COHESIVE HEALTHCARE MANAGEMENT & CONSULTING

MANGUM REGIONAL MEDICAL CENTER

TITLE		POLICY
Location, Security, Maintenance and Destruction of Medical Records		**HIM-039**
MANUAL	EFFECTIVE DATE	REVIEW DATE
Health Information Management	**8/22/2016**	**8/28/2017, 5/2018, 8/30/2019, 12/1/2020**
DEPARTMENT	REFERENCE	
Health Information Management	**See below**	

PURPOSE

To ensure the integrity, safety, security, and confidentiality of the medical record. Further, to prevent loss and inappropriate access or unauthorized use.

POLICY

It is the Mangum Regional Medical Center policy that medical records be maintained in a secure and confidential manner. The Hospital Health Information Management ("HIM") Manager shall be responsible for the security, storage, and maintenance of medical records (including paper or electronic format) and/or individual patient reports against loss, defacement, tampering, removal from the Hospital and unauthorized use. Access and security of systems containing protected health information ("PHI") is based on designated roles and responsibilities.

PROCEDURE

A. Medical Record Reconciliation and Related Functions:
   1. The HIM department will ensure receipt of all original paper medical records after patient discharge from the hospital.
   2. Copies (duplicate) of individual reports maintained by hospital departments (such as emergency, radiology, or pharmacy) shall only be used for providing follow-up information to the attending or primary care physician, or for responding to requirements for regulatory information (such as those required by pharmacy).

B. Physical Security:
   1. HIM personnel are trained to protect the integrity, safety, security and confidentiality of the record. They are also trained in loss prevention practices, as well as who may or may not access records and for what reasons.

2. All hospital personnel are trained to protect against any anticipated threats or hazards to the security and integrity of patient PHI.
3. When the hospital contracts with an external company to store and maintain the records, such company will also be responsible for retrieving, delivering, and returning the records to storage, when applicable. Requests for retrieval should be granted through HIM and Administration as negotiated in individual contracts.
    a. This also applies to PHI that is stored electronically with an outside vendor that can offer electronic access to scanned images of the record.
4. All contractors must have a written contract with the Hospital. Contractors must also sign and comply with business associate requirements as set forth by the Health Insurance Portability and Accountability Act ("HIPAA") privacy regulations, state regulations and the signed Business Associate Contract / Business Associates Agreement.
5. PHI storage regardless of whether in the HIM department or through a record storage company will be in accordance with state fire safety standards. Smoke and fire alarm systems should be in place to limit smoke and fire damage.
    a. If PHI is stored electronically with an outside vendor, a copy of the vendor's disaster plan should be provided and reviewed before the contract is signed to ensure a backup plan is available should the vendor's system fail.
6. The HIM department shall provide office space to HIM employees only. To prevent unauthorized use, inappropriate access, and loss of paper documentation non-HIM employees will not be allowed to office in the HIM department or have access to the HIM department unless an HIM employee is present.

C. Maintenance of a Complete and Accurate Medical Record

1. Timely processing and scanning of paper documentation shall occur within twenty-four (24) to forty-eight (48) hours of discharge to prevent loss and ensure record integrity.
2. Incomplete record analysis process shall occur within twenty-four (24) to seventy-two (72) hours to ensure an accurate and complete record.
3. Re-analysis process, to include phone calls and letters, shall occur daily in order to obtain identified deficiencies on a daily basis.

D. Removal of Records from the Hospital

1. Removal of medical records or copies of medical records from the hospital is strictly prohibited except as outlined below and will result in immediate disciplinary action.
    a. In response to a subpoena or court order addressed to the Hospital Administrator or HIM Manager.
    b. Risk management and/or hospital administration must be notified when records leave the Hospital under these circumstances.
2. Medical records shall be released in accordance to the Uses and Disclosures of Protected Health Information policy (See HIP-000); Release of Information; Patient & Third-Party Requests policy (See HIP-001), as well as HIM Department specific policies related to Release of Information.

E. Record Retention

1. Medical records will be retained for a period of ten (10) years after the last episode of care.

F. Technical Safeguards

1. Access to Electronic Health Record requires secure user Id's, passwords and is role-based.
2. Staff are required to log off or lock computer when leaving the area.
3. Automatic log off procedures are enabled.
4. Workstations require person authentication.
5. Routine audits of access and changes to EMR are conducted.
6. Contingency plans and data backup plans are in place.
7. Data is encrypted.
8. Anti-hacking and anti-malware software is installed.

G. Destruction

1. Hospital has a duty to protect the confidentiality and integrity of confidential PHI and ePHI as required by law.
2. Hospital, its officers, employees, and agents must destroy data that is no longer necessary to retain in the regular course of business pursuant to Hospital's Retention Schedule. Hospital, its officers, employees, and agents must not destroy data that is involved in audit, investigation, or litigation.
3. Hospital's employees and agents must destroy data as follows:
    a. Destruction of Paper PHI Documents.
    b. Do not dispose of paper documents containing PHI in trash bins, dumpster or in other containers accessible by the public or unauthorized persons.
    c. Methods to dispose paper documents containing PHI include burning, shredding, pulping, and pulverizing so that PHI is essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
    d. Records involved in any open litigation, audit, or litigation must not be destroyed until the litigation case has been closed.
4. The Information Technology Manager and the HIM Manager are responsible for determining whether to shred in-house or to use a commercial destruction service. The Information Technology Department and the HIM Manager must approve the method of destruction. Destruction and disposal of Hardware and electronic media.
    a. Computers and/or hard drives must be degaussed upon disposal or otherwise disposed of in a manner approved by the Information Technology Manager and the HIM Manager.
    b. Magnetic media and tapes must be degaussed or demagnetized (reducing magnetic induction to zero by applying a reverse magnetizing field) or erased by overwriting and purging using an approved program. The Information Technology Manager and the HIM Manager are responsible for choosing a method of destruction and for determining whether to destroy in-house or to use a commercial destruction service. The Information Technology Manager and the HIM Manager must approve the method of destruction.
    c. Microfilm or microfiche methods of destruction include recycling and pulverizing.

d. Hard drives, flash drives, and USBs are destroyed by shredding, disintegrating, pulverizing or burning by licensed incinerator.
e. DVDs are destroyed by shredding or cutting.
f. Laser discs used in write once-read many document-imaging applications are destroyed by pulverizing.
g. Hardware shall be properly logged and disposed of when no longer used through the Information Technology Manager .

5. Destruction and Disposal of Leased Equipment or Devices
    a. Hospital cannot destroy leased equipment or devices.
    b. Any IT equipment leased to the Hospital by a vendor that contains data storage such as internal hard drives (e.g. computers, mobile phones, tablets copy machines, multi-function devices, printers, fax machines, medical equipment, etc.) must be wiped of all data before being returned to the vendor. This includes returns due to service as well as lease-end.
        i. Lease agreements will include requirements for the vendor to irretrievably destroy all data on internal storage devices.
        ii. The vendor will provide a Certificate of Disposal in compliance with applicable federal, state and/or local regulations.
        iii. Certificates of Disposal are maintained by Hospital and retained for a minimum of six (6) years.
6. Hospital shall clear data from mobile phones or tablets by completing the following steps. Follow these steps to erase sensitive information from mobile devices:
    a. Remove the memory/SIM card.
    b. Go to the devices setting and select Erase All Settings, Factory Reset, Memory Wipe, etc. The language differs from model to model but all devices should have some version of this option.
    c. Destroy the memory/SIM card so that it cannot be used again.
    d. Deactivate the storage account (Apple ID for iPhones and iPads) associated with the device.
7. Department directors will keep destruction records for not less than six (6) years and include the following:
    a. Individual's records destroyed.
    b. The dates of services included in the records.
    c. Date of destruction.
    d. Description of the disposed records.
    e. Method of destruction.
    f. The signatures of the individuals supervising and witnessing the destruction.
8. The Information Technology Manager and the HIM Manager is responsible for ensuring that selected destruction services have signed business associate contracts before providing destruction services.
    a. In accordance with HIPAA privacy rules, if destruction is accomplished through a business associate, the contract must include:
        i. Method of destruction.
        ii. The time that will elapse between acquisition and destruction.
        iii. Safeguards against security breaches.

iv. Indemnification for the Hospital or provide for loss due to unauthorized disclosure.
v. Business associate will have liability insurance in the amount specified.

REFERENCES

42 CFR § 485.638(b)(1),(2),(3)(c)

45 CFR § 164.306, 164.310 and 164.312

45 CFR Parts 160 and 164

UPDATES/REVISIONS

Date	**Brief Description of Revision/Change**
8/30/2019	Change in header, number, font, format, and update in procedure.
12/1/20	Change in header and spacing. Apply acronym. Use number word format. Add Attachments section. Add References section. Renamed policy from Location, Security and Maintenance of Medical Records to Location, Security, Maintenance and Destruction of Medical Records. Change paragraph numbering format. Consolidated information from policy HIP-061 for clarity, concise and pertinent content.