**Contingency Plan**

**Purpose:**

Per the HIPAA Security Rule [§ 164.308(a)(7)], this policy has been established to produce rules for continuing business without the normal resources of the organization.

**Policy**:

**Data Backup Plan**

1. See Data Backup Policy

**Disaster and Data Recovery Plan**

1. The Information Security Officer will be the Disaster Recovery Coordinator and is in charge of maintaining these policies and procedures along with the Privacy Officer.
2. The Information Security Officer is responsible for setting up and ensuring that they receive SMS and/or email notifications when disasters occur.
3. The Information Security Officer is responsible for carrying out the steps to recover from a disaster.
4. If any outage is encountered that results in data loss, then the Information Security Officer logs the failure including the date/time and any data that was lost. They will also immediately inform management via email.
5. The Information Security Officer or a designee might perform manual EC-2 server and RDS and Elasticsearch database recovery using the corresponding AMI and most recently available backups. Custom documents that exist in either but not both RDS and Elasticsearch services will be reconciled using the API.
6. The Recovery Point Objective is 100% of all data and servers, unless S3 goes down across the entire globe, in which case log data can be reconstructed from the Elasticsearch database.
7. The Recovery Time is dependent on the AWS services coming back online, but once all systems are available the services should be restored within 1-48 hours.
8. The Disaster Recovery Plan is made available to the necessary personnel at all times.
9. The Data Recovery Plan will be tested at least annually and tracked on the Data Recovery Plan worksheet in the Periodic Ledger workbook.

**Emergency Mode Operation Plan**

1. Emergency mode operation involves the following that shall occur to protect the business continuity during and immediately after a crisis situation:
   1. The Information Security Officer has access to SSH keys and AWS account passwords granting them access to ensure business continuity and protection of ePHI.
   2. In the event of an issue affecting the availability of the ISO, a backup leader has been appointed who can access the AWS account. This individual is trained on how to ensure ePHI is secured and normal operations can function and will work with customers to determine the most appropriate path forward.
2. Emergency mode operation involves the following that shall occur to protect the security of ePHI during and immediately after a crisis situation:
   1. All automated alarms and available logs will be assessed to identify failed systems or configurations.
   2. If the failure exposes ePHI in any manner, then the access point will be identified and a fix implemented immediately.
3. These procedures are tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

**Testing and Revision Procedure**

1. The Information Security Officer or designee will test data backups and restoration procedures at least annually.
2. In some instances a test will be performed as part of an upgrade. This counts as the corresponding annual test.
3. This document will be reviewed at least annually or in response to the following events:
   1. Any configuration change or new AWS service introduction.
   2. Major upgrade to Picard API
   3. Breach

**Application and Data Criticality Analysis**

1. The Information Security Officer and Privacy Officer will meet at least annually to identify the criticality of applications and data.
2. The applications and data used in the Data Backup and Disaster Recovery Plans will be specifically discussed to ensure they are still in use.
3. Any other services will be identified and their roles explained in the sections above.