# ORCHID SURGICAL, LLC

# HIPAA SECURITY POLICIES AND PROCEDURES

# ORCHID SURGICAL, LLC
# HIPAA SECURITY POLICIES AND PROCEDURES

## Table of Contents

# General Policy for Electronic Health Information

## Introduction:

It is the policy of Orchid Surgical, LLC ("Company") that all workforce members must preserve the integrity, confidentiality, and availability of electronic protected health information (ePHI) and other sensitive information pertaining to patients of our covered entity clients. The purpose of these *HIPAA Security Policies and Procedures* is to ensure Company's compliance with applicable standards, implementation specifications, and requirements of the HIPAA Security Rule with respect to ePHI. Furthermore, the purpose of these *HIPAA Security Policies and Procedures* is to ensure that Company and its workforce have the necessary medical and other information to provide the highest services possible while protecting the confidentiality of that information to the highest degree possible so that covered entities do not fear providing information to Company and its workforce.

The following individual shall act as the Security Officer for Company: Shonte Amato-Grill. The Security Officer is responsible for the development and implementation of these *HIPAA Security Policies and Procedures.*

## General Policy:

To ensure Company's compliance with the HIPAA Security Rule, Company and its workforce shall:

- Ensure the confidentiality, integrity, and availability of all ePHI Company creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
- Ensure compliance with the applicable HIPAA Security Rule and these *HIPAA Security Policies and Procedures* by its workforce.

## Procedures:

1) Company will use any security measure that allows Company to reasonably and appropriately implement the standards and implementation specifications as specified in the HIPAA Security Rule.

2) In deciding which security measures to use, Company will take into account the following factors:

   - The size, complexity, and capabilities of Company.
   - Technical infrastructure, hardware, and software security capabilities of Company.
   - The costs of security measures.
   - The probability and criticality of potential risks to ePHI.

3) For certain standards and implementation specifications under the HIPAA Security Rule, Company will do the following:

- Assess whether such procedure is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution of the procedure to protecting Company's ePHI.
- If the procedure is reasonable and appropriate, Company shall implement the procedure.
- If implementing the procedure is not reasonable and appropriate, Company shall document why implementation is not reasonable and appropriate, and will implement an equivalent alternative measure, if reasonable and appropriate.

4) These *HIPAA Security Policies and Procedures* and all other security measures implemented by Company in order to comply with the HIPAA Security Rule shall be reviewed by Company and modified as needed to continue Company's provision of reasonable and appropriate protection of its ePHI and Company's compliance with the HIPAA Security Rule.

**Sanctions**:

Company has the right to apply any sanction or combination of sanctions to deal with violations of these *HIPAA Security Policies and Procedures*. Sanctions for workforce members may include, but are not limited to: retraining, verbal warnings, written warnings, paid and unpaid suspensions, exclusion from the premises, loss of privileges and/or benefits, demotion, and termination, in accordance with applicable personnel policies. Please refer to the *Sanctions Policy* in Company's *HIPAA Privacy Policies and Procedures*.

**Enforcement:**

All members of Company's workforce **must** adhere to these *HIPAA Security Policies and Procedures*. Company will not tolerate violations of these Policies. Violation of these Policies is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with Company's personnel policies. Any disciplinary actions will be noted in the staff member's relevant personnel files.

## Documentation

*Standard: 164.316(b)*

**General Policy:**

These *HIPAA Security Policies and Procedures* are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. Company may change these policies and procedures at any time, provided that such changes are documented and implemented in accordance with this *Documentation Policy and Procedure*.

**Procedures**:

1) Company will maintain these *HIPAA Security Policies and Procedures* in written (which may be electronic) form. If an action, activity or assessment is required by the HIPAA Security Rule or this *Documentation Policy and Procedure* to be documented, Company shall maintain a written (which may be in electronic form) record of the action, activity, or assessment.

2) Company will retain the documentation required by the HIPAA Security Rule and this *Documentation Policy and Procedure* for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

3) Company will make the documentation required by the HIPAA Security Rule and this *Documentation Policy and Procedure* available to those persons responsible for implementing the procedures to which the documentation pertains, such as Company's Security Officer and Privacy Officer. All workforce members will be issued a hard copy of these policies, and receipt is to be recorded.

4) Company will review and update its documentation periodically, as needed, in response to environmental or operational changes affecting the security of the ePHI.

## Administrative Safeguards – Security Management Process

*Standard: 164.308(a)(1)*

**General Policy:**

Company will implement policies and procedures and take reasonable steps to prevent, detect, contain, and correct security violations.

**Procedures:**

Company shall:

1) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Company. This risk analysis will occur annually.
2) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule, which generally requires that Company protect the confidentiality, integrity and availability of ePHI. The security measures Company has adopted to accomplish the foregoing purpose include the following:

   - Only authorized personnel shall install or de-install software or hardware on Company servers.
   - Personnel shall not open attachments sent from untrusted or unknown sources.
   - Maintenance of a firewall to act as a gateway between the Internet and its private network.
   - Installing appropriate software security patches.
   - Prohibit personnel from leaving unsecured electronic media containing ePHI unattended.
   - Use appropriate mechanisms to ensure the transmission security and appropriate access to Company's systems used to store and/or transmit ePHI, including authenticating users with passwords or another appropriate authentication mechanism.
   - Test security measures periodically.

3) Apply appropriate sanctions against its workforce members who fail to comply with these *HIPAA Security Policies and Procedures*.

4) Regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Such review may include periodically performing a technical and nontechnical evaluation of Company's security measures to establish the extent to which such security measures meet the requirements of the HIPAA Security Rule and these *HIPAA Security Policies and Procedures*.

- Such reviews shall be conducted annually and/or when Company has reason to suspect wrongdoing. In conducting these reviews, Company shall examine audit logs for security-significant events including, but not limited to, the following:

    - Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

    - User Accounts – Review of user accounts, including audit logs and access reports, within all systems to ensure users that no longer have a business need for ePHI no longer have such access to the information and/or system.

- The Security Officer shall forward all completed reports, as well as recommended actions to be taken in response to findings, to Company management for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Company's administrative, physical, and technical safeguards.

## Administrative Safeguards – Workforce Security

*Standard: 164.308(a)(3)*

### General Policy:

Company shall ensure that all members of its workforce have appropriate access to ePHI in accordance with the *Information Access Management Policy and Procedure* and will prevent those workforce members who do not have access in accordance with the *Information Access Management Policy and Procedure* from obtaining access to ePHI.

### Procedures:

1) Authorization and/or supervision of workforce members who work with ePHI.

   - Only those individual workforce members that have a business need to view ePHI will have access to ePHI.
   - Company will document all individuals with authorization to access ePHI.

2) Workforce clearance.

   - Conduct background checks and/or check references before hiring a new employee who will have access to ePHI.
   - Grant access to ePHI only to those personnel who need such access to perform their duties.

3) Termination procedures.

   - The Security Officer shall rescind access to ePHI upon an employee’s termination (or the end of a subcontractor’s engagement) from Company.
   - The Security Officer shall ensure that all terminated employees or other workforce members will have their employee accounts disabled.

## Administrative Safeguards – Information Access Management

*Standard: 164.308(a)(4)*

**General Policy:**

Company will implement policies and procedures for authorizing access to ePHI.

**Procedures:**

1) Access authorization.

   - The Security Officer shall grant access to ePHI only to workforce members showing a business need to have such access.
   - ePHI shall be stored only in specific databases and software designated by the Security Officer.

2) Access establishment and modification.

   - The Security Officer will be responsible for overseeing the configuration of Company’s information system to permit access in accordance with the privileges granted under this *Information Access Management Policy and Procedure.*
   - The Security Officer or appropriate Company managers shall periodically review the access privileges established under this *Information Access Management Policy and Procedure* and modify them as necessary.

## Administrative Safeguards – Security Awareness and Training

*Standard: 164.308(a)(5)*

**General Policy:**

Company shall implement a security awareness and training program for all members of its workforce. All workforce members shall receive appropriate training concerning Company's Security Policies and Procedures. Such training shall be provided on an ongoing basis to all new employees who have access to ePHI.

**Procedures:**

1) Provide periodic security updates.

   - The Security Officer shall generate and distribute to all workforce members routine security reminders on an as needed basis.
   - Periodic reminders may address password security, malicious software, incident identification and response, and access control.
   - The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletters, posters, sticky notes, etc.

2) Provide training to address for guarding against, detecting, and reporting malicious software (i.e., viruses) as set forth in the *Security Incident Procedures Policy and Procedures.* Training shall include:

   - Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail;
   - The importance of updating operating system software and how to check a workstation or other device to determine if operating system software is current;
   - Instructions to never download files from unknown or suspicious sources;

3) As technologically feasible, the Security Officer may monitor unauthorized log-in attempts and report discrepancies as set forth in the *Security Incident Procedures Policy and Procedures.*

4) The Security Officer shall provide training to address creating, changing, and safeguarding passwords as set forth in the *Person or Entity Authentication Policy and Procedure.*

5) The Security Officer shall provide annual training for all members of the workforce related to the *Security Incident Procedures Policies and Procedures* and to the security of ePHI in general and will track attendance. The attendance log for each training will be maintained for a minimum of six (6) years.

## Administrative Safeguards – Security Incident Procedures

*Standard: 164.308(a)(6)*

### General Policy:

Company shall regularly review records of information system activity, such as audit logs and access reports, and address security incidents. Responsibility for the security of Company's information system will be vested in the Security Officer.

Company management, in consultation with the Security Officer, shall be responsible for the development, implementation and updating of the policies and procedures required by the HIPAA Security Rule, and other such responsibilities as may be given to the Security Officer under these *HIPAA Security Policies and Procedures* and the HIPAA Security Rule.

### Procedures:

1) Identify and respond to suspected or known security incidents.

   - It is the responsibility of all workforce members to notify the Security Officer of any security incidents.
   - The Security Officer, in consultation with Company management as appropriate, shall respond to any suspected or known security incidents.

2) The Security Officer shall mitigate the harmful effects of security incidents using appropriate technology remedies, such as removing such devices from the network, wiping devices, and consulting with outside vendors as to appropriate solutions.

3) Document security incidents and their outcomes.

   - Workforce members discovering security incidents shall document such security incidents in the Security Incident Report.
   - The Security Officer shall maintain the Security Incident Report.

4) Engage in the following activities in monitoring and responding to security incidents:

   - Reports of irregular or unauthorized activity will be made to the Security Officer. The Security Officer will take or oversee the appropriate actions in response to such reports. Employees are required to immediately report any breach of security of which they become aware.
   - Company management approval is required for resolution of the highest level of security incidents, which are those threatening the system's continued operation.
   - In the event Company's information system is breached, the Security Officer will notify Company management.
   - All security incident reports will be maintained in accordance with *Documentation Policy and Procedure.*

## Security Incident Report

| | | | |
|---|---|---|---|
| **Section 1: Incident Reporter** | | | |
| Name: | | | |
| Title: | | | |
| Email Address: | | | |
| **Section 2: Incident Details** | | | |
| Date and Time of Discovery of Incident: | | Estimated Date and Time Incident Started: | |
| Description of Incident – **Be Specific**: | | | |
| PHI Compromise Suspected? | □ Yes □ No | | |
| Location of Incident: | | | |
| Current Status of Incident: | | | |
| Source or Cause of Incident: | | | |
| Employees, Contractors or Others with Incident Knowledge – **List all known potential witnesses**: | | | |
| Operating System, version, and patch level: | | | |
| Description of Affected Resources: | | | |
| Mitigating Factors: | | | |
| Estimated Technical Impact of Incident: | | | |
| Response Actions Performed: | | | |
| Other Organizations Contacted: | | | |
| Report Augmented By: | | | |
| Additional Comments: | | | |

I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge on the date indicated below. If I obtain any additional information regarding this incident, I agree to provide said supplementary information to the Security Officer. I agree to cooperate fully with all investigators of this incident until the incident is closed.

Incident Reporter's Signature Date

## SECURITY INCIDENT REPORT INSTRUCTIONS

- **Description of the Incident** may include how it was detected, what occurred, who detected it, etc.
- **PHI Compromise Suspected** should be "Yes" if there is any concern by any person contributing to this report that personal health information (PHI) was compromised. "No" should only be indicated if all persons contributing to the report are certain that PHI was not compromised.
- **Location of Incident** may be a campus, building, department, or room. Please be as specific as possible.
- **Current Status of the Incident** may be an ongoing attack, one-time occurrence, resolved issue, etc.
- **Source or Cause of Incident** (if known) may include the computer's location, host name, and/or IP address; user account; etc.
- **Operating System** may include systems like Windows; Mac; Linux; Unix; etc.
- **Affected Resources** may include a network device, a workstation, an application, or specific data and may be described as hardware location, IP address, and host name; a system name, location, and function; a user account; etc.
- **Technical Impact** may include data deleted or compromised, system crashed, application unavailable, nonfunctional workstation, etc.
- **Response Action Performed** may include shutting off the computer, disconnecting the computer from the network, beginning malicious software removal, disabling an affected user account, etc.; documentation should include the action taken and identify who took the action.
- **Organizations Contacted** may include software vendor(s), hardware vendor(s), contracted IT support and others; recorded information should include organization, contact's name, date and time of initial contact, and contact method (phone, email, etc.). Any response from the contacted organizations should be noted in the Additional Comments field.
- **Report Augmented By** should list the contact information of everyone except the initial reporter who provided data for the report.

This Report is based on the guidelines found in Exhibit 3 of NIST SP 800-61 Rev. 1: *Computer Security Incident Handling Guide*.

## Administrative Safeguards – Contingency Plan for Emergencies

*Standard: 164.308(a)(7)*

**General Policy:**
Company shall establish and implement contingency plans for responding to an emergency or other occurrence (for example, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

**Procedures:**

1) Disaster Recovery Plan.

   - Company's Disaster Recovery Plan is attached as Exhibit A.

2) Emergency Mode Operations Plan

   - Company's Emergency Mode Operations Plan is attached as Exhibit B.

3) Data Backup Plan.

   - Company will implement data backup procedures for all Critical Business Processes listed in Exhibit A. Backup procedures should be tested to ensure accuracy.

4) Testing and revision of contingency plans.

   - The Security Officer shall periodically test and revise contingency plans by accessing the backups and ensuring that they are correctly maintaining exact copies of the ePHI.
   - The Security Officer will test and revise contingency plans upon a change in backup vendors or backup methods.

5) Applications and data criticality analysis.

   - The Security Officer will periodically assess the software applications used by Company to determine which applications are needed during an emergency.
   - Currently, the following software applications will be necessary when operating in an emergency mode:
     - Orchid Web Platform (www.orchidsurgical.com)

## Administrative Safeguards – Evaluation

*Standard: 164.308(a)(8)*

**General Policy:**

Company shall perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the HIPAA Security Rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, which establishes the extent to which these *HIPAA Security Policies and Procedures* meet the requirements of the HIPAA Security Rule.

**Procedures:**

1) Evaluation

- The Security Officer will on an annual basis review these *HIPAA Security Policies and Procedures.*
- The Security Officer will review these *HIPAA Security Policies and Procedures* upon any known change to the HIPAA Security Rule or when guidance is issued by HHS.
- The Security Officer will evaluate these *HIPAA Security Policies and Procedures* as necessary to ensure that these policies are up to date with Company's business model.
- The Security Officer will evaluate these *HIPAA Security Policies and Procedures* upon a change in the technology securing the ePHI.

2) Modification

- The Security Officer will modify these *HIPAA Security Policies and Procedures* as necessary based on the evaluations conducted above.
- Company management shall be consulted when making modifications to these *HIPAA Security Policies and Procedures.*
- The Security Officer shall notify workforce members of changes to the *HIPAA Security Policies and Procedures.*

## Administrative Safeguards – HIPAA Subcontractor Agreements

*Standard: 164.308(b), 164.314(a)*

**General Policy:**

Company is a business associate of its covered entity clients and as such may permit a subcontractor to create, receive, maintain or transmit ePHI on its behalf only if it obtains satisfactory assurances, in accordance with the HIPAA Security Rule and the underlying Business Associate Agreement with the applicable covered entity, that the subcontractor will appropriately safeguard the information.

**Procedures:**

1) Form of HIPAA Subcontractor Agreement.

   - Company shall require all subcontractors having access to ePHI to execute a HIPAA Subcontractor Agreement.
   - The HIPAA Subcontractor Agreement shall either be the Company's HIPAA Subcontractor Agreement (template) or shall be an agreement drafted by the subcontractor,
   - All HIPAA Subcontractor Agreements must be in writing.

2) Contents of HIPAA Subcontractor Agreement. The terms of the HIPAA Subcontractor Agreement shall include, but are not limited to, the following:

   - The subcontractor must agree to comply with all applicable requirements of the HIPAA Security Rule.
   - The subcontractor will report to Company any security incident of which it becomes aware that affect ePHI, including breaches of unsecured PHI.

## Physical Safeguards – Facility Access Controls

*Standard: 164.310(a)*

**General Policy:**

Company shall limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

**Procedures:**

1) Contingency operations. When Company has a physical facility, establish and implement, as needed, procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

2) Facility security plan. When Company has a physical facility, company shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

    - Company shall lock its physical office location when the office is not otherwise open.
    - Company shall position computer terminals so that they may not be viewed or accessed by unauthorized persons.

3) Access control and validation procedures, as applicable when Company has a physical facility.

    - Access to Company workspace is limited to Company workforce members and contractors as permitted by Company management.
    - All visitors must be invited by Company workforce members onto the premises.
    - The Security Officer must permit any access to software programs containing ePHI for testing and revision.

4) When Company has a physical facility, the Security Officer shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

## Physical Safeguards – Workstation Use and Security

*Standard: 164.310(b), 164.310(c)*

**General Policy:**

Company shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Furthermore, Company shall implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.

**Procedures:**

1) Workstation Use:
    - Company systems (including network access, systems access, email, voicemail, internet access, and remote access) must be used only for conducting the business of Company. Occasional personal use of the system is permitted, but information, data, and messages that are accessed, processed, shared, retrieved, and stored in these systems will be treated no differently from other Company records. Incidental personal use of Company systems is permissible only if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with staff productivity, (c) does not preempt any business activity, and (d) does not otherwise violate Company policy (i.e. engaging in gambling or viewing adult web site).
    - Workforce members and contractors are required to locate their computers in a manner so that they cannot be easily viewed by visitors.
    - All copyright or other protections must be observed. Hardware and software installed on Company computers and devices must be licensed to Company.
    - The Security Officer or Company management may revoke system privileges for users at any time and as they deem necessary.
    - All workforce members and contractors will report any irregularities found in information or information systems to the Security Officer immediately upon detection.

2) Workstation Security:

    - Workforce members and contractors are required to safeguard all laptops in order to prevent their unauthorized use. This includes not leaving laptops unattended.
    - Workforce members and contractors are required to monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of the data contained in the computer system.
    - Workforce members and contractors are required to safeguard passwords and log-in credentials.

- Workforce members and contractors shall not log onto the system using another's password nor permit another to log on with their password. Workforce members and contractors shall not enter data under another person's password.
- Workforce members and contractors are prohibited from the unauthorized copying, removal, transmission of ePHI via unsecured mediums.

## Physical Safeguards – Device and Media Controls

*Standard: 164.310(d)*

### General Policy:

The receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility shall be governed by this *Device and Media Controls Policy and Procedure.*

### Procedures:

1) Disposal of ePHI

- Company shall securely delete all ePHI when use of the ePHI is no longer necessary, keeping in mind obligations to maintain ePHI and standards of care.
- Company shall take reasonable steps to ensure that ePHI cannot be read or copied from hardware or electronic media prior to its disposal by securely wiping such devices.
- Company shall track the disposal of hardware or electronic media that contained PHI.

2) Storage of PHI

- Staff are not permitted to store ePHI on laptops, smartphones, and other mobile devices.
- Company shall take reasonable steps to ensure that ePHI cannot be read or copied from hardware or electronic media prior to its re-use by securely wiping such devices.

3) Accountability

- Company shall use maintain a record of devices permitted to access ePHI and who the users are on each device.

4) Data backup and storage - see *Administrative Safeguards – Contingency Plan for Emergencies Policy and Procedure* for information on data backup and storage.

## Technical Safeguards – Access Control

*Standard: 164.312(a)*

### General Policy:

Company shall allow access to electronic information systems that maintain ePHI only to those persons or software programs that have been granted access rights as specified in the *Information Access Management Policy and Procedure.*

### Procedures:

1) Each Company workforce member or contractor shall have a unique name and/or number for identifying and tracking user identity.

2) Individuals needing access to ePHI in an emergency must request such access from the Security Officer.

3) Users shall be automatically logged off of the Company system containing ePHI after 60 minutes or once the browser session has ended, unless the system detects active use.

## Technical Safeguards – Audit and Integrity Controls

*Standard: 164.312(b), 164.312(c)*

### General Policy:

Company shall protect ePHI from improper alteration or destruction. Furthermore, Company shall use hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

### Procedures:

Company shall:

1) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain ePHI.

    - Company shall utilize hardware and software audit logs contained in its systems to examine logins and access as needed upon a Security Incident or suspected Security Incident.

2) Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

    - Company shall use access controls, audit logs and perform routine data back-ups to ensure the integrity of ePHI.
    - Upon an incident, compare ePHI to backups to ensure that modifications and deletions have not been made to ePHI in an unauthorized manner.

3) Review reports created from audit logs periodically as required by the *Security Incident Policy and Procedure.*

## Technical Safeguards – Person or Entity Authentication

*Standard: 164.312(d)*

**General Policy:**

Company shall implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

**Procedures:**

Company shall:

1) Verify an individual or entity's identity by requiring the use of passwords as a condition to granting access to User.

   When utilizing passwords for authentication purposes:

   - Users are required to change their passwords every 365 days.
   - Passwords should be at least 8 characters in length with at least 3 of the following characteristics: Upper and lower case alpha characters, numbers, or symbols.
   - Personnel are prohibited from writing their passwords on post-its, notes or any other document that may easily be viewed or found by an unauthorized person.
   - Use of default passwords will be prohibited.

## Technical Safeguards – Transmission Security over an Electronic Communications Network

*Standard: 164.312(e)*

**General Policy:**

Company shall guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

**Procedures:**

Company shall:

1) Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of properly.

   - Use of unsecured e-mail to transmit PHI is prohibited (including usage of personal non-Company owned e-mail). Prior to sending e-mail internally or externally containing PHI Company personnel shall consult the Security Officer for appropriate transmission mediums.
   - The Company personnel shall notify the Security Officer immediately if PHI appears corrupted or incomplete.

2) Encryption and Decryption. Company shall implement and use the following mechanisms to encrypt ePHI whenever deemed appropriate:

   - Laptops and Other Mobile Devices
     - All new laptops with access to ePHI shall deploy full disk encryption.
     - Staff will use the minimum amount of identifying health information when communicating via mobile devices (use of initials, first name only, etc.). Staff will follow the acceptable uses of the Device and Media Use Policy.
   - Servers
     - Servers that store PHI shall be encrypted and be maintained in a physically secure environment to prevent access by unauthorized personnel.
   - Software
     - To the extent that software purchased by Company contains encryption mechanisms which can be deployed, for a reasonable cost, by Company, shall software encryption shall be deployed.

## Exhibit A: Disaster Recovery and Emergency Mode Operations Plan

### Scope/Objective

The objective of this Disaster Recovery and Emergency Mode Operations Plan (Plan) is to develop, test, and document a clear plan to restore any loss of data or system access affecting Company's handling and protection of ePHI in the event of a disaster.

All workforce members must be aware of this Plan and their specific responsibilities. This Plan should be periodically tested to ensure that it addresses the necessary issues and that workforce members understand how to execute it. Lastly, this Plan is to be updated as necessary to reflect changes in business process and information systems.

### Recovery Objectives

In the event of any emergency, Company expects this plan to enable access to ePHI within 12 hours, and enable the delivery of critical services to clients within 48 hours.

### Disaster Recovery and Emergency Mode Operations Coordinator

Ari Wes, MD has been assigned the role of Disaster Recovery and Emergency Mode Operations Coordinator. The Coordinator's primary duties include:

- invoking elements of the Plan as appropriate;
- ensuring workforce members are notified and perform duties as specified in the Plan; and
- maintaining and updating the Plan;

### Key Workforce Contact Information

| Name | Title | Contact Type | Contact Details |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

### External Contact Information (e.g. vendors)

| Provider | Contact Type | Contact Details |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

### Application Priority

- Orchid Web Platform

**Disaster and Emergency Scenarios**

It is important to consider the disruptions to the above equipment and systems in a variety of disaster and emergencies. The following situations are considered:

- Loss of Facility (Likelihood: Low): office and equipment rendered unusable by fire, flood, etc.
- Loss of Workstations (Likelihood: Medium): Office workstation(s) not available for use by workforce members due to hardware/software failure, theft, malware, etc.
- Power Outage (Likelihood: Medium): A sustained loss of electricity to the office
- Loss of Internet Connectivity (Likelihood: Medium): A sustained loss of internet connectivity at the office
- SaaS Failure (Likelihood: Low): A situation in which a web-based service is unable to provide the expected information or data due to a failure of the provider's servers, databases, or network, malicious hacking, etc.

**Recovery Strategy by Disaster Type**

The actions required ensure the security of ePHI and delivery critical services to clients depend upon the type of disaster or emergency. Recovery steps for each ePHI-related and critical patient service are presented below for each disaster type.

- <u>Loss of Workstations</u>

  In the event of office workstation(s) being stolen, failing due to hardware failure or malicious software, or becoming otherwise non-functioning, workforce members would lose access to the cloud-based services used to access ePHI. Correcting this only requires purchasing a standard Windows-based or Apple computer containing a standard browser and Microsoft Office software applications, all of which are available for download.

- <u>Facility Access / Loss of Facility</u>

  When Company has a physical facility, in the event of Company's office being destroyed or inaccessible, workforce member computers may be destroyed, and internet access may be interrupted. Given that all ePHI-related services are cloud-based, restoring workforce access to ePHI requires:

  1. Restoring internet connectivity: This can be achieved by contacting Company's internet service provider (see External Contact Information above). If the internet service provider cannot restore access in a reasonable time period, a wifi "hotspot" can be purchased from any mobile carrier, which will create an immediate internet-connected wifi network in Company's office.
  2. Replacing damaged workstations: Any Windows-based or Apple computer or laptop can replace the office workstation, and with a web browser will enable access to all ePHI.

- <u>Power Outage</u>

  If the office loses power, workstations will also be unusable. To correct this, a standard Windows or Apple laptop can be charged offsite and brought in along with for limited time period. Given that ePHI is stored by cloud-based services, it is not necessary to maintain an uninterrupted power supply (UPS) for each device.

- Loss of Internet Connectivity

  Restoring lost internet connectivity can be achieved by contacting internet service provider. If the internet service provider cannot restore access in a reasonable time period, a wifi “hotspot” can be purchased from any mobile carrier, which will create an immediate internet-connected, secure wifi network in Company’s office.

- SaaS Failure

  Company utilizes cloud-based services for all ePHI services and systems, such as electronic file storage, email, calendar, and address book. Company has signed HIPAA Subcontractor Agreement with each service provider who is a HIPAA Subcontractor. Under such agreements, the service providers represent that they perform robust, secure data backups and have plans and procedures in place to restore data in a reasonable period of time in case of a partial or full system failure. This plan relies on these representations that ePHI would be restored and available to access within a reasonable period of time. Company takes the additional precaution of maintaining a backup copy of all ePHI data on a storage device in its office. Given this, if the electronic file storage service provider suffered a cataclysmic failure and loss of data, Company would have a complete, current copy of all PHI that would be immediately available to any authorized workforce members. Furthermore, a backup of that copy is periodically made and stored offsite in a secure location.

**Workforce Training**

Management will review this Plan with all workforce members at least annually and record such training. Training will include the specific responsibilities assigned to workforce members, and the on-premise location of a hard copy of this plan.

**Media**

The media priorities during a disaster or emergency are to avoid adverse publicity and take advantage of opportunities for positive publicity. All media inquiries should be directed to the Disaster Recovery and Emergency Mode Coordinator.

**Financial Assessment**

The Disaster Recovery and Emergency Mode Coordinator shall prepare an initial assessment of the impact of the disaster or emergency on the financial condition of the organization, including:

- cash position and near-term cash flow
- loss of revenue
- upcoming non-deferrable expenses (e.g., payroll, payroll taxes, insurance premiums)
- borrowing capabilities

**Legal Assessment**

The Disaster Recovery and Emergency Mode Coordinator should consider consulting legal counsel. Depending upon the nature of the emergency, potential issues include:

- legal exposure of the organization
- expected insurance proceeds
- basis for legal action against other parties

### Insurance

The Disaster Recovery and Emergency Mode Coordinator should review the insurance policies in place and contact the necessary parties to identify any actions required to ensure the maximum favorable outcome.  The relevant policy information is presented in the below table:

| Policy Type | Provider | Contact Name | Contact Details | Amount of Coverage | Renewal Date |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

### Plan Documentation Distribution and Storage

All workforce members will be issued a hard copy of this plan, and receipt is to be recorded.  An electronic copy of this plan will be stored securely using a cloud storage provider.