ARK LABORATORY, LLC D/B/A HELIX DIAGNOSTICS ("COMPANY")
HIPAA SECURITY POLICES AND PROCEDURES

DEFINITIONS

Unless otherwise provided, the definitions set forth below apply to all of the HIPAA Security Policies and Procedures reflected herein. Any capitalized terms used and not defined herein shall have the meanings ascribed to them pursuant to HIPAA.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Business Associate means a person or entity who is not a member of Company's workforce and performs or assists in the performance of a function or activity for or on behalf of Company regarding healthcare operations or payment purposes or for any other function or activity involving PHI.

Company means Ark Laboratory, LLC d/b/a Helix Diagnostics.

Company owned means equipment, Workstations, devices, or hardware/software considered the property of Company for purposes of these HIPAA Security Policies and Procedures regardless of whether it is owned, leased, administered or maintained by Company, or is otherwise under the custody and control of Company.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Confidential Information means any information that is the property of Company and may cause financial, reputational or other harm to Company if disclosed to unauthorized persons, either because of legal or business concerns. If there is a question as to whether information is considered confidential, individuals should consult with their supervisor or other superior and may also consult with the Security Official.

Disclosure (or Disclose) means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic Information System means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Electronic Media means electronic storage media on which data is or may be recorded electronically, including, for example devices in computers (i.e. hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disc, optical disc, or digital memory card. It also includes transmission media that is used to exchange

information already in electronic storage media. Transmission media may include the internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

Email means or system for transmitting written messages electronically between terminals linked by telephone lines, cable networks, or other relays.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. For purposes of these policies, encryption must be consistent with the methods described in NIST Special Publication 800-111 which can be found at http://*csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf*.

HIPAA means the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, 45 CFR Parts 160 and 164, as they are amended from time to time.

HIPAA Security Rule means the regulations at 45 CFR Part 160 and Parts A and C of 45 CFR Part 164, which contain the standards for the security of electronic PHI pursuant to HIPAA.

Individually Identifiable Health Information means information, including demographic information collected from an individual that is created or received by the Company and which relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. Information is considered PHI where the information identifies the individual or where there is a reasonable basis to believe the information can be used to identify an individual.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Mobile Devices include, but are not limited to, Personal Digital Assistants (PDAs), notebook computers, Tablet PCs, iPhones, iPads, iPods, Microsoft Pocket PCs, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, and other similar devices**.**

Personal Information means an individual's first name, first initial and last name or any middle name and last name, in combination with any one or more of the following unencrypted data elements: (a) social security number; (b) driver's license number or state identification card number; (c) account number, credit card number, or debit card number,

in combination with any required security code, access code or password that would permit access to an individual's financial account.

Protected Health Information ("PHI") has the same meaning as in 45 CFR 164.103.

Risk Analysis means an assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of electronic PHI held by Company. For purposes of these HIPAA Security Policies and Procedures, risk analysis is synonymous with risk assessment.

Risk Management Plan means the implementation of security measures sufficient to reduce the risks and vulnerabilities to Company's electronic PHI and ensure the Confidentiality, Integrity, and Availability thereof, including protecting against reasonably anticipated threats, hazards, and non-permitted Uses or Disclosures of such information.

Security Breach means the acquisition, access, Use or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of PHI. An impermissible Use or Disclosure of PHI is presumed to be a breach unless the covered entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a Risk Analysis.

Security Incident means the attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

Screen Lock means a password-protected mechanism used to hide data on a visual display while a device continues to operate. Screen locks can be activated manually or automatically.

Screen Timeout means a mechanism that turns off a device display after the device has not been used for a specified time period.

Security Official means the person designated by Company with overall responsibility for Company's compliance with the HIPAA Security Rule. The Security Official is responsible for the development and implementation of the HIPAA Security Policies and Procedure reflected herein. The Security Official may delegate responsibilities or tasks described in these HIPAA Security Policies and Procedures as needed and as appropriate, provided he or she maintains oversight of such delegated responsibilities or tasks.

Unsecured Protected Health Information ("PHI") or Unsecured electronic PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons

through the use of a technology or methodology specified by the Secretary. Essentially, secured PHI is encrypted or has been destroyed beyond the ability to recover (e.g. shredded).

Use (or Uses) means, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User means anyone with authorized access to Company business information systems containing electronic PHI. This includes all Workforce Members, permanent and temporary employees, third-party personnel such as temporaries, contractors, or consultants, and other parties with valid company access accounts.

Workforce Member means staff, employees, or other individuals whose conduct in the performance of work for Company is under the direct control of Company.

Workstation means an electronic computing device such as a laptop, desktop computer or any other device that performs similar functions and stores Electronic Media in its immediate environment.

SECURITY MANAGEMENT – POLICY (1) AND PROCEDURE (1.1)

1. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements regarding its Risk Analysis and Risk Management Plan in accordance with 45 CFR 164.308(a)(1)(ii)(A)-(B), 45 CFR 164.308(a)(8), and 45 CFR 164.312(b).

1.1 **Procedure**:

a. **Risk Analysis**

i. Company and/or its Security Official will:

1. Identify, classify, and maintain an inventory of all of Company's information systems (including Workstations) that maintain or store electronic PHI. Company's inventory will include the type of PHI maintained in the respective information system;
2. Identify Workforce Members whose roles involve using or disclosing electronic PHI, or that have information that is relevant to Company's Risk Analysis;
    a. These Workforce Members will be included in the Risk Analysis process as applicable, or necessary, including, for example, the Privacy Official.
3. Conduct a risk assessment of all its information systems maintaining or storing electronic PHI, which will include:
    a. Identifying and/or classifying their criticality (e.g., severe, high, medium, low, etc.);
    b. Identifying all threats and vulnerabilities thereto;
    c. Reporting (to appropriate Company personnel) the probability that an identified vulnerability may be exploited;
    d. Identifying and reporting (to appropriate Company personnel) the potential impact that a successfully exploited vulnerability would have on such systems;
    e. Analyzing the effectiveness of any controls that have or are planned to be implemented;
    f. Identifying and recommending additional controls, as needed and as necessary, for such systems; and
    g. Documenting all activities involved in the risk assessment process, including the results thereof, and reporting the same to appropriate Company personnel.
4. Make good faith efforts to review and update Company's risk assessment periodically (and no less than once annually) in response to changes in Company's electronic environment (as it relates to electronic PHI), including, but not limited to:

a. An introduction of new information system(s) or application(s);
b. Upgrades to an existing information system(s) or application(s);
c. Retirement or disposal of existing information systems;
d. Physical relocation of an information system(s) or its corresponding assets;
e. Introduction of new lines of business; or
f. Reorganization of Company's management or business structure.

ii. Company and/or its Security Official will report identified risks that present a significant risk to the Availability, Confidentiality or Integrity of Company's electronic PHI to appropriate Company personnel.

iii. Company and/or its Security Official will conduct a Risk Analysis of all Company's Business Associates both prior to engaging the Business Associate and thereafter as needed (e.g., in the event that Business Associate causes a breach of electronic PHI or otherwise violates the Business Associate Agreement).

iv. Company and/or its Security Official will maintain completed risk assessments (including updates thereto) in accordance with Company's HIPAA Privacy Retention of Documentation Policy and Procedure.

b. **Risk Management Plan**

i. Company and/or its Security Official will:

1. Implement a Risk Management Plan for all threats and vulnerabilities identified in Company's Risk Analysis to Company's electronic PHI;
2. Ensure Company's Risk Management Plan:
   a. Corresponds to Company's Risk Analysis;
   b. Is designed to reduce, mitigate, and/or manage identified risks or vulnerabilities to a level determined to be acceptable to Company; and
   c. Includes the adoption of administrative, physical, and/or technical safeguards (or solutions), as deemed appropriate and necessary by Company, in order to minimize and mitigate the risk of the unauthorized Use or Disclosure of Unsecured electronic PHI. Such safeguards may include: Workforce Member training and sanctions (which shall be completed or carried out in accordance with Company's HIPAA Privacy Policies and Procedures), including developing materials and education to support the same, performing periodic audits or evaluations of processes or implemented safeguards in order to assess their effectiveness; and
3. Gather and present information to appropriate Company personnel if a safeguard that the Security Official has deemed to be reasonable and

necessary would require an expenditure of resources that would require Company's approval.

ii. Company will maintain completed Risk Management Plans (including updates thereto) in accordance with its HIPAA Privacy Retention of Documentation Policy and Procedure.

c. **Information System Audits**

i. Company and/or its Security Official will:

1. Determine which reports, information systems, and software programs (containing electronic PHI) are capable of generating information, including, but not limited to audit logs, access reports, and Security Incident tracking reports;
2. Periodically conduct selective, focused audits on information system operations. Such audits may include analysis of audit logs without respect to specific Users in order to assess whether security measures are performing as intended;
3. The Security Official will, whenever technically possible, maintain any reports, logbook, or other information generated by the audits;
4. Ensure Users are notified that their activity is subject to administrative monitoring and that they should have no expectation of privacy;
5. In reviewing network activity, look for "red flags," which may include (but are not limited to):
    a. Account creations/deletions;
    b. High volumes of unsuccessful log-in attempts;
    c. Unusually high internet gateway activity;
    d. Unusually high volumes of database access or file creation, modification, or deletion;
    e. Unusually high access records for specific accounts;
    f. Inappropriate or unauthorized network use by staff members or outsiders;
    g. Virus infestation notices; and
    h. Irregular Workstation behavior, including unusual slowdowns, slow response times, or display errors;
6. The Security Official will periodically review audit logs from various information systems for "red flag" behaviors; and
7. The Security Official will periodically review reports from email monitoring systems in order to track and investigate potential sending of unsecure PHI.

d. **Evaluation**

i. Company and/or the Security Official 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 electronic PHI, that establishes the extent to which Company's HIPAA Security Policies and Procedures meet the requirements of 45 CFR 164, Subpart C.

Effective Date: **JUNE 25, 2021**

WORKFORCE SECURITY – POLICY (2) AND PROCEDURE (2.1)

2. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(3) and 45 CFR 164.312(a)(1).

2.1 **Procedure**:

a. **Access to Information Systems Maintaining or Storing Electronic PHI**

i. The Security Official will be responsible for ensuring that Workforce Members with access to Company's electronic PHI are:

1. Screened in accordance with Company's Policy for Personnel Security, to the extent applicable. Screening will include inquiry as to whether the Workforce Member has ever been disciplined for breaching security at his or her previous employer;
2. Trained in accordance with Company's HIPAA Security Policy (4) and Procedure (4.1) – Security Awareness and Training, Company's HIPAA Privacy Policy (13) and Procedure (13.1) – Workforce Patient HIPAA Education and Training, and Company's Policy for Personnel Security, to the extent applicable, prior to being granted such access;
3. Only provided with such access if and to the extent it is needed for the performance of the Workforce Member's job function and/or responsibilities and that such access is consistent with Company's HIPAA Privacy Policy (6) and Procedure (6.1) – Minimum Necessary; and
4. Only provided with remote (i.e., off-site) access to electronic PHI if reasonable and appropriate and if safeguards are in place that are consistent with these Policies and Procedures (e.g., VPN access that is otherwise consistent with these Policies and Procedures).

ii. The Security Official will be responsible for ensuring that non-Workforce Members with access to Company's electronic PHI (e.g., Business Associates, agents, contractors, etc.):

1. Are only provided with access to Company's electronic PHI to the extent necessary to perform services on Company's behalf and that such access, to the extent it's needed, is commensurate with the services to be performed and consistent with Company's HIPAA Privacy Policy (6) and Procedure (6.1) – Minimum Necessary;
2. Are properly monitored and audited, to the extent necessary, and that any changes in access needs are communicated and implemented;
3. Are trained, to the extent necessary, consistent with paragraph 2.1.a.i.2 above; and

4. Have properly executed necessary privacy, security, confidentiality or other agreements prior to be providing with such access (e.g., Business Associate agreement).

b. **Termination of Access to Information Systems Maintaining or Storing Electronic PHI**

i. In the event that a Workforce Member or non-Workforce Member no longer needs access to Company's electronic PHI (e.g., as a result of termination, resignation, expiration of a services contract, etc.), the Security Official is responsible for:

1. Ensuring that such individual's access to all Company's Information Systems containing electronic PHI is deleted, removed, or disabled as soon as reasonably possible; and
2. Ensuring that such individual's means of accessing any physical location wherein electronic PHI is accessible has been removed or revoked (e.g., access-badges have been returned).

Effective Date: **JUNE 25, 2021**

INFORMATION ACCESS – POLICY (3) AND PROCEDURE (3.1)

3. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(4) and 45 CFR 164.312(a)(1).

3.1 **Procedure**:

a. **Authentication/Authorization**

i. In the event that a Workforce Member needs access to an Electronic Information System, the Security Official is responsible for ensuring that:

1. Each Workforce Member is assigned a unique username for the Electronic Information System to which access is required;
2. Each Workforce Member has an appropriate level of access pursuant to HIPAA Security Policy (2) and Procedure (2.1) – Workforce Security;
3. Each Workforce Member develops a unique password that complies with Company's HIPAA Security Policy (16) and Procedure (16.1) – Username and Password; and
4. Ensuring each Workforce Member's level of access to electronic PHI is based on job function and consistent with Company's HIPAA Privacy Policy (6) and Procedure (6.1) – Minimum Necessary.

ii. The Security Official will maintain a list of Workforce Members with remote access to Company Electronic Information Systems.

iii. The Security Official will maintain an inventory list of registered devices with remote access to Company Electronic Information Systems, including, where possible, serial numbers or other identifying characteristics to differentiate such devices from other similar devices.

iv. The Security Official will ensure that Users do not have access to Company's Electronic Information Systems via the wireless or-cloud based network via personally-owned communication devices.

b. **Workforce Responsibilities Related to Access**

i. All Users with access to Company's Workstations are responsible for:

1. Using reasonable measures to protect electronic PHI and preventing connections to the network by unauthorized individuals, including applying the same precautions to remote access as required for Workstation security (i.e., Workforce and non-Workforce members must treat the remote access locations as though they were on-site at the Company);
2. Not using any personally-owned communication devices to access Company's Electronic Information Systems via the wireless or-cloud based network; and
3. Complying with the access levels and restrictions that apply to their positions.

Effective Date: **JUNE 24, 2021**

SECURITY AWARENESS AND TRAINING – POLICY (4) AND PROCEDURE (4.1)

4. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(5).

4.1 **Procedure:**

a. **Security Training**

i. The Security Official is responsible for:

1. Ensuring all new Workforce Members receive basic HIPAA training within approximately 30 days of their start date with Company;
2. Periodically communicating to applicable Workforce Members HIPAA security and privacy reminders and updates in a form deemed appropriate by the Security Official (e.g., re-training, newsletters, email reminders); and
3. Arranging for or conducting re-training of any Workforce Members that request re-training or that the Security Official determines need re-training.

b. **Protection from Malicious Software**

i. The Security Official and/or Security Official's designee will:

1. Ensure that every Company owned Workstation has appropriate anti-virus software installed or activated to constantly monitor and safeguard the Workstation against malicious software;
2. Update anti-virus software as updates become available; and
3. Prohibit Workforce Members from accessing electronic PHI on any computing devices found to have security vulnerabilities or other software deficiencies until the problems are resolved and cleared by the Security Official.

ii. The Security Official will communicate the following guidelines to all Users and Users will be required to follow the same:

1. Users are not permitted to open any files or macros attached to an email from an unknown, suspicious or untrustworthy source (e.g., unknown senders or organizations). Users are to delete these attachments immediately then empty the deleted items folder;
2. Users are not permitted to download files from unknown or suspicious sources;
3. Users are to avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so. If storage media is shared

between Workstations, anti-virus software should scan the media before allowing its contents to be accessed by the Company owned Workstation. Users should assume that portable storage media are not automatically scanned by each Company owned Workstation; and

4. If system software conflicts with anti-virus software, Users must notify the Security Official.

iii. In addition to the guidelines required under 4.1.b.ii, all Users must adhere to the following guidelines:

1. Users are not permitted to add, remove or download software programs to any Company owned Workstation without first obtaining the permission of the Security Official;
2. Users may install minor system updates as they become available but are not permitted to install major system updates without permission of the Security Official and/or designated IT personnel.
    a. For purposes of this policy, a "minor update" is an update that does not result in a change in the product version (e.g., going from a version 1.1 to 1.2). A "major update" is a comprehensive update that warrants a change in the product code (e.g., going from a version 1.1 to 2.0 or higher).
3. Users are not permitted to open attachments on Company owned Workstations associated with personal e-mail;
4. Users are expected to alert the Security Official if they receive suspicious or unusual e-mail;
5. Users are not permitted to disable anti-virus or similar software installed on any Company owned Workstation;
6. Users must notify the Security Official if they are unable to login to an information system or other application containing electronic PHI or if they encounter anything suspicious during the login process;
7. Any information system or device that is found to have security vulnerabilities or other software deficiencies cannot be used to access electronic PHI until the problems are resolved and the information system or device is cleared by Security Official; and
8. Users with remote access to Company's wireless network may not download or transfer documents or other information containing electronic PHI onto the hard drives or other Electronic Media of non-registered electronic devices.

c. **Log-in Monitoring**

i. The Security Official and/or the Security Official's designee is responsible for:

1. Ensuring that all Company owned Workstations maintain a log of log-in attempts (both successful and unsuccessful);

2. Periodically reviewing login logs for anomalies or upon receipt of login reports, receipt of anomalous incidents; and
3. Reviewing and implementing login monitoring and reporting procedures and safeguards based on the capabilities of each Electronic Information System. Such safeguards may include, for example:
    a. Notification displays upon log-in stating that the system must only be accessed by an authorized Workforce Member;
    b. Removal of any help messages that could assist an unauthorized User; and
    c. Configuring all Company owned Workstations and Mobile Devices with access to Company's electronic PHI and to automatically lock out Users and report to the Security Official a certain number of unsuccessful log-in attempts.

d. **Password Management**

i. The Security Official will be responsible for ensuring that:

1. Workforce Members with access to Company's electronic PHI develop a password to access electronic PHI that complies with Company's HIPAA Security Policy (16) and Procedure (16.1) – Username and Password Username; and
2. Workstations connected to the internet have a Screen Timeout after a certain period of non-use as deemed appropriate by the Security Official.

Effective Date: **JUNE 25, 2021**

SECURITY INCIDENTS – POLICY (5.0) AND PROCEDURE (5.1)

5. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(6).

5.1 **Procedure**

a. **Identification and Reporting of Security Incidents**

i. The Security Official will be responsible for implementing and overseeing Security Incident detection efforts.

ii. Workforce Members will be trained to identify and report Security Incidents to the Security Official. Examples of Security Incidents that must be identified and reported include, without limitation:

1. Passwords that have been lost, stolen, shared, or used by persons other than the User to whom the password was assigned;
2. Introduction of viruses, worms, trojan horses or other malicious software into Company's information systems;
3. Unauthorized access to networks, information systems, or facilities/equipment rooms housing the information systems or devices;
4. Destruction of electronic PHI; and
5. Failed log-in attempts of a suspicious nature.

b. **Documentation of Security Incidents and Response**

i. The Security Official is responsible for documenting all Security Incidents, the results of investigations of Security Incidents, and Company's response and steps taken to mitigate harmful effects of Security Incidents.

1. The Security Official must maintain such documentation in accordance with Company's HIPAA Privacy Retention of Documentation Policy and Procedure unless there is an ongoing investigation or litigation, in which case the Security Official should consult with risk management or legal counsel to determine if the information should be retained for a longer period of time.

c. **Mitigation**

i. If a Security Incident results in an unauthorized Disclosure of Unsecure electronic PHI, the Security Official or the Security Official's designee will be responsible for determining what steps should be taken, if any, to mitigate harmful effects of the Security Breach.

1. The Security Official or the Security Official's designee may consult with others in the field or expert consultants in addressing potential mitigation options and, depending on the severity of the issue, may coordinate with legal counsel with regard to the matter prior to making any final recommendations or taking any actions.

2. All documentation related to mitigation of harmful effects of a Security Breach must be maintained in accordance with Company's HIPAA Privacy Retention of Documentation Policy and Procedure.

d. **Breach Notification**
   i. When a Security Incident involves a successful unauthorized Use or Disclosure of Unsecured PHI, the Security Incident will be treated as a suspected breach and will be handled in accordance with Company's HIPAA Privacy Policy (12) and Procedure (12.1) – Breach Notification, in coordination with Company's Privacy Official and Security Official.

e. **Non-retaliation**
   i. Retaliation against those who report or complain about Security Breaches or Security Incidents is strictly prohibited.

f. **Cybersecurity Incidents**
   i. If Company experiences a cyber-attack or other cyber Security Breach, the Security Official is responsible for:
      1. Executing all applicable steps and/or processes reflected in HIPAA Security Procedure (5.1) and (6.1), to the extent applicable; and
      2. Reporting the crime to law enforcement agencies, reporting the cyber threat indicators to the federal and information sharing and analysis organizations, and reporting the breach in accordance Company's HIPAA Privacy Policy (12) and Procedure (12.1) – Breach Notification.

Effective Date: **JUNE 25, 2021**

CONTINGENCY PLAN – POLICY (6.0) AND PROCEDURE (6.1)

6. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(7)(i).

6.1 **Procedure**

a. **Applications and Data Criticality Analysis**

i. The Security Official is responsible for determining the criticality of electronic PHI. Criticality will be determined on both a long term and a short-term basis.

1. Information is critical on a short-term basis if daily operations could not be continued without this information; and
2. Information is critical on a long-term basis if Company would have liability exposure if the information was permanently lost or lost for a long-term period.

b. **Data Backup and Disaster Recovery Plan**

i. Electronic PHI will be backed up based upon a schedule determined by Company's applicable IT personnel with input from the Security Official.

1. Developed back-up schedules will take into account the criticality of the electronic PHI stored on each information system.

ii. The Security Official is responsible for overseeing the recovery of electronic PHI as set forth in the disaster recovery plan in the event of a disaster impacting Firm's information systems containing electronic PHI, which shall involve the following:

1. The Security Official and his/her designees shall assess the damage to any equipment, hardware, software, and/or databases that contain electronic PHI, determine equipment needs, and initiate any replacement of equipment;
2. The Security Official and his/her designees shall restore programs and lost data, test or otherwise ensure the Integrity of the programs and data and restore communications and networking capabilities, based upon the data criticality analysis;
3. The Security Official and his/her designees shall take delivery and set up new equipment, if needed, and work to restore full communications and networking capabilities; and
4. The Security Official shall update this disaster recovery plan as needed.

c. **Emergency Mode Operation Plan**

i. The Security Official, working with designated IT personnel, will ensure that the electronic PHI (or other data supporting the same) deemed to be most critical to Company's daily operations will be restored first (to the extent that it does not impair the potential for recovery of information that is critical from a long-term perspective).

d. **Testing and Revision Procedures**

i. The Security Official must:

1. Periodically meet IT personnel to ensure that IT personnel understand their roles for restoring data and emergency mode operations as set forth in the disaster recovery plan; and
2. With the assistance of IT personnel, periodically test the disaster recovery plan in a manner that is the least disruptive to daily operations while still allowing the Security Official to discover potential flaws in the plan.

Effective Date: **JUNE 25, 2021**

FACILITY ACCESS CONTROLS – POLICY (7.0) AND PROCEDURE (7.1)

7. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.310(a).

7.1 **Procedure**

a. **Contingency Operations**

i. The Security Official will identify certain individuals who will require access to Company's facilities to minimize losses and restore electronic PHI in the event of a disaster and determine appropriate procedures for gaining access to buildings and/or facilities as necessary to restore data.

b. **Facility Security Plan/Access Control and Validation**

i. The Security Official is responsible for:

1. Maintaining a list of individuals who are permitted access to areas where sensitive electronic PHI is housed and regularly reviewing this list to determine whether the access is appropriate and the list is up to date;
2. Ensuring that Company has the capability of tracking the individuals who have access to PHI located in the building;
3. Maintaining a list of individuals who are permitted special access to the building (e.g., after-hours access) and regularly reviewing this list to determine whether the access is appropriate and the list is up to date; and
4. In the event that an individual with special access or access to sensitive data is terminated or ceases to be affiliated with Company, the Security Official must take steps to ensure that any keys/key cards are obtained prior to termination and work with IT personnel and the building management to determine whether special modifications are required (e.g., locks changed, key codes changed, etc.).

ii. Workforce Members are prohibited from sharing keys/key cards with non-Workforce Members.

iii. The Security Official is responsible for ensuring that the responsibility for the security of Company's premises is delegated appropriately (e.g., landlord, Company's Director of Operations, security personnel, etc.) and will confirm that maintenance records are kept to the extent such records are relevant to the safeguarding of Company's electronic PHI.

c. **Visitor and Non-Workforce Member Control**

i. Workforce Members are required to monitor areas with access to PHI and immediately report to the Security Official or Privacy Official any attempt by a visitor or non-Workforce Member to gain access to PHI (in electronic or paper form).

d. **Maintenance Records**

i. The Security Official will be responsible for overseeing documentation of any maintenance that impacts the physical security of the Company's premises, such as repair or replacement of security cameras, doors, windows, walls or locks.

Effective Date: **JUNE 25, 2021**

WORKSTATION USE AND SECURITY – POLICY (8) AND PROCEDURE (8.1)

8. **Policy:** It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.310(b)-(c).

8.1 **Procedure**

a. **Workstation Safeguards**

i. To safeguard the Integrity and Availability of Company's information systems containing electronic PHI, every person that is authorized to access such systems (i.e., Users) must comply with the following rules:

1. Individuals who access systems with electronic PHI must do so through a unique User ID or username in accordance with Company's HIPAA Security Policy (3) and Procedure (3.1) – Information Access, and must set up a password in accordance with Company's HIPAA Security Policy (16) and Procedure (16.1) – Username and Password;
2. To the extent that a non-Company email account is used to receive electronic PHI from outside emails or via electronic faxes, the Security Official shall establish mechanisms to track which Workforce Members access said email account;
3. Individuals should not open e-mail attachments from individuals or organizations who they do not know;
4. Individuals that have portable Company owned Workstations (e.g., laptops or iPads) that are used to access electronic PHI must comply with Company's HIPAA Security Policy (13) and Procedure (13.1) – Mobile Device Security;
5. Individuals are prohibited from accessing electronic PHI or conducting Company business on personally-owned devices;
6. To the extent reasonable, individuals with Company owned Workstations in areas where visitors and others may see the screen should turn or relocate the screen or use auxiliary equipment such as a screen protector to minimize unauthorized observation of electronic PHI;
7. Individuals should not eat or drink at Company owned Workstations;
8. Unless the Security Official has granted a specific, documented exception, each Company owned Workstation should have a screen saver enabled that will automatically activate and require a password before further use if the Workstation is idle for more than 10 minutes;
9. Individuals are responsible for reporting any Security Incidents of which they become aware to the Security Official in accordance with Company's HIPAA Security Policy (5) and Procedure (5.1) – Security Incidents;

10. Individuals are responsible for password protecting any Company owned Workstation or Mobile Device that is used to access electronic PHI in accordance with Company's HIPAA Security Policy (13) and Procedure (13.1) – Mobile Device Security;
11. Individuals with remote access to Company electronic PHI will not store or download electronic PHI on a personally-owned device and will not leave a Workstation or Mobile Device unattended if they are logged into a Company system;
12. Individuals may not store electronic PHI in cloud storage services such as Dropbox, SkyDrive, or iCloud unless they have received approval from the Security Official in writing in accordance with Company's HIPAA Security Policy (17) and Procedure (17.1) – Cloud Storage;
13. Individuals will report lost or stolen devices that contain electronic PHI to the Security Official immediately (including those devices containing applications that can access electronic PHI); and
14. Individuals will use Workstations for purposes of fulfilling their job responsibilities for Company.

ii. Workstation Use and Security Policies will be included in HIPAA Security Training and will be the topic of security reminders where deemed necessary by the Security Official.

iii. The Security Official will be responsible for observing Workstation use and retraining Workforce Members, as necessary, and Workforce Members are responsible for reporting issues to the Security Official.

Effective Date: **JUNE 25, 2021**

DEVICE AND MEDIA CONTROLS – POLICY (9.0) AND PROCEDURE (9.1)

9. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.310(d).

9.1 **Procedure**

a. **Disposal of Electronic Storage Media, Data Backup and Storage**

i. In the event of disposal of computer hard drives, devices in computers, systems, or removal/transportable media containing electronic PHI, Company is responsible for:

1. Destroying all disks, tapes, CDs, USB thumb drives and other portable media that may contain electronic PHI prior to disposal;
2. When hard drives are disposed of, completely destroying or erasing the hard drives pursuant to the Department of Defense standards and or the most current standards adopted by the National Institute of Standards and Technology;
3. Creating a duplicate copy of any hard drive prior to be disposed of if the Security Official determines it should be retained;
4. In the event that a Business Associate is to perform disposal services on Company's behalf, receiving and maintaining a certificate of destruction that verifies an approved deletion/disposal method(s) was used by the Business Associate (the same will be confirmed prior to engaging the Business Associate's services); and
5. If electronic PHI is stored within information systems that are not owned by Company and/or under its full control (e.g., leased copiers), Company will obtain assurances from the manufacturer of such information system in writing that any electronic PHI remaining on the information is destroyed upon its return to the manufacturer.

b. **Re-use of Media**

i. Thumb drives or other types of removal/transportable storage devices that can be re-used must be encrypted and/or secured in accordance with Company's HIPAA Security Policy (13) and Procedure (13.1) – Mobile Device Security.

c. **Offsite Use of Media**

i. Any portable media that contains electronic PHI, such as USBs, will be encrypted and/or secured in accordance with Company's HIPAA Security Policy (13) and Procedure (13.1) – Mobile Device Security.

ii. Users may not store electronic PHI in cloud storage services such as Dropbox, SkyDrive, or iCloud unless they have received approval from the Security Official.

d. **Accountability**

i. The Security Official is responsible for:

1. Working with IT personnel to maintain an inventory of all Company owned devices such as Workstations and will document the removal of any device;
2. Maintaining a log of any portable media such as USBs that are used to transfer, transport or store electronic PHI and will identify individuals who are responsible for safeguarding that portable media; and
3. Creating retrievable, exact copies of electronic PHI, when needed, before movement or destruction of equipment.

Effective Date: **JUNE 25, 2021**

TECHNICAL ACCESS CONTROL – POLICY (10) AND PROCEDURE (10.1)

10. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.312(a)(2).

10.1 **Procedure**

a. **Unique User Identification Policy**

i. Each Workforce Member who is authorized to access electronic PHI (i.e., Users) will be assigned a unique username for the various systems containing electronic PHI or that allows access to electronic PHI. Assigned usernames may not be changed without the approval and assistance of the Security Official.

b. **Emergency Access Procedure**

i. The Security Official is responsible for responding to requests for temporary access to electronic PHI by individuals that have not been granted access to electronic PHI, but who may occasionally need access or require access during emergencies.

1. To the extent that a request for access is necessary, the Security Official will generate a username and password for limited, temporary use.
2. Whenever granting emergency access, the Security Official must:
    a. Ensure such access is consistent with Company's HIPAA Privacy Policy (6) and Procedure (6.1) – Minimum Necessary;
    b. Whenever possible, grant the lowest level of access possible which will allow Users to perform their job functions; and
    c. If it is not possible to limit access during emergencies, determine whether alternatives exist to protect electronic PHI, such as assigning a different User to a required task who has clearance to access appropriate electronic PHI levels.
3. Consistent with Company's HIPAA Privacy Policies and Procedures and notwithstanding the existence of an emergency situation, any User who accesses or attempts to access electronic PHI beyond their clearance levels will be subject to disciplinary action.

c. **Automatic Logoff**

i. Each Company owned Workstation must have Screen Timeout enabled that will automatically activate and require a password before further use if the Workstation is idle for more than a certain period of time as determined appropriate by the Security Official based upon the environment where the Workstation is being used.

ii. The Security Official is responsible for periodically confirming that the Screen Timeout feature on each Company owned Workstation is active and set to work after the assigned period of inactivity.

iii. Consistent with Company's HIPAA Privacy Policies and Procedures, Users that intentionally disable Screen Timeouts or that lengthen the period of inactivity required to trigger the Screen Timeout without approval from the Security Official will be subject to disciplinary action.

iv. Users who feel that they need to lengthen the period of inactivity before the Screen Timeout activates (due to the nature of their job responsibilities) should request an exception from the Security Official.

v. Users will receive awareness training of the fact that logging into a Company owned Workstation creates an open doorway to Company's systems; accordingly, all Users remain responsible for Company owned Workstations whenever they leave them unattended.

d. **Encryption and Decryption**

i. Company and/or the Security Official will ensure that:

1. All data in motion and at rest will be encrypted where Company has the current resources to encrypt such electronic PHI (e.g., where settings can be changed with regard to existing software); and
2. Where Company requires additional technology or other resources to encrypt electronic PHI, it will analyze options as part of the risk management process and will develop an IT strategy for managing risks.

ii. All Users with access to electronic PHI through their Mobile Devices must comply with Company's HIPAA Security Policy (13) and Procedure (13.1) – Mobile Device Security.

iii. For email communications, all Users must comply with Company's HIPAA Security Policy (12) and Procedure (12.1) – Electronic Mail Containing PHI.

e. **Firewalls**

i. Company and/or the Security Official is responsible for ensuring that:

1. All Electronic Information Systems and applications containing electronic PHI that are accessible outside of Company must have perimeter security and access control with a firewall approved by the Security Official in consultation with IT personnel; and
2. Firewalls must be configured to support the following minimum requirements:

a. Limit network access to only authorized Workforce Members and Users (e.g., Business Associates, agents, contractors, etc.);

b. Limit network access to only legitimate or established connections (an established connection is return traffic in response to an application request submitted from within the secure network);
c. Console and other management ports must be appropriately secured or disabled;
d. Mechanisms must be present to log failed access attempts; and
e. Servers and other devices containing firewalls must be located in a physically secure environment allowing access to only necessary Users.

Effective Date: **JUNE 25, 2021**

INTEGRITY/AUTHENTICATION OF ELECTRONIC PHI – POLICY (11) AND PROCEDURE (11.1)

11. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.312(c).

11.1 **Procedure**

a. Through the risk management process, the Security Official will:
    i. Address which data must be authenticated and evaluate which data authentication methods are available for each system to corroborate that data containing electronic PHI has not been altered or destroyed in an unauthorized manner (e.g., error correcting memory, magnetic disc storage); and
    ii. Make good faith efforts to activate or enable any capabilities that are available on each information system which requires data authentication.

Effective Date: **JUNE 25, 2021**

ELECTRONIC MAIL CONTAINING PHI – POLICY (12) AND PROCEDURE (12.1)

12. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.312. This policy and the procedures set forth herein apply to emails and electronic faxes received and sent via email.

12.1 **Procedure**

a. **Email Communications Containing PHI within Company**

i. Emails containing PHI may only be sent from one helixmdx.com email address to another helixmdx.com email address.

ii. Emails containing PHI should be limited to the minimum necessary to meet the requestor's needs, should be de-identified whenever possible, and should be sent only to individuals who have a need to know the information, in accordance with Company's HIPAA Privacy Policy (6) and Procedure (6.1) – Minimum Necessary.

iii. The sender of any email containing PHI is responsible for ensuring that the recipient's address is within the helixmdx.com email system and the name and email address of the recipient is verified as correct before the message is sent.

iv. Email and email accounts that include, or could potentially include, electronic PHI may not be manually forwarded or auto-forwarded to any unsecure email accounts, including but not limited to personal and commercial email accounts.

v. Distribution lists may not be used for sending email(s) containing PHI.

vi. The following message should be included in all email transmissions containing PHI:

> "This communication may contain information that is legally protected from unauthorized use or disclosure. If you are not the intended recipient, any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this message in error, you should notify the sender immediately by telephone or by return email and delete this email from your computer."

b. **Email Communication Containing PHI with External Entities or Individuals**

i. Emails containing PHI with external entities must be sent one of the following methods:

1. Password protect the document and send as an attachment, then send the password to the document in a separate-email or call the recipient and provide the password verbally;
2. Send via encrypted e-mail; or
3. Send via secure email platform.

c. **Email Monitoring**
    i. No Workforce Members shall have the expectation of privacy in anything they create, receive, maintain or transmit using Company's email system.
    ii. Company reserves the right to periodically access, monitor and disclose the contents of email messages.
    iii. Access and disclosure of individual employee messages may only be done with the approval of the Security Official and/or its legal counsel.

d. **Forwarding Email**
    i. To prevent the unauthorized or inadvertent Disclosure of sensitive information such as PHI, automatic email forwarding, and the potentially inadvertent transmission of sensitive information by all Users is prohibited.

e. **Encryption**
    i. Workforce Members are required to use the encryption services approved by the Security Official to send emails or electronic documents that contain PHI.

Effective Date: **JUNE 25, 2021**

MOBILE DEVICE SECURITY – POLICY (13) AND PROCEDURE (13.1)

13. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.312 and 45 CFR 164.306.

13.1 **Procedure**

a. **Permission for Accessing, Storing, or Using Electronic PHI or Company-Related Confidential Information or Information on Mobile Devices**

i. Electronic PHI and Company-related Confidential Information and/or Personal Information may not be used, stored or accessed on a Mobile Device unless it is necessary for a legitimate business purpose and approval has been obtained from the Security Official.

ii. The Security Official must maintain documentation of Workforce Members granted permission to Use, store or access electronic PHI or Company-related Confidential and/or Personal Information on a Mobile Device.

b. **Encryption**

i. If permission is granted to access, store or Use electronic PHI or Company-related Confidential Information or Personal Information on a Mobile Device, the device must be secured in the following manner:

1. In the case of Company owned devices, IT personnel will encrypt all existing Mobile Devices with an encryption product determined by the Security Official to be the best encryption solution for the device at issue. Devices will be encrypted and secured in order of priority based upon the risk that the device may be used to access, Use, store, or transmit electronic PHI or upon request of Workforce Members who have a need to access, Use, store, or transmit electronic PHI.

ii. If a Mobile Device cannot be encrypted according to these standards, then the device must not be used to access, Use or store electronic PHI or Company-related Confidential Information.

c. **Physical Security**

i. The physical security of Mobile Devices is the responsibility of the User to whom the device has been assigned in the case of Company owned devices. Users must safeguard their Mobile Devices as follows:

1. Whenever possible, all Mobile Devices must be password protected. The password must not be a sequence of numbers, or an address or digits of a telephone number associated with the User. The User must change the password at least once per year;
2. Mobile Devices must be kept with the User whenever possible. Whenever a device is being stored, it must be stored in a secure place, preferably out-of-sight in a locked cabinet or desk drawer.

Mobile Devices should not be left in unlocked vehicles under any circumstances. Mobile Devices should be removed from locked vehicles whenever possible and should always be hidden from view; and

3. Whenever possible, all Mobile Devices should have Screen Lock and Screen Timeout functions enabled.

ii. If a Mobile Device is lost or stolen, the User must immediately report the incident to the Security Official.

iii. All Users with access to Company-related Confidential Information or electronic PHI on Mobile Devices must sign an attestation agreeing to safeguard applicable Mobile Devices as required by this policy, including an attestation that they will follow appropriate procedures for wiping/destroying such devices when no longer in use.

d. **Destruction/Disposal**

i. All Company-related Confidential Information or electronic PHI contained on a Company owned Mobile Device must be "wiped" or securely deleted at the conclusion of the stated purpose for having such information on the Mobile Device, upon termination of employment at Company, or upon termination of affiliation with Company in the event that such Mobile Device stores PHI. The exact methodologies will be dependent on the device as determined by IT personnel and/or the Security Official.

e. **Enforcement**

i. Consistent with Company's HIPAA Privacy Policies and Procedures, non-compliance with this Policy and/or this Procedure may be cause for disciplinary action. Depending on the circumstances, federal or state law may permit civil or criminal litigation and/or restitution, fines, and/or other penalties for actions that would constitute a violation of this Policy or Procedure.

ii. Any individual observing what appears to be a breach of security, violation of this Policy or Procedure, violation of state or federal law, theft, damage, or any action that might place Company resources at risk must immediately report the incident to the Security Official.

Effective Date: **JUNE 25, 2021**

SANCTIONS – POLICY (14) AND PROCEDURE (14.1)

14. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(1)(ii)(C).

14.1 **Procedure**

a. **Workforce Members**
   i. Workforce Members that violate Company's HIPAA Privacy or Security Policies and Procedures be subject to disciplinary action as reflected in Company's HIPAA Privacy Policy (14) and Procedure (14.1) – Sanctions.

b. **Volunteers**
   i. Volunteers who materially violate the Company's HIPAA Privacy or Security Policies, and/or the HIPAA/HITECH regulations will not be permitted to provide further service to Company as a volunteer and may be reported to authorities resulting in legal consequences such as possible prosecution.

c. **Business Associates**
   i. If Company knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under its contract with Company or the HIPAA/HITECH regulations, Company will take reasonable steps to cure the breach or end of the violation, as applicable, and if such steps are unsuccessful or not appropriate, must:
      1. Terminate the contract, if feasible; or
      2. Report the problem to the Secretary of the Department of Health or Human Services or other applicable enforcement agency.

d. **Documentation of Sanctions**
   i. Documentation regarding any sanction imposed for a violation of Company's HIPAA Privacy or Security Policies or HIPAA/HITECH regulations must be retained in accordance with Company's HIPAA Privacy Retention of Documentation Policy and Procedure. Copies of such documentation should be forwarded to the Security Official upon request.
   ii. Documentation of any sanction imposed against a Business Associate relating to a Breach of Company's electronic PHI should in accordance with Company's HIPAA Privacy Policy (15) and Procedure (15.1) – Retention of Documentation.

e. **Retaliation**
   i. Company will not impose sanctions against Workforce Members or non-Workforce Members for:
      1. Engaging in whistleblower activities;

2. Submitting a complaint to the Secretary of the Department of Health and Human Services;
3. Participating in an investigation; or
4. Registering opposition to a violation of the HIPAA Security Rule.

Effective Date: **JUNE 25, 2021**

BUSINESS ASSOCIATES – POLICY (15) AND PROCEDURE (15.1)

15. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(b) and 45 CFR 164.314(a).

15.1 **Procedure**

a. **Disclosure of PHI to Business Associate**

i. All Business Associates of Company will be required to sign a Business Associate Agreement ("BAA") consistent with Company's HIPAA Privacy Policy (10) and Procedure (10.1) – Business Associates and Business Associate Agreements, in order to receive or maintain PHI.

ii. All Business Associates that will access, Use, Disclose, store, or otherwise maintain Company's electronic PHI will agree to:

1. Fully comply with the HIPAA Security Rule;
2. Report to Company any Security Incident affecting Company's electronic PHI of which the Business Associate is aware; and
3. Obtain a downstream BAA with any subcontractor Business Associate engages that will access, Use, Disclose, store, or otherwise maintain Company's electronic PHI.
    a. Company's Business Associates will obtain written assurances from such subcontractors that said subcontractor will adhere to the same or substantially similar restrictions as Business Associate with regard to the subcontractor's access, Use, Disclosure, or storage of Company's electronic PHI.

iii. Workforce Members must confirm that a BAA is in place prior to sending PHI. If there is a question regarding whether an entity or individual is a Business Associate, or should enter into a BAA, the Privacy Official must be contacted for guidance.

b. **Implementation of the Policy**

i. The Privacy Official is responsible for maintaining a current inventory of third parties with whom Company is sharing PHI.

c. **Enforcement of Business Associate Agreements**

i. If Company knows of a pattern of activity of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under its BAA with Company, Company will proceed consistently with Company's HIPAA Privacy Policy (10) and Procedure (10.1) – Business Associates and Business Associate Agreements.

Effective Date: **JUNE 25, 2021**

USERNAME AND PASSWORD – POLICY (16) AND PROCEDURE (16.1)

16. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.308(a)(5)(ii)(d).

16.1 **Procedure**

a. **Usernames and Passwords**
   i. The Security Official is responsible for:
      1. Assigning unique usernames to each individual User that has access to Company's email and electronic PHI;
      2. Establishing minimum standards for passwords for Company electronic devices and systems;
      3. Creating and updating passwords for each individual User; and
      4. Ensuring that, to the extent possible, applications and electronic devices providing access to technical resources enforce the password standards set by the Security Official.
   ii. Workforce Members and other authorized Users must adhere to the standards for all systems and applications that come into contact with Company technical resources.

b. **Systems that Cannot Comply with Minimum Password Standards**
   i. If the minimum standards for passwords cannot be met, the electronic device or system must be protected by other means, such as but not limited to, a dedicated firewall, limited network access or multi-factor authentication.
      1. These mitigating controls will be documented by the Security Official for audit purposes.

c. **Remedies**
   i. Company reserves the right to:
      1. Suspend access to preserve the Confidentiality, Integrity and Availability of the network, systems or information;
      2. Periodically audit passwords for compliance; and
      3. Pursue disciplinary action for non-compliance.

d. **Username Standards**
   i. The current policy for Users is to create a User ID from a combination of the first initial User's first name concatenated with their last name. If the username already exists, Company will add a number.

      Example:
      John Smith
      Username: jsmith@helixmdx.com

e. **Minimum Password Standards**

i. Absent a more secure password selection, the minimum baseline password standard for Users and owners of systems utilized by Company is as follows:

1. Passwords chosen *must* be a minimum of eight (8) characters in length;
2. Contain at least three (3) characters from the following categories:
    a. Uppercase letter (A-Z);
    b. Lowercase letter (a-z);
    c. Digit (0-9); and
    d. Special character ((~`!@#$%^&*()+=_-{}[]\|:;”’?/<>,.);
3. Be private;
4. Passwords *must not* contain a common proper name; the User’s account name; login ID; email address; initials; or parts of the User’s first, middle or last name that exceed two (2) consecutive characters; and
5. Each password must be new and different.

ii. Company will enforce the following system parameters to ensure more secure controls:

1. Maximum password age –180 days;
2. Minimum password age – 1 day (meaning that the User will not be able to change the new password they choose on their own for at least 1 day after the change is made); and
3. Remembered passwords (History) – 10 (meaning that the User will not be able to use the last 10 passwords that they have used prior to the current password).

iii. Passwords for generic accounts must be changed immediately when a User that had access to that account is no longer with Company in the same capacity.

iv. If an account or password is suspected of having been compromised, the incident must be reported to the Security Official and the password(s) must be changed immediately.

v. Password auditing may be performed on a periodic or random basis by IT personnel or the Security Official. If a password is determined to be too weak during one of the audits, the User will be notified and required to change it immediately.

vi. Workforce Members and authorized Users are prohibited from sharing their passwords with anyone except the Security Official.

Effective Date: **JUNE 25, 2021**

CLOUD STORAGE POLICY – POLICY (17) AND PROCEDURE (17.1)

17. **Policy**: It is the policy of Company to effect and maintain compliance with applicable HIPAA/HITECH requirements of 45 CFR 164.306.

    For purpose of this Policy and Procedure, "Cloud Storage" means any service model in which data is maintained, stored, managed or backed up remotely and made available to Users over a network (typically the internet).

17.1 **Procedure**

a. **Use of Cloud Storage Prohibited Without Preapproval**

i. Electronic PHI may not be stored using a Cloud Storage service model unless the service model has been approved in writing in advance of the use by the Security Official.

ii. In evaluating requests to use Cloud Storage, the Security Official will consult with IT personnel to determine:

1. Whether there the Cloud Storage offering can be appropriately configured to secure and/or encrypt electronic PHI; and
2. Whether the requestor has a legitimate need which justifies any risks associated with the Cloud Storage service chosen.

iii. If the Security Official determines there is a legitimate need for Cloud Storage, the Security Official will ensure that there is an appropriate Business Associate Agreement in place in accordance with Company's HIPAA Security Policy (15) and Procedure (15.1) – Business Associates.

Effective Date: **JUNE 25, 2021**