Patient Medical Record Security and Privacy

803.1 PURPOSE AND SCOPE

The purpose of this policy is to establish appropriate administrative, technical, and physical safeguards for patient medical records and to provide reasonable safeguards against prohibited uses and disclosures of protected health information (PHI) in accordance with federal and state law, to include the following:

- Health Insurance Portability and Accountability Act (HIPAA) (42 USC § 201 et seq.)
- ORC § 1347.01 et seq.

803.1.1 DEFINITIONS

Definitions related to this policy include:

Health information - Any information, whether oral or recorded in any form or medium, that is created or received by the Department and relates to a person's past, present, or future physical or mental health or condition, or past, present, or future payment for the provision of health care to a person (45 CFR 160.103).

Individually identifiable health information - Health information, including demographic information, created or received by the Department that relates to an individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to an individual that can either identify the individual, or provide a reasonable basis to believe the information can be used to identify the individual (45 CFR 160.103).

Limited data set - PHI that excludes the following direct identifiers of an individual or of relatives, employers, or household members of the individual (45 CFR 164.514(e)):

- Names
- Postal address information, other than town or city, state, and ZIP code
- Telephone or fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers

- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and/or any comparable images

Patient medical records - Department records or data containing any information identifying a patient. However, media recorded by department body-worn cameras is for quality assessment and improvement purposes, not patient care, and therefore is not part of a patient's medical records.

Protected Health Information (PHI) - Individually identifiable health information that is created or received by the Department. Information is protected whether it is in writing, in an electronic form, or communicated orally (45 CFR 160.103).

Protected Personal Information (PPI) - Information that includes but is not limited to PHI, pictures or other forms of voice or image recording, patient address, telephone numbers, Social Security number, date of birth, age, or any other information that could be reasonably used to uniquely identify the patient or that could result in identity theft if released for unauthorized purposes or to unauthorized personnel.

803.2 POLICY

It is the policy of the Department to reasonably safeguard PHI and comply with HIPAA and the implementing regulations through the use of policy and procedures, system access security and passwords, and limited physical access to hard copy files (45 CFR 164.530(c)).

803.3 RESPONSIBILITIES

Members shall protect the security, confidentiality, and privacy of all patient medical records in their custody at all times.

Possessing, releasing, or distributing PPI, including for unauthorized purposes, is prohibited and may violate HIPAA and/or other applicable laws. Members who have not received department training on the proper handling of these records shall not access patient medical records.

Members with occupational access to patient medical records shall be trained in the proper handling of PHI in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Training Policy and shall reasonably ensure that no unauthorized person shall have access to PHI without the valid authorization of the patient, except as provided by law (45 CFR 164.530(b); 45 CFR 164.512).

803.4 PRIVACY OFFICER

The Fire Chief shall be the privacy officer who is responsible for all matters relating to the privacy of patient medical information, including PHI. The privacy officer shall (45 CFR 164.530):

(a) Identify who may have access to PPI and PHI.

(b) Resolve complaints under HIPAA.

(c) Mitigate, to the extent practicable, any harmful effects known to the Department regarding any use or disclosure of PHI in violation of this policy or the HIPAA regulations.

(d) Ensure members are trained in the proper handling of PHI in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Training Policy.

(e) Ensure technical and physical safeguards are implemented to maintain security and confidentiality of PHI and to allow access to PHI only to those persons or software programs that have been granted access rights.

803.5 PROCEDURE

Records containing PHI or PPI, including Patient Care Reports (PCRs), shall be kept out of view unless the report is being completed during an incident, during input of information into the National Fire Incident Reporting System (NFIRS), or during processing or review at Mansfield Fire Department facilities by authorized personnel (45 CFR 164.530(c)).

803.6 SECURITY

All patient records containing PHI or PPI shall be kept secure at all times whether the record is in written, verbal, electronic, or any other visual or audible format (45 CFR 164.306(a)).

Documents provided by a patient or caregiver will receive the same level of confidentiality and security as department records during the time department personnel retain possession of the documents.

No patient record, including documents and electronic images containing PHI, shall be visible to the public.

803.6.1 ELECTRONIC PHI SECURITY

All computer workstations and servers within the Department shall require appropriate security measures, such as user identification and login passwords, to access electronic documents, including electronic PHI (45 CFR 164.308(a)(5)).

Members with access to electronic data shall lock their workstations when left unattended and shall shut down their workstations when leaving for the day to prevent unauthorized access to electronic PHI (45 CFR 164.310; 45 CFR 164.312).

Remote access to department computer workstations requires that appropriate security measures be provided for access to PHI (45 CFR 164.312).

PHI may be transmitted electronically, provided the transmission occurs through a secure process that allows end-to-end authentication and the recipient is authorized to receive the information. Electronic transmission consists of email, file transfer protocol, internet web posting, and any configurable data stream. End-to-end authentication is accomplished when the electronic referral does not leave a secure network environment and the recipient is known, or when encryption and authentication measures are used between sender and recipient, thus verifying full receipt by

the recipient. Any electronic PHI traveling outside a secure network environment, via the internet, requires encryption and authentication measures (45 CFR 164.312(e)).

803.6.2 HARD COPIES

Hard copies of PCRs shall be kept in a secured area when unattended by authorized personnel. An area of the Department is considered unattended when members are physically outside of the office area and unable to maintain record security. This includes but is not limited to breaks, lunch, or meetings outside the Department.

Hard copies of PCRs should be stored in a locked area whenever practicable for ease of record retention and retrieval.

Patient records shall not be removed from the Department without express authorization from the Custodian of Records.

803.7 PHI RECORD REQUESTS

The following procedures apply to PHI record requests:

(a) Requests and subpoenas for copies of patient records shall be processed by the Custodian of Records.

(b) The Custodian of Records or the authorized designee shall not release records containing PHI without a properly completed authorization to release medical records that is signed by the patient or legal representative of the patient.

1. Verification that the person completing the authorization is the patient or the legal representative of the patient shall be made with government-issued identification and documentation (45 CFR 164.508(c)).

(c) Fulfilled records requests shall be placed in a sealed envelope for release to the requestor.

(d) A full copy of the valid subpoena or authorization to release medical records form shall be maintained in the file with the PCR.

803.7.1 PROHIBITED DISCLOSURES OF PHI AND PPI

The Department shall not use or disclose PHI or PPI without authorization. Prohibited disclosures include any form of communication, except as permitted in this policy, including but not limited to (45 CFR 160.103):

(a) PHI or PPI contained in email or other forms of written communication.

(b) Sharing of PHI or PPI on any website, blog, or other form of social or public media.

(c) Verbal discussions.

(d) The use of any imaging device capable of capturing and storing still or moving images, such as digital or other cameras, video cameras, cellular telephones with picture-taking or video-recording capability, or any other device with picture-taking or video-recording capability while engaged in patient care, while at the scene of a medical emergency or hospital, or at any time when such use could reasonably be expected to result in the inappropriate capture of PHI or PPI.

803.7.2 PERMITTED DISCLOSURES OF PHI AND PPI

The Custodian of Records may release records containing PHI or PPI without authorization from the patient under any of the following circumstances:

(a) For the department's use to carry out treatment, payment, or health care operations (45 CFR 164.506)

(b) Where the PHI is requested pursuant to a valid subpoena or court order (45 CFR 164.512(e))

(c) Where the PHI is part of a limited data set (45 CFR 164.514(e))

(d) Where the PHI is used for public health activities authorized by law, including when the information is necessary to report child abuse or neglect (45 CFR 164.512(b))

(e) Where the PHI is disclosed to a government authority because the person is believed to be a victim of abuse, neglect, or domestic violence (45 CFR 164.512(c))

(f) To law enforcement as provided in this policy (45 CFR 164.512(f))

(g) Where the Department believes that disclosure of the information is necessary to avert a serious threat to the health or safety of a person or the public (45 CFR 164.512(j))

(h) Where the PHI is required for workers' compensation purposes (45 CFR 164.512(l))

803.7.3 REQUIRED DISCLOSURES

The Department must disclose PHI when:

(a) The PHI is requested by and provided to the individual to whom the PHI belongs (45 CFR 164.502(a)(2)).

(b) The information is required by the U.S. Secretary of Health and Human Services to investigate compliance with HIPAA (45 CFR 164.502(a)(2)).

803.7.4 SUBPOENAS

Records containing PHI or PPI will be disclosed only if one of the following is present (45 CFR 164.512(e)(1)):

(a) A court order or subpoena signed (or stamped) by a judge that requires no additional assurances or notification to the individual whose records are requested

(b) A subpoena or discovery order signed by an attorney which requires additional proof of service that written notification has been given to the individual whose records are requested. In such a case, the subpoena or discovery order must be accompanied by a declaration by the requesting party showing that reasonable efforts have been made to ensure that notice has been provided to the individual whose records are being requested, or that there is a qualified protective order. No records relating to the person named in the notice will be produced until the time to respond to the notice has lapsed and no objections to the production of the materials requested have been made. If written notification to the individual is not provided, the declaration must establish all of the following:

1. The requesting party has made a good faith effort to provide written notice to the individual.

2. The notice includes sufficient information about the litigation or proceeding for which the PHI is requested to allow the individual to raise an objection.
3. The time for the individual to raise objections to the court or tribunal has elapsed.
4. No objections were filed or all objections have been resolved.
5. In lieu of a declaration, records may be released if there is a court order or a stipulation by the parties to the litigation that both:
    (a) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested.
    (b) Requires the return to the Department or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

803.7.5 RELEASE OF PHI TO LAW ENFORCEMENT

The release of PHI to a law enforcement agency is permitted under the following circumstances:

(a) In response to a law enforcement officer who completes the department's release of PHI to law enforcement form and requires the PHI (45 CFR 164.512(f)(1)):
    1. To report certain types of wounds or other physical injuries.
    2. In compliance with a court order or court-ordered warrant, a subpoena or summons, a grand jury subpoena, or an administrative request for which a response is required by law.
(b) In response to a law enforcement officer who completes the department's release of PHI to law enforcement form for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. In such a case, the Department may only disclose the following PHI (45 CFR 164.512(f)):
    1. Name and address
    2. Date and place of birth
    3. Social Security number
    4. ABO blood type and Rh factor
    5. The character and extent of injuries
    6. Date and time of treatment
    7. Date and time of death, if applicable
    8. A description of distinguishing physical characteristics
(c) The name and address, if known, of an individual to whom naloxone was administered due to an actual or suspected drug overdose should be disclosed upon request to a law enforcement agency in accordance with ORC § 3715.505 and 45 CFR § 164.512.

803.7.6 ADDITIONAL RESTRICTIONS FOR REPRODUCTIVE HEALTH CARE RECORDS

Records related to reproductive health records as defined by 45 CFR 160.103 are subject to additional disclosure restrictions as provided in 45 CFR 164.502 and 45 CFR 164.509. Requests

that may include reproductive health care records should be evaluated by the Custodian of Records in consultation with legal counsel before disclosure to ensure compliance with federal law.

803.8 INDIVIDUAL RIGHTS

The privacy officer is responsible for ensuring the Department complies with all of the following rights of patients:

(a) The right to request restrictions on certain uses and disclosures of PHI (45 CFR 164.522(a))

(b) The right to receive their PHI confidentially (45 CFR 164.522(b))

(c) The right to inspect and copy their PHI (45 CFR 164.524)

(d) The right to request amendments to their PHI (45 CFR 164.526)

(e) The right to receive an account of disclosures of PHI (45 CFR 164.528)

803.8.1 PHI AMENDMENT REQUESTS

Patients have the right to review their PHI records and, if necessary, to request that amendments be made. A patient must make a request in writing to have their medical record amended. Included in the request must be the patient's account of the incident and what specific amendment is being requested (45 CFR 164.526(b)(1)).

The privacy officer has the authority to deny the request for amendment where the PHI (45 CFR 164.526(a)(2)):

(a) Was not created by the Department.

(b) Is not part of the designated record.

(c) Is not available for inspection by the requestor pursuant to 45 CFR 164.524.

(d) Is accurate and complete.

Within 60 days of receipt of the request for amendment, the privacy officer must provide the basis for its denial in writing or, in the case that the request is approved, provide notice of approval (45 CFR 164.526(b)(2)).

The time for response may be extended for up to 30 days with a written statement to the requestor identifying the reasons for the delay and the date by which the action will be completed (45 CFR 164.526(b)(2)).