

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY (BCP/DRP)

<<insert date>>

Information Security Office
ENTER PRACTICE NAME HERE

ENTER PRACTICE NAME HERE

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY (BCP/DRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

TABLE OF CONTENTS

I.	Purpose	2
II.	Scope	2
III.	Business Continuity and Disaster Recovery Policy	2

Revision History

Date of Change	Responsible	Summary of Change
September 2018	TTG SAS	TTG template revision v4

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY (BCP/DRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

I. PURPOSE

The purpose of this policy is to address the minimum features that must be documented and implementable in plans that are developed for emergency situations.

To comply with 45 CFR 164.308 to ensure that plans are developed to respond to emergency or similar occurrences.

II. SCOPE

The HIPAA Security rule requires that HIPAA Covered Entities create, implement and test contingency plans to respond to allow for business continuity and disaster recovery of data and systems in emergency or similar situations. Five standard contingency planning components are identified within the HIPAA Security Rule:

1. Data Backup Plan – 45 CFR 164.308 (a) (7) (ii) (A) requires Covered Entities to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
2. Disaster Recovery Plan – 45 CFR 164.308 (a) (7) (ii) (B) requires Covered Entities to establish (and implement as needed) procedures to restore any loss of data.
3. Emergency Mode Operation Plan – 45 CFR 164.308(a) (7) (ii) (C) requires Covered Entities to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information (ePHI) while operating in emergency mode.
4. Testing and Revision Procedures – 45 CFR 164.308(a) (7) (ii) (D) requires Covered Entities to implement procedures for periodic testing and revision of contingency plans.
5. Applications and Data Criticality Analysis– 45 CFR 164.308 (a) (7) (ii) (E) requires Covered Entities to assess the relative criticality of specific applications and data in support of other contingency plan components.

III. BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY

The Practice must implement written Business Contingency set of instructions focused on how to sustain mission/business processes during and after a disruption. Each HIPAA-Covered Component shall develop a Contingency Plan for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages IT resources that contain ePHI.

The Contingency Plan shall include the following components:

1. Identify key personnel and ensure the safety of and minimize injuries to staff during a disaster.

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY (BCP/DRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

2. Establish communication channels and chains of command for decision-making and communication with employees.
3. Document and maintain an application and data criticality analysis to assess the relative criticality of specific applications and data in support of the contingency plan components.
4. Facility access procedures shall be developed, documented and maintained for access to support recovery efforts.
5. Contingency plan testing and revision procedures shall be developed, documented and periodically executed for verifying recovery capabilities. The BCP requires periodic **monitoring** reviews as modified or new procedures may be required to ensure effective recovery of services by all critical departments during any disaster.
6. A data backup plan shall be established, documented and implemented to create and maintain retrievable exact copies of ePHI.
7. Emergency access procedures shall be established, documented and implemented for the retrieval of ePHI during an emergency.
8. A disaster recovery plan shall be established, documented, implemented and tested to restore any loss of data in the event of a disaster.
9. An emergency mode operations plan shall be developed, documented and implemented to protect ePHI during emergency operations of business processes

BUSINESS CONTINUITY & DISASTER RECOVERY POLICY (BCP/DRP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

1 Getting Started

This section addresses the importance of management support and how to effectively organize your plan and employees.

Obtain
Management
Endorsement

Concept of
Operations

Roles and
Responsibilities

Assign
Employees/
Assemble
Employee Info

2 Understanding Your Risks

This section addresses risks facing your company, and examines various disaster scenarios and the protection of employees.

Threat
Assessment

Create an
Evacuation Plan

3 Determining Impact on Operations and Profitability

This section examines your company's potential recovery strategies, including vital records and data.

Vital Records
Necessary to
Recover

Data and
Software
Backup

Offsite
Requirements
and Alternate
Facilities

4 Emergency Response and Operations

This section addresses your company's authority and decision making, emergency response procedures, and crisis communications plans.

Authority
and Decision
Making

Emergency
Response Plan

Strategies for
Types of
Emergencies

Crisis
Communications
Plan

5 Testing and Training

This part of the plan addresses steps to validate the effectiveness of the plan, how to keep plan current, and training of staff.

Exercise
Your Plan

Training and
Keeping the
Plan Current