**Policy and Procedure: Medical Documentation**

<Incorporate your organization’s existing policies and procedures that apply to these recommendations.>

<FIND and REPLACE WORDS: Look for the words in GREY. Find and replace the following words to shortcut development of this policy and procedure:>

* <insert Organization’s name> = Your Organization’s Name
* Patient, patients, patient = Use the most appropriate words that describes the individuals that your organization services (i.e., patient, resident, participant, client)

Insert additional organizational information in all other areas marked in GREY.

<Delete these instructions in RED>

## Policy: Medical Documentation

During disasters, resources, communications, and access to power may be uncertain. It is important for organizations to develop a policy and procedure to guide continuity of medical services. This policy developed by <insert Organization’s name> identifies a system to provide medical documentation that preserves and protects patient confidentiality, while securing availability of medical records during a disaster. This policy establishes standards for staff to effectively document medical services rendered during a disaster and loss of power. This policy complies with the Health Insurance Portability and Accountability Act (HIPAA) Center for Medicare and Medicaid Services (CMS) regulations as well as local, state, and federal licensing standards.

### Policy and Procedure Objectives: Medical Documentation

* Preserves and protects the confidentiality of patient information
* Secures and maintains the availability of medical records
* Defines a “Go to Paper” protocol that will be utilized to document medical services when electronic medical records cannot be accessed during a disaster

### Procedures: Medical Documentation

This procedure will ensure that staff are able to document medical services provided should electronic systems and/or utilities fail. This procedure will also provide staff with a process to secure patient records and maintain continuity of care during an emergency.

### Staff Responsibilities

* Understand and comply with this Medical Documentation Policy & Procedure
* Understand their unique role during an emergency
* Follow the Incident Command System assignments
* Follow orders given by public safety authorities (fire, police, etc.)
* Remain calm and use common sense and good judgment

### Organizational Responsibilities

During an emergency or disaster, continued access to patient medical information is vital. <insert Organization’s name> has implemented the following procedures to preserve and secure patient’s Personal Health Information (PHI).

* + Documentation of patient’s medical records including PHI are completed according to HIPAA and CMS regulations as well as local, state, and Federal licensing standards.
* Specific HIPAA regulations include 45 CFR parts 160 and 164 for Emergency Contacts, Medication and Problem List, and Allergy and Adverse Medication Reaction List.
* Review the disaster recovery plan <insert frequency of review>.
* Determine a process to document patients’ records should computer systems become disabled or damaged by a disaster.
* Develop a detailed process to ensure timely availability of electronic medical record systems.

### “Go to Paper” Protocol in the Event of a Power or Utility Outage

If power is lost during a disaster and electronic medical records (EMR) are inaccessible, it is important for <insert Organization’s name> to be able continue to provide medical services to the furthest extent as possible as well as document all aspects of care provided.

* All paper records that include PHI must be kept secured.
* All medical records will be stored out of sight of unauthorized individuals, and should be locked in a cabinet, room, or building when not in use.
* A designated staff member will supervise all aspects of the Go to Paper Protocol**.**
* All incidents that may involve the loss or theft of any paper records will be reported to your Privacy Officer or supervisor.
* Determine which staff members are authorized to access the area where patient files are located.
* Patient folders with blank medical record forms will be readily available for use in the event of an EMR outage.
* Transportation of medical records within a program site must adhere to the following guidelines:
* Ensure PHI is facing away from public view.
* Use an envelope or accordion folder to store PHI.
* Place PHI in secure containers or cover the records when on a rolling cart.
* Never leave PHI (including portable media devices) unattended.
* Transportation of medical records that contain PHI outside of the program site must adhere to the following guidelines:
* Transportation of PHI to an off-site location must be approved by your supervisor and may only be transported if it is necessary.
* Transport the minimum amount of PHI necessary.
* Never leave PHI (including portable media devices) unattended; this includes vehicles.
* Maintain a log of all files and documents that are physically transferred.
* Upon arrival at the new location, immediately ensure you are in possession of all listed files.
* Once the power/utility outage has been restored, paper medical records shall be incorporated into the patient’s medical record.

<Incorporate your existing procedures here. Delete these instructions in RED>.

### Securing and Maintaining the Availability of Records

As required by HIPAA, a disaster recovery plan includes a series of systematic steps that will be followed when it is time to return to normal operations:

<Insert organization’s name> Information Technology Disaster Recovery components include:

* Activation (when and how to declare a disaster)
* Assessment (determining the root cause and assessing the disaster's impact)
* Containment and control (steps to prevent escalation)
* Recovery (steps to get mission critical applications and systems quickly restored)
* Emergency mode operation procedures (how the organization will function until operations return to normal)
* Restoration (returning to normal operations may mean shifting data center operations from an alternate site to the primary data center) and exercising (when and how the disaster recovery plan will be tested)

### Disaster Recovery Strategies

* **High Availability/Redundancy:** Use of virtualized servers and systems to maintain high availability.
* **Data Back-Up Plan:** Implementation and testing of a data back-up plan with recovery point objectives.
* **Mission Critical Systems:** An inventory of applications and systems including their designated criticality to the mission. The business impact analysis identifies and prioritizes application systems as well as defines recovery objectives.
* **Emergency Operations Procedures:**The IT Disaster Recovery Plan Business Continuity Plan provides guidance during an emergency. Normal business processes and procedures may have to be suspended during a disaster recovery situation. Refer to the IT Disaster Recovery Plan Business Continuity Plan for more information.
* **Recovery (Resynchronization):** Information stored on paper must be reintegrated into electronic systems, procedures.