Ochsner Health

Operational Standard

TITLE: Business Continuity

EFFECTIVE DATE: 11/27/2020

APPROVER(S): Laura Wilt (Sys VP-CIO)

NUMBER: OHS.IS.OS.004

I. Purpose

The purpose of this operational standard is to enable continued operation of business and patient care processes in the event of a disruption to, or outage of, supporting computer systems.

II. Scope

This operational standard applies to (i) Ochsner Health, (ii) Ochsner Clinic Foundation, and/or (iii) all facilities and entities wholly owned and/or leased by Ochsner Clinic Foundation ("Ochsner").

This operational standard covers both centralized and decentralized computer systems that create, access, transmit, receive or store ePHI used for treatment, payment, or health care operations. This operational standard also covers other computer systems that are critical to patient care or business needs of Ochsner.

III. Definitions

A. Disruption – An unexpected incident that causes a disruption in the normal processing of an Information Asset.

B. Downtime – A planned or unplanned state caused by a planned or unplanned disruption to or outage of a supporting Information Asset.

C. Electronic Protected Health Information (ePHI) - under HIPAA means any electronic health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; And that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual (like phone number, address, SSN, etc.).

D. Information Assets -Hardware or software that creates, receives, stores or transmits electronic data used for patient care, clinical research or in support of Ochsner business processes; including all data maintained or accessed through systems owned or administered by or on the behalf of Ochsner.

E. System Administrators – the custodians of the system as assigned by the system owner/s. Those designated by the system owner to manage process or store Information Assets.

F. Outage – The unavailability of an Information Asset.

IV. Operational standard Statements

A. Formal documented Business Continuity Plans must be developed in order to continue critical business operations and patient care in the event of a Disruption to or Outage of an Information Asset.

V. Standards and Roles & Responsibilities

A. Ochsner units in coordination with System Administrators must develop a documented Business Continuity Plan to follow in the event of a Disruption to, or an Outage of, a supporting Information Asset. The Plan must be developed in coordination with the appropriate System Administrator(s).

B. Business Continuity Plans must at a minimum include the following components:

1. Activation Procedures – Provides guidance on what issues would warrant the activation of a unit's Business Continuity Plan and who is authorized to activate the plan.

2. Key Roles and Responsibilities – Assigns key roles and responsibilities during the response to and recovery from a Disruption or Outage.

3. Work Around Procedures – Details how to continue operations/patient care during information system unavailability which can include:

    a. Working in "off-line mode" – Some systems allow for the capturing of transactions in an "off-line or disconnect mode which temporarily store the transactions for later posting when the system resumes normal operations. Unit personnel should be familiar with and be trained in the use of this capability.

    b. Paper transactions – Pre-designed Forms must be designed and available to unit personnel to aid in the capture of transactions during an Outage or Disruption to a supporting Information Asset. Forms should copy the requirements of online screens as much as possible.

    c. Human elements – How to interact with patients and/or other parties during the Disruption or Outage.

    d. Transaction flows – A description of how the downtime/manual process works as a whole including effects or interrelationships with other units or third parties.

e. Contact information – An up-to-date list of contact information including key personnel and key management.

f. Inventories – Procedures on how to ensure accurate accounting of supply usage.

4. Entry/posting of the off-line transactions when the system becomes available.

VI. Enforcement and Exceptions

A. Requests for exceptions to this standard MUST be submitted in writing to the Chief Information Officer and Chief Compliance Officer and MUST

1. Describe the reason for requesting an exception.

2. Describe the specific impact on workflow process or patient care if request is denied

3. Describe any system limitations causing compliance issues with this Operational standard along with any future plans to address.

4. Requests for exceptions will be answered in writing within 30 days of receipt of the request, approving, denying, or requesting additional information.

B. Failure to comply with this operational standard may result in progressive discipline up to and including termination of employment for employees or termination of contract or service for third-party personnel, students or volunteers.

VII. References

HIPAA Security Rule164.308(a)(7) Contingency Plan

VIII. Operational standard History

OHS.IS.004 Business Continuity