the Company may extend the response time by an additional 30 days.
 - 3.6. Upon approval of access, patient will 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.
 - 3.7. The business office will establish a reasonable charge for copying PHI for the patient or appropriate representative.
 - 3.8. Patient access may be denied for the reasons listed below, and in some cases the denial of access may be appealed to the Company for review.

- 3.9. 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:
 - 3.9.1. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
 - 3.9.2. 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.
- 3.10. The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:
 - 3.10.1. 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;
 - 3.10.2. 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;
 - 3.10.3. 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 you is reasonably likely to cause harm to the individual or another person.
- 3.11. If the denial of the request for access to PHI is for reasons 2.10.1,2,or 3, then the patient may request a review of the denial of access by sending a written request to the Privacy Officer.
- 3.12. The Company will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The Company will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. The Company will provide the patient with written notice of the determination of the designated reviewing official.
- 3.13. 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 Company's determination.
- 3.14. Access to the actual files or computers that contain the DRS that may be accessed by the patient or requestor should not be permitted. 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 Company staff member. **UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.**
- 3.15. If the patient or requestor would like to retain copies of the DRS provided, then the Company may charge a reasonable fee for the costs of reproduction.
- 3.16. Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book 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.

3.17. 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.

4. Requests for Amendment to PHI

4.1. The patient or appropriate requestor may only request amendment to PHI contained in the DRS. The "Request for Amendment of PHI" Form must be accompanied with any request for amendment.

4.2. The Company must act upon a Request for Amendment within 60 days of the request. If the Company is unable to act upon the request within 60 days, it must provide the requestor with a written statement of the reasons for the delay, and in that case may extend the time period in which to comply by an additional 30 days.

5. Granting Requests for Amendment

5.1. All requests for amendment must be forwarded immediately to the Privacy Officer for review.

5.2. If the Privacy Officer grants the request for amendment, then the requestor will receive a letter indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.

5.3. There must be written permission provided by the patient so that that the Company may notify the persons with which the amendments need to be shared. The Company must provide the amended information to those individuals identified by having received the PHI that has been amended as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

5.4. The patient must identify individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving the Company permission to provide them with the updated PHI.

5.5. The Company will add the request for amendment, the denial or granting of the request, as well as any statement of disagreement by the patient and any rebuttal statement by the Company to the designated record set.

6. Denial of Requests for Amendment

6.1. The Company may deny a request to amend PHI for the following reasons: 1) If the Company did not create the PHI at issue; 2) if the information is not part of the DRS; or 3) the information is accurate and complete.

6.2. The Company must provide a written denial, and the denial must be written in plain language and state the reason for the denial; the individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement; a statement that, if the individual does not submit a statement of disagreement, the individual may request that the provider provide the request for amendment and the denial with any future disclosures of the PHI; and a description of how the individual may file a complaint with the covered entity, including the name and telephone number of an appropriate contact person, or to the Secretary of Health and Human Services.

- 6.3. If the individual submits a “statement of disagreement,” the provider may prepare a written rebuttal statement to the patient’s statement of disagreement. The statement of disagreement will be appended to the PHI, or at the Company’s option, a summary of the disagreement will be appended, along with the rebuttal statement of the Company.
- 6.4. If the Company receives a notice from another covered entity, such as a hospital, that it has amended its own PHI in relation to a particular patient, the ambulance service must amend its own PHI that may be affected by the amendments.

7. Requests for Restriction

- 7.1. The patient may request a restriction on the use and disclosure of their PHI.
- 7.2. The Company is not required to agree to any restriction, and given the emergent nature of our operation, we generally will not agree to a restriction.
- 7.3. **ALL REQUESTS FOR RESTRICTION ON USE AND DISCLOSURE OF PHI MUST BE SUBMITTED IN WRITING ON THE APPROVED COMPANY FORM. ALL REQUESTS WILL BE REVIEWED AND DENIED OR APPROVED BY THE PRIVACY OFFICER.**
- 7.4. If the Company agrees to a restriction, we may not use or disclosed 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, the Company may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.
- 7.5. The agreement to restrict PHI will be documented to ensure that the restriction is followed.
- 7.6. 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 the Company as long as the Company notifies the patient that PHI created or received after the restriction is removed is no longer restriction. PHI that was restricted prior to the Company voiding the restriction must continue to be treated as restricted PHI.

8. Members with access to entire designated record set and purposes

- 8.1. Billing personnel for billing purposes
- 8.2. Chief or his/her designee for quality assurance programs, investigating deviations from standard operating guidelines or medical protocols, billing purposes
- 8.3. Organization President or his/her designee for investigating deviations from standard operating guidelines or medical protocols, billing purposes

9. Members with restricted access to designated record set and purposes

- 9.1. General members providing care while on duty for ensuring continuity of care, conveying pertinent information to receiving healthcare providers, documentation, quality assurance programs

10. Lower Providence Community Center Ambulance 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.

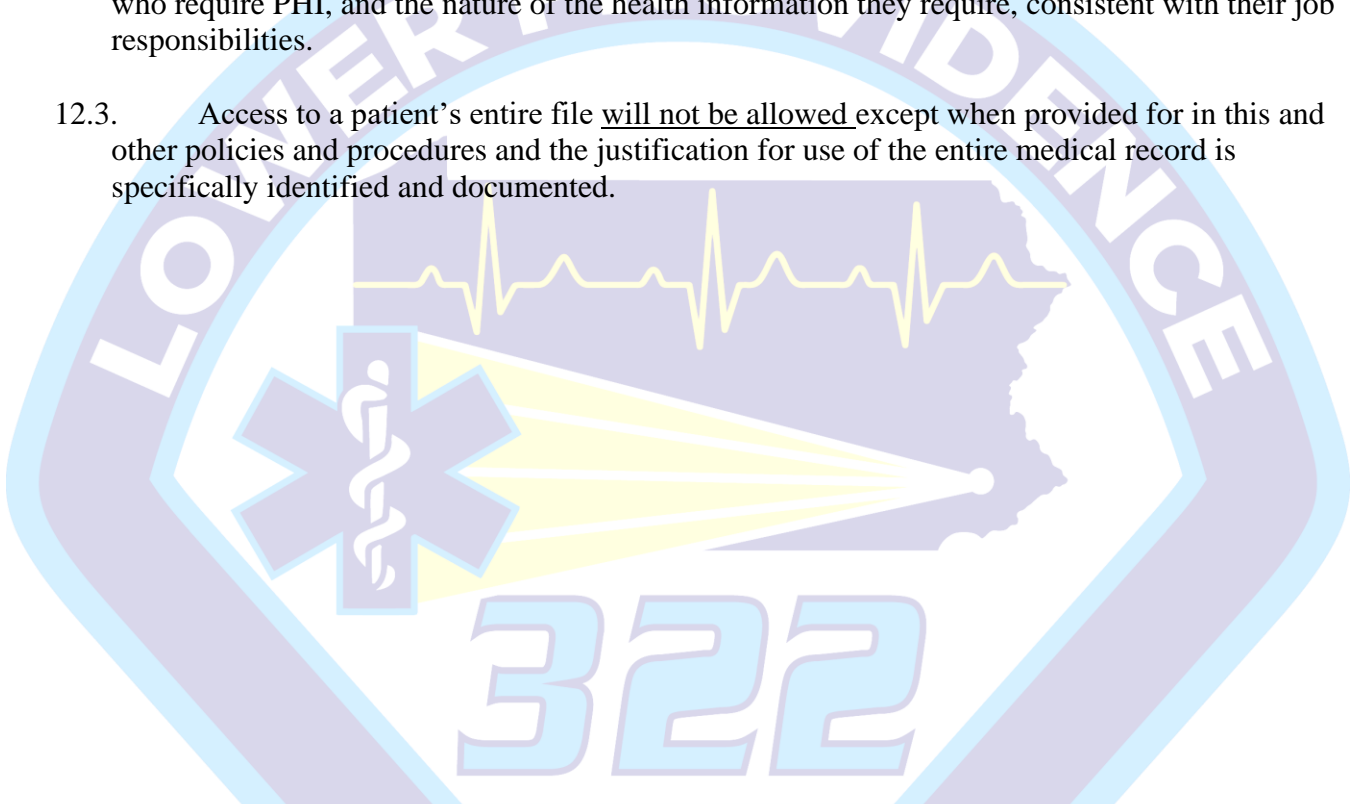
11. When PHI is accessed, disclosed, and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

12. Role Based Access

12.1. 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.

12.2. Access to PHI is limited to the below-identified person(s) only, and to the identified PHI only, based on the Company’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.

12.3. 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.



Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
EMT	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
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
Field 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
Dispatcher	Intake forms, preplanned CAD information on patient address	May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty
Training Coordinator	Intake forms from dispatch, patient care reports	May access only as a part of training and quality assurance activities. All individually identifiable patient information should be redacted prior to use in training and quality assurance activities
Department Managers		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel

13. Disclosures to and Authorizations from the Patient

- 13.1. You are not required to limit to the minimum amount of information necessary required to perform your job function, or your 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 the Company.
- 13.2. Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct you to release PHI to those entities are not subject to the minimum necessary standards.
- 13.3. For example, if we have a patient's authorization to disclose PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, the Company is permitted to disclose the PHI requested without making any minimum necessary determination.

14. Company Requests for PHI

- 14.1. If the Company 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 is non-recurring or non-routine, like making a request for documents via a subpoena, we must review 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

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

15. *Incidental Disclosures*

15.1. The Company 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.

15.2. The fundamental principle is that all staff needs to be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information. Coworkers 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.

15.3. 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:

16. Verbal Security

- 16.1. 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.
- 16.2. 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.
- 16.3. 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.

17. Physical Security

- 17.1. 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.
- 17.2. 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.
- 17.3. 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 Lower Providence Community Center Ambulance Policy on Use of Computer Equipment and Information Systems.