

Zuora, Inc.
HIPAA Privacy and Security
Policies and Procedures

Effective as adopted: July 1, 2025

Table of Contents

I. Introduction.....	5
A. Purpose.....	5
B. No Third Party Rights.....	5
C. Right to Amend Without Notice.....	5
D. Definitions.....	5
II. General Policies.....	9
A. General Responsibilities.....	9
B. Designation of HIPAA Privacy and Security Officers	9
C. HIPAA Workforce Training.....	10
D. Notice of Privacy Practices or Privacy Notice.....	10
E. Disclosure of PHI to Business Associates.....	11
F. Amendment of the Plan Documents.....	13
G. Documentation of Compliance Activity	13
H. Violation Policy and Procedures.....	15
1. Complaints.....	15
2. Notification of Privacy Officer.....	15
3. Sanctions for Violations of Privacy or Security Policy, the Privacy, Security, or Breach Notification Rule, or these policies and procedures.....	15
4. Mitigation of Known Harmful Effects of Use or Disclosure of PHI in Violation of Plan's Privacy Policies and Procedures or the Privacy Rule.....	16
5. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy Rights.....	16
6. Violation Tracking	17
III. Privacy Policies and Procedures	18
A. Limitations on Access to PHI.....	18
B. Handling Individual Rights.....	20
1. Requests for Accounting of Disclosures.....	20
2. Requests for Access (Inspection and Copying)	21
3. Requests for Amendment or Correction	22
4. Requests for Confidential Communications	24
5. Requests for Restrictions on Uses and Disclosures of PHI.....	25
C. Use and Disclosure Policy and Procedures.....	26
1. Disclosures of PHI to the Department of Health and Human Services (HHS).....	26
2. Uses and Disclosures for Purposes of Treatment, Payment, and Health Care Operations	27
3. Disclosures of PHI Pursuant to an Authorization.....	28
4. Disclosures to Personal Representatives.....	30
5. Disclosure of PHI to Business Associates	31
6. Disclosures of PHI for Legal and Public Policy Purposes.....	33
7. Disclosures to Someone Involved in Individual's Care.....	37
8. Disclosures by Whistleblowers	38
9. Complying With the "Minimum-Necessary Standard" for Routine Uses and Disclosures or PHI.....	38
10. Non-Routine Uses and Disclosures of PHI	42
11. Disclosures of De-Identified Information.....	42
D. Physical and Technical Security for PHI in Written, Electronic, and Oral Format.	43

1. PHI Storage and Access.....	43
<i>E. Data Breach Policy and Procedures</i>	<i>47</i>
1. Breach of Information.....	47
IV. Security Policies and Procedures.....	52
<i>A. Security Management Process.....</i>	<i>52</i>
1. Risk Management	52
2. Risk Analysis.....	53
3. Sanction Policy	54
4. System Activity Review	55
<i>B. Workforce Security.....</i>	<i>55</i>
1. Authorization and Supervision	55
2. Workforce Clearance	56
3. Termination Procedures	56
<i>C. Information Access Management.....</i>	<i>57</i>
1. Access Authorization	57
2. Access Establishment and Modification	57
<i>D. Security Awareness and Training.....</i>	<i>58</i>
1. Protection from Malicious Software.....	58
2. Log-in Monitoring	58
3. Security Training, Awareness, and Reminders.....	58
4. Password Management	59
<i>E. Security Incident Procedures.....</i>	<i>60</i>
1. Response and Reporting.....	60
<i>F. Contingency Plan</i>	<i>61</i>
1. Data Backup Plan	61
2. Disaster Recovery Plan	61
3. Emergency Mode Operation.....	62
4. Contingency Plan Testing and Revision Procedures	62
5. Applications and Business Criticality Analysis.....	63
<i>G. Evaluation</i>	<i>63</i>
<i>H. Facility Access Controls.....</i>	<i>64</i>
1. Contingency Operations	64
2. Facility Security Plan	64
3. Access Control and Validation Procedures	64
4. Maintenance Records	65
<i>I. Workstation Use</i>	<i>65</i>
<i>K. Device and Media Control.....</i>	<i>66</i>
1. Disposal.....	66
2. Media Re-Use.....	67
3. Accountability	67
4. Data Backup and Storage.....	67
<i>L. Access Control.....</i>	<i>68</i>
1. Unique User Identification.....	68
2. Encryption and Decryption	68

3. Emergency Access Procedure	69
4. Automatic Lockout.....	69
<i>M. Person or Entity Authentication.....</i>	<i>69</i>
<i>N. Audit Controls (Activity Logs).....</i>	<i>70</i>
<i>O. Transmission Security</i>	<i>70</i>
1. Integrity Controls	70
2. Encryption.....	71

I. Introduction

A. Purpose

Our organization sponsors a group health plan providing benefits which are subject to the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) and its implementing regulations, issued under the Regulations at 45 C.F.R. Parts 160 and 164 (the Security and Privacy Regulations). Those benefits, which form an organized health care arrangement (as that term is used under HIPAA) include the following:

Medical and Prescription Drug
Dental
Vision

Health FSA
Health Reimbursement Arrangement
Employee Assistance Program

These benefits shall collectively be “the Plan.” The Plan and our organization intend to comply fully with the requirements of the HIPAA Security and Privacy Regulations. Thus, our organization and the Plan establish these HIPAA Privacy and Security Policies and Procedures (the Policy).

Certain members of our workforce create, receive, maintain, and/or transmit electronic Protected Health Information (PHI) either (1) on behalf of the Plan itself; or (2) on behalf of our organization, to perform administrative functions for the Plan. This Policy shall provide appropriate guidelines for members of our workforce who have access to PHI.

Employees, volunteers, trainees, and other persons whose work performance is under the direct control of our organization, whether or not they are paid by our organization, are considered part of the our workforce for purposes of this Policy.

B. No Third Party Rights

This Policy does not create any third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or Business Associates). The Policy shall be merely a guideline and shall not be binding upon our organization to the extent this Policy establishes requirements and obligations above and beyond those required by the Security and Privacy Regulations. This Policy does not address requirements under other federal laws or under state laws.

C. Right to Amend Without Notice

We reserve the right to amend or change this Policy at any time (and even retroactively) without notice, except to the extent that notice is required by the Security and Privacy Regulations.

D. Definitions

The terms used, but not otherwise defined in this Policy, shall have the same meaning as those terms are defined in the Security and Privacy Regulations. The following definitions shall specifically apply:

Authorized Personal Representative: An authorized personal representative is any one of the following:

- A parent, guardian, or other person acting in loco parentis for an un-emancipated minor. As a general rule, a parent or guardian is a child’s personal representative except under the following circumstances:
- When the minor is able to lawfully obtain the health care service at issue without the consent of a parent, guardian, or other person acting *in loco parentis*, or

- When the parent, guardian, or other person acting *in loco parentis* consents to confidentiality between the Plan or health care provider and the minor with regard to the health care service at issue. (The plan must honor the agreement of confidentiality.)
- An executor, administrator, or other person who has authority to act on behalf of a deceased individual or that individual's estate; or
- A person who has the authority (under applicable state law) to make health care decisions on behalf of an individual who is unable to make health care decisions for himself or herself. (For example, a spouse may have a health care Power of Attorney for an individual who is incapacitated.)

Business Associate. An entity that:

- Performs or assists in performing a Plan function or activity involving the creation, receipt, maintenance, or transmission of protected health information (PHI) including claims processing or administration, data analysis, underwriting, patient safety activities, etc. for any other function or activity regulated by the Privacy or Security Regulations on behalf of the Plan; or
- Provides, other than in the capacity as a Workforce Member, legal, accounting, actuarial, consulting, data aggregation, management, accreditation, data transmission, or financial services, where the performance of such services involves giving the service provider access to PHI; or
- A subcontractor of a Business Associate, who performs functions for or provides services to a Business Associate on behalf of a covered entity, other than in the capacity of a member of the workforce of a Business Associate, and creates, receives, maintains, stores, or transmits PHI on behalf of a Business Associate.

Covered Component. Information system Covered Components are components of an information system that process, store, or transmit ePHI. Examples include: mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), input/output devices (e.g., scanners, copiers, printers), network components (e.g., firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, sensors), operating systems, virtual machines, middleware, and applications that create, receive, transmit, or maintain ePHI.

Covered Entity. A health plan, health care provider, or health care clearinghouse subject to the Security and Privacy Regulations.

Designated Record Set: "Designated Records Sets" are records containing PHI used to make decisions about individual members such as enrollment, claims adjudication, or case management information maintained by or for a group health plan about an individual.

Device. A unit of physical hardware or equipment that provides one or more computing functions within a computer system. A device is capable of providing input, receiving output, or both.

Disclosure. Disclosure means any release, transfer, provision of access to, or divulging in any other manner of protected health information to any person or entity outside of the Plan.

Disposal. The removal or destruction of ePHI from Electronic Media.

ePHI. Any protected health information that is covered under the Privacy and Security Regulations and is produced, saved, transferred, or received in electronic form.

Electronic Media. Either:

- Electronic storage media (including memory devices in computers such as hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- Transmission media used to exchange information already in electronic storage media (including, but not limited to, the internet, extranet, leased lines, dial-up lines, private networks, and the physical

movement of removable/transportable electronic storage media). Certain transmissions (such as paper, voice via telephone, and facsimile) are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately prior to transmission.

Encryption. A method of scrambling or encoding electronic data to prevent unauthorized access. Only individuals with access to a password or key can decrypt (unscramble) and use the data.

Facility. A building owned or leased by our organization in which the workforce accesses PHI or ePHI.

HIPAA. The Health Insurance Portability and Accountability Act of 1996, as amended.

HIPAA Privacy Rule or Privacy Rule: The Health Insurance Portability and Accountability Act of 1996 (as amended), regulations found at 45 C.F.R. Part 160 and Subparts 164 (as amended), and associated sub-regulatory guidance.

HIPAA Security Rule or Security Rule: The Health Insurance Portability and Accountability Act of 1996 (as amended), regulations found at 45 CFR Part 160 and subsections A and C of Part 164 that apply only to ePHI, requiring covered entities to implement certain administrative, physical, and technical safeguards to protect the electronic information created, received, transmitted, or maintained by the Plan or on behalf of the Plan.

HIPAA Workforce Member. Any individual who is an employee, volunteer, trainee, or other person whose conduct, in the performance of work for our organization, is under the direct control of our organization, whether or not that individual is paid by our organization, and who is authorized to access, use, receive, or maintain PHI.

HITECH Act. The Health Information Technology for Economic and Clinical Health Act contained in Public Law 111-5, as amended.

IT. Refers to the department or team responsible for managing the computers, networks, and other technical areas of our organization.

Minimum Necessary Rule. Under HIPAA, when using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This requirement does not apply to: (i) disclosures to or requests by a health care provider for treatment; (ii) uses or disclosures made to the individual, as specified in the HIPAA Privacy Rule; (iii) uses or disclosures made pursuant to an authorization; (iv) disclosures made to the Secretary of Health and Human Services; (v) uses or disclosures that are required by law, as described in the Privacy Rule; and (vi) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

Portable media. Devices carried or moved with ease, such as smart phones, laptops, flash drives, and other electronic media that can contain ePHI.

Protected Health Information (PHI). Information that:

- identifies an individual or for which there is a reasonable basis to believe the information can be used to identify the individual; and
- is created, maintained, or received by the Plan; and
- relates to:
 - the past, present, or future physical or mental health or condition of an individual;
 - the past, present, or future provision of health care to an individual; or
 - the past, present, or future payment for the provision of health care to an individual.

PHI includes information of persons living or deceased (except that the Privacy and Security Rules do not protect the individually identifiable information of persons who have been deceased for more than 50 years).

Security Incident. A potential HIPAA violation or a breach of confidentiality of PHI, including the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system.

Server. A computer or device on a network that manages network resources.

Server room. The room where all of the servers are housed.

System. Any application or hardware, which creates, maintains, transmits, or stores ePHI.

Transmit. The act of sending a message or data using an electronic medium, including email, electronic (Internet Protocol [IP]) faxing, or other electronic communication.

Use. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within our organization on behalf of the Plan, or by a Business Associate of the Plan.

Workforce Member. Any individual who is an employee, volunteer, trainee, or other person whose conduct, in the performance of work for our organization, is under the direct control of our organization, whether or not that individual is paid by our organization.

II. General Policies

A. General Responsibilities

Under the Privacy Regulations, our organization has certain obligations to perform on behalf of the Plan. Those obligations include the following:

- Designating a HIPAA Privacy Officer;
- Providing HIPAA Workforce Member training;
- Creating physical and technical safeguards to protect PHI;
- Creating internal policies and procedures;
- Creating and distributing a Notice of Information Practices, or a Privacy Notice, and if needed, Breach Notifications;
- Amending health plan documents;
- Obtaining any needed Business Associate Agreements;
- Responding to requests for access, copies, amendments to PHI, restrictions on use of PHI, confidential communication of PHI, and accounting of disclosures of PHI as required by the Privacy Regulations; and
- Documenting compliance activity.

Under the Security Regulations, our organization has certain obligations to perform on behalf of the Plan. Those obligations include the following:

- Designating a Security Officer;
- Appropriately training all HIPAA Workforce Members regarding HIPAA security and privacy laws;
- Identifying all ePHI;
- Performing Security Risk Analyses;
- Documenting and implementing Risk Management measures to address vulnerabilities found from the Risk Analysis;
- Continuing security measures required by the HIPAA Privacy Regulations;
- Implementing a strong and proactive Business Associate management program and amending Business Associate agreements (as necessary);
- Ensuring policy and procedures content are kept current;
- Recommending updates to the Security policy and procedures in response to changes in law, technology, service delivery, or other challenges to the security environment;
- Amending health plan documents; and
- Documenting compliance activity.

Set forth below are the guidelines our organization, on behalf of the Plan, will follow in order to meet these obligations.

B. Designation of HIPAA Privacy and Security Officers

Brittani Campbell shall serve as the Privacy Officer for the Plan. The Privacy Officer's contact information is: bcampbell@zuora.com

Martin Rues shall serve as the Security Officer for the Plan. The Security Officer's contact information is: mrues@zuora.com

C. HIPAA Workforce Training

The Plan will train all HIPAA Workforce Members on its privacy policies and procedures and applicable safeguards for ePHI. The Privacy Officer will develop training schedules and programs so that all HIPAA Workforce Members receive the training necessary and appropriate to permit them to carry out their functions within or on behalf of the Plan. Newly hired HIPAA Workforce Members will be trained within 30 days of joining our organization. Subsequent training will occur promptly after any material change in these policies and procedures for HIPAA Workforce Members affected by the material change and all HIPAA Workforce Members shall undergo periodic refresher training.

HIPAA Workforce Members undergoing training will be required to document their participation in training sessions. Documentation shall include the date of the training, the participant's name, and the participant's signature. The Privacy Officer shall keep a record of training sessions for six years from the date of training.

HIPAA Workforce Members shall also be requested to sign an **EMPLOYEE CONFIDENTIALITY AGREEMENT (FORM A)** affirming their obligation to maintain the confidentiality of all Plan participants' PHI. The Privacy Officer shall maintain copies of the Employee Confidentiality Agreements for six years from the date of execution.

If a HIPAA Workforce Member fails to undergo necessary training within the applicable timeframe, the HIPAA Workforce Member will be reassigned to a position that does not require access to PHI, or appropriate corrective action (up to and including termination) may be taken.

D. Notice of Privacy Practices or Privacy Notice

The Privacy Officer will update and maintain a notice of the Plan's privacy practices that describes:

- The uses and disclosures of PHI that may be made by the Plan for treatment, payment, and health care operations, including at least one example of each;
- A description of each of the other purposes for which the Plan may use or disclose PHI with an individual's written authorization;
- A statement that other types of uses and disclosures not described in the Notice will be made only with an individual's written authorization and a statement that the individual may revoke the authorization at any time; and
- Any more stringent restrictions applicable under state law.
- A statement if the Plan engages in any of the following activities: (1) fundraising using PHI; (2) disclosures to the Plan Sponsor; (3) if engaged in underwriting activities, a statement that the plan will not use genetic information for underwriting purposes except for use with a long-term care policy that is subject to the HIPAA Privacy Regulations;
- An individual's rights under the Privacy Regulations (right to request access on uses and disclosures of PHI, including a statement that Plan is not required to comply except under circumstances specified under the Privacy Rule; right to receive confidential communications, right to inspect and copy PHI held by the plan in a Designated Record Set; right to amend PHI held by Plan; right to an accounting of disclosures; and right to obtain a paper copy of Notice);
- The Plan's obligations (including obligation to provide a Notice of Privacy Practices, to abide by terms of Notice in effect, and in case of a change or amendment to the Notice, a reservation of right to amend the Notice with description of process to provide notice to impacted individuals);
- Our organization's right to access PHI in connection with Plan administrative functions or on behalf of the Plan;
- The name, address, and telephone numbers of the contact person for further information or for filing complaints (including contact information for the Privacy Officer and the Secretary of Health and Human Services); and
- The effective date of the Notice.

The Privacy Notice will be individually delivered to all Plan participants:

- At the time of the participant's enrollment in the Plan;
- Upon request; and
- Within 60 days after a material change to the notice.

The Plan will post the Notice on an applicable website where employee benefits are address. At least every three years, the Plan will provide notice of availability of the Privacy Notice.

E. Disclosure of PHI to Business Associates

The Plan may allow a Business Associate to create, receive, maintain, or transmit PHI on behalf of the Plan if our organization, on behalf of the Plan, obtains satisfactory assurances from the Business Associate that it will employ reasonable and appropriate security measures to protect PHI. The Security Officer, in conjunction with the Privacy Officer, will identify organizations as Business Associates. The Security Officer, in conjunction with the Privacy Officer and legal counsel, will enter into Business Associate Agreements with Business Associates meeting the applicable HIPAA Security Rule requirements.

A Business Associate must provide a written agreement promising that it will:

- Employ administrative, physical, and technical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that the Business Associate creates, receives, maintains, or transmits on behalf of the Plan;
- Ensure that any agents or subcontractors who receive PHI from the Business Associate on behalf of the Plan agree to employ reasonable and appropriate security measures to protect the Plan's PHI;
- Report any security incident that is or may be a violation to the Plan's Security Officer; and
- Agree that our organization, on behalf of the Plan, may terminate the Business Associate agreement if our organization, on behalf of the Plan, or the Plan determines that the Business Associate has violated a material term of the agreement.

The Security Officer and the Privacy Officer will follow standardized Business Associate contract language incorporating the requirements above. The Privacy Officer will also determine what disclosures of PHI are appropriate and consistent with the Plan's permissible Uses and Disclosures Policies and Procedures, including the Minimum Necessary Standard Rule.

If the Plan becomes aware of a pattern of activity or practice of a Business Associate that constitutes a material violation of the Business Associate's obligations under an applicable Business Associate Agreement with the Plan, the Plan shall take steps to cure the breach or end the violation.

[illegible]

F. Amendment of the Plan Documents

Any applicable plan documents for the individual health benefit plans comprising the Plan shall be amended to require our organization to:

- Not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- Ensure that any agents or subcontractors to whom it provides PHI received from the Plan agree to the same restrictions and conditions that apply to our organization;
- Not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan unless authorized to do so pursuant to a written authorization;
- Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- Make PHI available to individuals who are the subject of the PHI, consider their amendments, and, upon request, provide them with an accounting of PHI disclosures as required by law;
- Make our organization's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (HHS) upon request;
- If feasible, return or destroy all PHI received from the Plan that our organization still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible;
- Establish separation between the Plan and our organization in accordance with the requirements of the Privacy Regulations;
- Implement administrative, physical, and technical safeguards that shall reasonably and appropriately protect the integrity, confidentiality, and availability of ePHI that our organization creates, receives, maintains or transmits on behalf of the Plan;
- Ensure that adequate and reasonable safety measures are in place to maintain the separation between the Plan and our organization as described in 45 C.F.R. §164.504(f)(2)(iii);
- Report to the Plan, at agreed upon times and frequency, the total number of unsuccessful, unauthorized attempts to use, access, disclose, modify, or destroy ePHI or to interfere with systems operations containing ePHI;
- Implement administrative, physical, and technical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that our organization creates, receives, maintains, or transmits on behalf of the Plan;
- Ensure that separation between the Plan and our organization (as established through the Plan's Privacy Policy and Procedures) is supported by reasonable and appropriate security measures;
- Ensure that any agents or subcontractors who receive ePHI from our organization on behalf of the Plan agree to employ reasonable and appropriate security measures to protect the Plan's ePHI; and
- Report any Security Incident or possible Security Incident to the Security Officer.

The Plan document will contain a requirement that our organization: (1) certify to the Plan that the Plan documents have been amended to include the above restrictions and that our organization agrees to those restrictions; and (2) provide adequate safeguards against unintentional or intentional disclosure of PHI.

G. Documentation of Compliance Activity

The Plan and our organization shall ensure that Plan documents are appropriately amended and that appropriate Business Associate Agreements are entered into and maintained. The Plan's HIPAA Policies and Procedures shall be documented and maintained for at least six years from the date of creation, or the last effective date, whichever is later. Policies, procedures, forms, plan documents, and business associate agreements will be (1) changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in

regulations); and (2) reviewed at least once every three years. Any changes to policies, procedures, forms, plan documents, and business associate agreements shall be promptly documented.

Policy

The Plan and the Organization shall retain required documents – either in written or electronic form – for six years from either the date the documents were created or the date the documents were last in effect, whichever is later.

Procedure

The Plan shall maintain copies of all of the following items for a period of at least six years from the date the documents were created or were last in effect, whichever is later:

- “Notices of Privacy Practices” issued to participants (copy of Notice shall be maintained in a file by Privacy Officer).
- Records of non-treatment, payment, health care operations disclosures or as set forth in the exceptions listed below (disclosure documents maintained by HIPAA Workforce Members and monitored by Privacy Officer):
 - The date of the disclosure;
 - The name of the entity or person who received the PHI and, if known, the address of such entity or person;
 - A brief description of the PHI disclosed;
 - A brief statement of the purpose of the disclosure; and
 - Any other documentation required under these Use and Disclosure Procedures.
- Completed **PROTECTED HEALTH INFORMATION DISCLOSURE** forms (**FORM C**) shall be maintained in an individual’s Designated Record Set for the applicable six-year period.
- Documentation of disclosures is not required if PHI is disclosed for any of the following:
 - For treatment, payment, or health plan operations;
 - To the individual (or his or her personal representative) about himself or herself;
 - For a facility directory, to next-of-kin, or to those involved in an individual’s care;
 - For national security or intelligence purposes;
 - To correctional institutions or law enforcement officials;
 - Based on an individual authorization;
 - As part of a limited data set; or
 - Incidentally to another permissible use or disclosure.
- Signed individual authorizations (maintained in Designated Record Set by Privacy Officer).
- Business Associate Agreements with Business Associates (maintained by Privacy Officer).
- Plan documents (maintained by Plan Administrator).
- Plan Policies on use and disclosure of PHI (maintained by Privacy Officer).
- Documentation concerning the following individual rights (maintained by the Privacy Officer):
 - The Designated Record Set subject to inspection and copying by an individual;
 - The name and title for the person or office receiving and responding to requests to amend or copy PHI;
- Any written requests for amendment and responses to requests for amendment (including the written denial, statements of disagreement, and the Plan’s rebuttal, if any); and
- Any agreed-upon restrictions on the use and disclosure of an individual’s PHI.
- Designation by Business Associates and Insurance Carriers of who can receive and/or discuss PHI of individuals participating in the Plan (maintained by Privacy Officer).
- Individual complaints and the outcome of the complaints (documentation to be maintained by the Privacy Officer).

- Records (maintained by the Privacy Officer) of any sanctions imposed on any employees, agents, subcontractors, or Business Associates for violations of these policies and procedures or the Privacy Regulations.
- Information on whether the Plan is part of an organized health care arrangement (maintained by the Privacy Officer).
- Workforce Member HIPAA Privacy training materials (maintained by the Privacy Officer).
- Certification of the Plan Sponsor regarding plan amendments and firewalls (maintained by the Privacy Officer).
- Documentation of any other action, activity, or designation (such as the designation of the Privacy Officer) required to be documented by the Privacy Regulations.
- Documentation may be maintained or created in written or electronic form.

H. Violation Policy and Procedures

1. Complaints

The Privacy Officer will be the Plan's contact person for receiving complaints about the Plan's compliance with the Breach Notification Rule, the Plan's Privacy policies and procedures, and the Plan's compliance with the Privacy Rule.

Individuals will use the following process to lodge complaints about the Plan's privacy procedures. Individuals making a written complaint should use the Plan's **COMPLAINT FORM (FORM D)**, but are not required to do so. Oral complaints may be made directly to the Privacy Officer. The Privacy Officer shall conduct an investigation into all complaints and shall make findings and recommend any necessary actions. The Privacy Officer's findings and recommendations should be in writing. A **COMPLAINT REVIEW (FORM E)** form shall be completed in connection with each complaint received. Complaints and documents reflecting the disposition of the complaints shall be retained for six years.

A copy of the complaint procedure shall be provided to any individual upon request. Individuals shall be notified of where to send complaints in the Privacy Notice and applicable forms.

There will be no retaliation, reprisal, or intimidation against anyone for reporting a violation of this Policy or the Privacy Regulations, or for cooperating with an investigation of a complaint under this Policy. The Plan's policy is to investigate each complaint promptly and to keep complaints and the result of any investigation confidential to the fullest extent practicable.

2. Notification of Privacy Officer

Any Workforce Member who believes that a violation of this Policy has occurred is required to contact the Privacy Officer immediately. In a confidential manner, the Privacy Officer will investigate the facts and circumstances of the alleged violations and determine an appropriate course of action.

3. Sanctions for Violations of Privacy or Security Policy, the Privacy, Security, or Breach Notification Rule, or these policies and procedures

If the Privacy Officer or Security Officer determines that a violation of the Plan's Privacy or Security Policies, the Privacy, Security, or Breach Notification Rules, or these policies and procedures has occurred, all involved parties (such as the individual whose PHI was improperly disclosed or used, the Business Associate or insurance carrier, and any other Organization Workforce Member) will be notified in a timely manner. The Privacy Officer and/or Security Officer will conduct an investigation into the alleged violation in a timely manner. If a violation has occurred, resolution of such violation will seek to restore the level of privacy and security that is required under this Policy. Any deficiency in the Plan's

Privacy or Security Policy, Breach Notification compliance, or related procedures that contributed to the violation will be corrected. If monetary damages are found to be due, then this issue will be settled by the Privacy Officer or the Employer's legal counsel under the laws of the state in which the individual whose PHI was improperly used or disclosed resides.

The workforce member(s) responsible for the violation will be dealt with according to standard Organization disciplinary practices. The disciplinary action will depend upon the severity and/or frequency of the violation and whether the violation was blatant. Disciplinary action may range from, but is not limited to, a verbal warning, written warning, and probation, up to and including termination of employment.

In investigating complaints under this policy, the Organization may impose discipline for inappropriate conduct without regard to whether the conduct constitutes a violation of the law and even if that conduct does not rise to the level of violation of this policy. Appropriate parties will be advised of the outcome of an investigation, although not necessarily all details of the actions the Organization and the Plan have taken to maintain the provisions of this Policy.

Sanctions for using or disclosing PHI in violation of this Policy will be imposed, up to and including termination. Individuals who inadvertently use or disclose PHI will be subject to a verbal or written warning. Individuals who blatantly and purposefully use or disclose PHI without regard for this Policy will be subject to having their employment terminated. The Privacy Officer shall document all sanctions and retain applicable records for six years.

4. Mitigation of Known Harmful Effects of Use or Disclosure of PHI in Violation of Plan's Privacy Policies and Procedures or the Privacy Rule

The Organization and the Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth in these Policies or the Privacy or Security Rule. As a result, if a Workforce Member becomes aware of a use or disclosure of PHI, either by a HIPAA Workforce Member or a Business Associate or another outside entity that is not in compliance with this Policy or the Privacy Rule, the Workforce Member should immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the individual can be taken.

The Privacy Officer and/or Security Officer shall act to stop the violation as soon as possible. Necessary steps may include, but not be limited to, suspending access privileges to PHI.

5. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy Rights

No Workforce Member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Regulations, in good faith. However, if the Workforce Member reporting the violation is also the source of the violation, appropriate sanctions may be asserted against that Workforce Member.

No individual shall be required to waive his or her privacy rights under the Privacy Regulations or rights under the Breach Notification Rule as a condition of treatment, payment, enrollment in the Plan, or eligibility for benefits.

If an individual believes that any Workforce Member has engaged in intimidation, threats, coercion, discrimination against, or any other retaliatory act against that individual for exercising rights, filing a complaint, participating in an investigation, or opposing any improper practice under the Privacy Rules, in good faith, the individual should file a complaint with the Privacy Officer.

6. Violation Tracking

The Privacy Officer will track all reported incidents of potential violation under this Policy whether or not a reported incident is ultimately found to be an actual violation. Tracking includes maintaining the relevant facts of a reported incident and the final determination or resolution.

III. Privacy Policies and Procedures

A. Limitations on Access to PHI

Access to Plan members' PHI shall be limited to the HIPAA Workforce Members identified on the **HIPAA WORKFORCE MEMBER DESIGNATION** (see next page).

The HIPAA Workforce Members identified on the **HIPAA WORKFORCE MEMBER DESIGNATION** may use and disclose PHI on behalf of the Plan. HIPAA Workforce Members may not disclose PHI to Workforce Members (other than HIPAA Workforce Members) unless an authorization is in place or the disclosure otherwise is in compliance with our Privacy Policies and the Privacy Regulations.

Each HIPAA Workforce Member's access to PHI shall be limited to the PHI necessary for that HIPAA Workforce Member to carry out his or her job duties. The Privacy and Security Officers will work with each HIPAA Workforce Member's supervisor or manager to determine the appropriate access for each HIPAA Workforce Member in connection with the individual's job title and job description. Each HIPAA Workforce Member's access level will be documented. (Use **FORM F - SECURITY ACCESS WORKSHEET**.)

HIPAA WORKFORCE MEMBER DESIGNATION

Access to Health Plan members' PHI shall be limited to the following HIPAA Workforce Members:

[illegible]

B. Handling Individual Rights

1. Requests for Accounting of Disclosures

Policy

PHI must be disclosed to an individual, who is the subject of PHI, seeking access to his or her own PHI or requesting an accounting of certain PHI disclosures.

Procedure

When an individual requests disclosure of his or her own PHI a request for an accounting of certain disclosures, the following steps should be followed:

- Verify the identity of the individual (or parent or personal representative).
- If the individual's identity and authority is known, no further documentation is necessary.
- If the individual's identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person's relationship with the child and confirm the child's age. Verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Check with the Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual's PHI, the following steps should be followed:
 - Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
 - Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.
- Verify that the identification matches the identity of the individual requesting access to the PHI.
- Contact the Privacy Officer if any doubts arise as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI.
- Make a copy of the identification provided by the individual and file it with the individual's Designated Record Set.
- Request that the individual complete an **Individual Request for Accounting of Disclosures of Protected Health Information (FORM G)**.
- Forward completed Form to the Privacy Officer for retention and any further necessary action.

If the individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, prepare a notice to the individual informing him or her that a fee for processing will be charged and providing the individual with a chance to withdraw the request. The Privacy Officer shall collect any processing fees. All necessary fees must be delivered to the Privacy Officer prior to the provision of additional accountings in the 12-month period.

- Respond to the request within 60 days by providing the accounting (as described in more detail below), or informing the individual that there have been no disclosures that must be included in an accounting. (Use **FORM C - Protected Health Information Disclosure**.) Original disclosure forms should be maintained in the individual's Designated Record Set.
- If the accounting cannot be provided within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Plan will respond.
- The accounting must include disclosures (but not uses) of the requesting individual's PHI made by Plan and any of its Business Associates during the period requested by the individual up to six years prior to the request. The accounting does not have to include disclosures made:
 - To carry out treatment, payment and health care operations;*
 - To the individual about his or her own PHI;
 - Incident to an otherwise permitted use or disclosure;
 - Pursuant to an individual authorization;
 - For specific national security or intelligence purposes;
 - To correctional institutions or law enforcement when the disclosure was permitted without an authorization; and
 - As part of a limited data set.
- Retain all appropriate documents in written or electronic format for the applicable six-year period.

* Except for disclosures made through an Electronic Health Record.

2. Requests for Access (Inspection and Copying)

Policy

The Plan will comply with a written request for an individual's right to inspect and obtain copies of the PHI that the Plan (or its Business Associates) maintains in a "Designated Record Set."

The Plan and our organization will not disclose PHI to family and friends of an individual except as required or permitted by the Privacy Regulations.

Procedure

Individuals seeking to inspect and copy their own PHI must complete a request form. (See **FORM H - INDIVIDUAL REQUEST TO INSPECT AND/OR COPY PROTECTED HEALTH INFORMATION**). HIPAA Workforce Members shall not create a request to inspect PHI form on behalf of plan members or other employees.

- Verify the identity of the individual (or parent or personal representative).
- If the individual's identity and authority is known, no further documentation is necessary.
- If the individual's identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person's relationship with the child and confirm the child's age. Verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual's PHI, the following steps should be followed:

- Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
- Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.

After verifying the identity of the requesting individual or obtaining the necessary authorization, take the following steps:

- Review the request to determine if the PHI requested is in the individual's Designated Record Set. See the Privacy Officer if it appears that the requested information is not in the individual's Designated Record Set. Only the Privacy Officer may deny a Request to Inspect Protected Health Information.
- Respond to the request by providing the information for inspection or copying or denying the request in writing within 30 days. Use the appropriate response form. (Use **FORM I - Response to Individual Request to Inspect And/or Copy Protected Health Information.**) All responses must be in writing. A copy of the request and the response shall be maintained in the individual's HIPAA file for the appropriate six-year period.
- If the requested PHI cannot be presented for inspection and copying within the 30-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 30-day period. The written notice must provide the reasons for the extension and the date by which the Plan will respond. (Use **FORM I - Response to Individual Request to Inspect And/or Copy Protected Health Information.**)
- If no grounds exist to deny a request to inspect and copy, provide the information requested in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
- If PHI is to be delivered electronically, verify the email address before sending the PHI to the intended recipient. This may be accomplished by sending a request for a confirmation to the intended recipient.
- If the Plan does not maintain the PHI for which access is requested, and the Plan knows where the requested PHI is held, the Plan will inform the individual where the PHI is held.
- Retain all appropriate documents in written or electronic format for the applicable six-year period.

3. Requests for Amendment or Correction

Policy

The Plan will comply with individuals' right to request that their PHI held by the Plan in the individual's Designated Record Set be amended or corrected. The Plan will consider written requests for amendment or correction.

Procedure

Upon receiving a request for amendment or correction of PHI held in a Designated Record Set from an individual (or a minor's parent or an individual's personal representative), take the following steps:

- Verify the identity of the individual (or parent or personal representative).
- If the individual's identity and authority is known, no further documentation is necessary.

- If the individual's identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person's relationship with the child and confirm the child's age. Verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual's PHI, the following steps should be followed:
 - Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
 - Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.
- Obtain a copy of documentation establishing the personal representative's authority (e.g., health care Power of Attorney), if applicable, and file in the individual's Designated Record Set.
- Request that the individual complete **INDIVIDUAL REQUEST TO AMEND OR CORRECT A RECORD (FORM J)**.
- Review the request to determine if the request for amendment or correction should be denied. ***No request for amendment or correction may be denied without approval from the Privacy Officer.***
- When an amendment is accepted, make the change in the Designated Record Set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.
- Respond to the request within 60 days by informing the individual in writing, using the **RESPONSE TO INDIVIDUAL REQUEST TO CORRECT OR AMEND A RECORD (FORM K)** that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period, stating the reasons for the extension and the date by which the Plan will respond.
- If the request is denied, provide the individual with a **STATEMENT OF DISAGREEMENT WITH RESPONSE TO REQUEST TO AMEND OR CORRECT A RECORD (FORM L)**.
- If, following the denial, the individual files a statement of disagreement, include the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement; and the Plan's rebuttal/response to such statement of disagreement, if any, with any subsequent disclosure of the record to which the request for amendment relates.
- Retain all appropriate documents in written or electronic format for the applicable six-year period.

4. Requests for Confidential Communications

Policy

The Plan shall accommodate written requests for alternative or confidential communications. However, the Plan shall accommodate such a request **ONLY** if the individual clearly provides information that the disclosure of all or part of that information could endanger the individual. The Privacy Officer has responsibility for administering requests for confidential communications.

Procedure

Upon receiving a written request – using the Plan’s form (**INDIVIDUAL REQUEST FOR CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION (FORM M)**) – from an individual (or a minor’s parent or an individual’s personal representative) to receive communications of PHI by alternative means or at alternative locations, take the following steps:

- Verify the identity of the individual (or parent or personal representative).
- If the individual’s identity and authority is known, no further documentation is necessary.
- If the individual’s identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver’s license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person’s relationship with the child and confirm the child’s age. Verification may take the form of confirming enrollment of the child in the parent’s plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual’s PHI, the following steps should be followed:
 - Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
 - Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual’s Designated Record Set.
- Determine whether the request contains a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.
- Determine whether the request provides for an alternative means of communication (e.g., alternate telephone number) or an alternate location for communication of PHI (e.g., an alternate address).
- Honor requests that include a clear statement that disclosure of the information would endanger the individual.
- Provide a written response (use **FORM N - RESPONSE TO INDIVIDUAL REQUEST FOR CONFIDENTIAL COMMUNICATION OF PROTECTED HEALTH INFORMATION**) unless a written response would be inappropriate. If a written response is inappropriate, contact the individual in person or by telephone.
- If a request will not be accommodated, contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- Retain all appropriate documents in written or electronic format for the applicable six-year period.

5. Requests for Restrictions on Uses and Disclosures of PHI

Policy

An individual may request restrictions on the use and disclosure of the individual's PHI: (1) to carry out the Plan's treatment, payment, or health care operations; (2) to family members, other relatives, close personal friends, or other persons involved in the individual's care without the individual present; (3) for disaster relief purposes; or (4) when the individual is deceased. It is the Plan's policy to attempt to honor such requests if, in the sole discretion of the Plan, the requests are reasonable, except as noted below. **All requests for restrictions must be in writing and approved by the Privacy Officer.**

Procedure

Upon receiving a written request from an individual (or a minor's parent or an individual's personal representative) to restrict access to an individual's PHI, the HIPAA Workforce Member must take the following steps:

- Verify the identity of the individual (or parent or personal representative).
- If the individual's identity and authority is known, no further documentation is necessary.
- If the individual's identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person's relationship with the child and confirm the child's age. Verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual's PHI, the following steps should be followed:
 - Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
 - Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.
- Request that the individual provide a written request. Provide **FORM O - Individual Request for Restrictions on Use or Disclosure of Protected Health Information**.
- Honor reasonable requests that restrict PHI use or disclosure for purposes of treatment, payment, or health care operations. Take steps to honor requests to restrict information given to persons involved in the individual's care.
- Provide a written response to the individual. Use **FORM P - Response to Individual Request for Restrictions on Use or Disclosure of Protected Health Information**. If a written response is inappropriate, contact the individual in person or by telephone.
- If a request will not be accommodated, contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.
- All requests for restrictions on use or disclosure of PHI that are approved must be tracked by the Privacy Officer or the Privacy Officer's designated staff member.

- Notify all Business Associates that may have access to the individual's PHI of any agreed-to restrictions by the Privacy Officer or the Privacy Officer's designated staff member via facsimile, email, or first-class mail.
- The Plan will terminate its agreement to honor a restriction only under the following circumstances:
- The individual agrees to or requests that the restriction terminate (the agreement must be in writing, or if the agreement is oral, the agreement must otherwise be documented);
- An emergency arises; or
- The Plan unilaterally terminates its agreement on a prospective basis and notifies the individual in writing of the termination (except the Plan may not unilaterally terminate any agreement to restrict disclosure of PHI for payment or healthcare operations where the individual has paid the health care provider in full).
- Retain all appropriate documents in written or electronic format for the applicable six-year period.

The Plan shall consider, but is not required to agree to any requested restrictions. If the Plan does agree to the restriction, it will comply with the restriction unless the information is needed to provide emergency treatment to the individual. The Plan will comply with an individual's request if: (1) the disclosure is to a health plan for purposes of payment or health care operations (not for purposes of treatment) and is not otherwise required by law, and (2) the PHI pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full.

C. Use and Disclosure Policy and Procedures

1. Disclosures of PHI to the Department of Health and Human Services (HHS)

Policy

PHI must be disclosed to the Department of Health and Human Services (HHS) when required by HHS to determine the Health Plan's compliance with the Privacy Regulations. Such a disclosure is only required to enforce the Privacy Regulations, and not for other reasons (e.g., coordinating benefits under the Medicare Secondary Payer laws).

Procedure

Upon receiving a request from a HHS official for disclosure of PHI, take the following steps to verify the public official's identity and authority:

- If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status.
- Make a copy of the identification provided and file it with the individual's Designated Record Set (if the information relates to an individual's Designated Record Set).
- If the request is in writing, verify that the request is on the appropriate government letterhead.
- If the request is by a person purporting to act on behalf of a public official. Request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Officer.
- Obtain approval for the disclosure from the Privacy Officer.
- Document the disclosure using the **Protected Health Information Disclosure (FORM C)**.
- Document disclosures in written or electronic form.

- Retain all appropriate documents for the applicable six-year period.

If a HIPAA Workforce Member receives a subpoena or a similar request from a government agency, such as HHS, refer to the Privacy Officer for the disclosure of PHI.

2. Uses and Disclosures for Purposes of Treatment, Payment, and Health Care Operations

Policy

PHI may be disclosed for the Plan's own treatment, payment, and health care operations purposes, and PHI may be disclosed to another covered entity for the payment purposes or certain health care operations of that covered entity.

Treatment. Treatment activities include the provision, coordination, or management of health care and related services by one or more health care providers, including coordination of care by a provider with a third party, consultations between providers, and referrals to other providers. For example, the plan may engage in disease management or may obtain the assistance of a third-party vendor to assist with disease management.

Payment. Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits under the Plan, or to obtain or provide reimbursement for health care. Such activities must relate to the individual to whom health care is provided, not violate the prohibition against using genetic information in violation of the Genetic Information Nondiscrimination Act, and include (but will not be limited to):

- Determination of eligibility for reimbursement of claims;
- Determination of coverage;
- Determination of cost sharing amounts;
- Collection of premiums;
- Coordination of benefits;
- Adjudication of health benefit claims (e.g., claim administration);
- Subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee status and demographic characteristics;
- Billing, collection activities, and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to customer inquiries about payments;
- Obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing;
- Review of health care services with respect to medical necessity, or reviews of appropriateness of care or justification of charges;
- Utilization review activities, including pre-certification of services, and concurrent or retrospective review of services; and
- Disclosure to consumer reporting agencies related to the collection of premiums or reimbursement (the following PHI may be disclosed for payment purposes: name and address, date of birth, Social Security number, payment history, account number and name and address of the provider and/or health plan).

Health Care Operations. Health care operations mean any of the following activities to the extent that they are related to Plan administration or other Covered Functions:

- Conducting quality assessment and improvement activities;
- Reviewing health plan performance;

- Underwriting and premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and securing a contract for reinsurance of risk relating to claims for health care (including stop loss insurance and excess of loss insurance) provided that the requirements of the Privacy Regulations are met, if applicable, and no genetic information shall be used for purposes of underwriting except for use with any applicable long-term care policy;
- Conducting or arranging for medical review, legal services and auditing functions, including, but not limited to, fraud and abuse detection and compliance activities;
- Patient safety activities;
- Business planning and development; and
- Business management and general administrative activities of the Plan, including, but not limited to, customer services, resolving internal grievances, or the sale, transfer, merger, or consolidation of all or part of the Plan with another covered entity and due diligence related to such activity.

Payment or Health Care Operations of another Covered Entity. PHI may be disclosed to another covered entity for purposes of the other covered entity's payment purposes, such as, for coordination of benefits or quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Procedure

(a) Uses and Disclosures for Plan's Own Treatment Activities, Payment Activities, or Health Care Operations.

The Plan may use and disclose an individual's PHI to perform the Plan's own treatment activities, payment activities or health care operations. Disclosures must:

- Comply with the Minimum Necessary Standard Rule (if the disclosure is not recurring, the disclosure must be approved by the Privacy Officer); and
- Applicable documents must be retained in written or electronic form for a period of six years.

(b) Disclosures for Another Covered Entity's Payment Activities or Certain Health Care Operations

The Plan may disclose an individual's PHI to another covered entity to perform the other entity's payment activities. PHI may also be disclosed for purposes of another covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the individual, who is the subject of the PHI, and the PHI requested pertains to that relationship. Disclosures must:

- Comply with the Minimum Necessary Standard Rule (if the disclosure is not recurring, the disclosure must be approved by the Privacy Officer); and
- Applicable documents must be retained in written or electronic form for a period of six years.

3. Disclosures of PHI Pursuant to an Authorization

Policy

PHI may be disclosed for any purpose if an authorization that satisfies all of the Privacy Regulations' requirements for a valid authorization is provided by the individual who is the subject of the PHI (or his or her designated personal representative or legal guardian) (See Form "Q" for designation of personal representative). Any use or disclosure of PHI made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

The Organization and the Plan have an approved **AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION (FORM Q)**, which should be used whenever possible. The **AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION** may be revoked at any time by an individual. (See **REVOCATION OF AUTHORIZATION (FORM R)**). Both authorizations and revocations shall be retained for the applicable six-year period.

Unless the individual, who is the subject of the PHI (or his or her designated personal representative or legal guardian), provides an authorization to use or disclose PHI for non-health plan purposes (as discussed in “Disclosures Pursuant to an Authorization” below) or the use is otherwise permissible pursuant to HIPAA, PHI may not be used or disclosed for the payment or operations of the Organization’s “non-health” benefits as defined by HIPAA (e.g., disability, workers’ compensation, life insurance, etc.).

Procedure

(a) Disclosures pursuant to an authorization

If disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Verify the identity of the individual (or parent or personal representative).
- If the individual’s identity and authority is known, no further documentation is necessary.
- If the individual’s identity and authority is not known, seek verification through one of the following:
 - Signature on a written request with a copy of a government issued or Company issued photo identification; or
 - Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver’s license number of the individual who is the subject of the PHI.
- When a parent requests access to the PHI of his or her minor child, take the following steps:
 - Verify the person’s relationship with the child and confirm the child’s age. Verification may take the form of confirming enrollment of the child in the parent’s plan as a dependent. Check with Privacy Officer to obtain information about relevant state law.
- When a personal representative requests access to an individual’s PHI, the following steps should be followed:
 - Request and obtain a copy of appropriate documentation such as a valid health care Power of Attorney, or a document permissible under applicable state law. If there are any questions, seek review by the Privacy Officer. Also, if the person claiming to be a personal representative relies upon a document permitted under applicable state law, seek review by the Privacy Officer.
 - Appropriate documentation may include one of the following:
 - Guardianship documents;
 - Power of Attorney (for health care decisions);
 - Authorization form naming personal representative; or
 - Other documentation showing authority under applicable state law to act as a personal representative.
- Make a copy of the documentation provided and file it with the individual’s Designated Record Set.
- Verify that the authorization form is valid. Valid authorization forms are those that:
 - Are properly signed and dated by the individual or the individual’s representative;
 - Are not expired or revoked [the expiration date of the authorization form must be a specific date (such as July 31, 2023) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the use or disclosure (e.g., for the duration of the individual’s coverage), but in no event longer than permitted by applicable state law];
 - Contain a description of the information to be used or disclosed;
 - Contain the name of the entity or person authorized to use or disclose the PHI;
 - Contain the name of the recipient of the PHI;

- Contain a statement regarding the individual's right to revoke the authorization and the procedures for revoking authorizations; and
- Contain a statement regarding the possibility for a subsequent re-disclosure of the information.
- Follow the terms and conditions of the authorization.
- Retain the Authorization (and any applicable Authorization Revocation) in the individual's Designated Record Set for the applicable six-year period.

The Plan has an approved authorization for Plan participant's use. Where at all possible, the Plan's authorization should be used. (See **FORM Q - AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION** form.)

(b) Disclosure of PHI for Non-Health Plan Purposes

If the payment or health care operations of non-health benefits (e.g., short-term disability or life insurance) requires an individual's PHI, follow these steps:

- Contact the Privacy Officer to determine if an authorization for this type of use or disclosure is already on file.
- If no form is on file, request that the individual complete an authorization form. See **FORM Q - Authorization for Release of Protected Health Information**.
- HIPAA Workforce Members shall not attempt to draft authorization forms. All authorizations for use or disclosure for non-Plan purposes must be on a form provided by (or approved by) the Privacy Officer.
- Make any necessary disclosures according to the Minimum Necessary Standard Rule.
- Document disclosures in written or electronic format.
- Retain all appropriate documents for the applicable six-year period.

4. Disclosures to Personal Representatives

Policy

The Plan shall treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under the Rule.

Procedure

(a) Request for Use or Disclosure from Individual, Parent of Minor Child, or Personal Representative

If the Plan receives a request from a parent, guardian, or other person acting *in loco parentis* (in the place of a parent) who has the authority to act on behalf of an un-emancipated minor with regard to health care decisions, the Plan will treat the person as the personal representative of the un-emancipated minor.

If the Plan receives a request from a minor child's (i.e., an un-emancipated minor's) parent or an individual's personal representative, take the following steps:

- Verify the individual's (or parent's or personal representative's) identity.
- If a minor child is involved, contact the Privacy Officer for guidance. Whether an individual is a minor child must be determined in accordance with the provisions of the applicable state law of the child's place of residence.
- Follow the applicable policy and procedure for use and disclosure of PHI as permitted by these Policies and Procedures.

(b) Request for Use or Disclosure from Personal Representative of Adult or Emancipated Minor

If the Plan receives a request from a person who has authority under applicable law to act on behalf of an individual who is an adult or an emancipated minor with regard to health care decisions, the Plan will treat that person as a personal representative, and take the following steps:

- Verify the individual's (or parent's or personal representative's) identity.
- Follow the applicable policy and procedure for use and disclosure of PHI as permitted by these Policies and Procedures.

(c) Requests for Use or Disclosure from Spouse, Family Member, or Friend

If the Plan receives a request for disclosure from a spouse, family member, or friend who is not a personal representative or the parent of a minor child, any use or disclosure must be authorized by the individual whose PHI is involved. An **AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION (FORM Q)** can be used for these purposes.

(d) Requests for Use or Disclosure on Behalf of Deceased Individual

If the Plan receives a request from an executor, administrator, or other person with authority to act on behalf of a deceased individual or a deceased individual's estate, the Plan will treat the person as a personal representative of the deceased individual, and will take the following steps:

- Verify the individual's (or parent's or personal representative's) identity.
- Follow the applicable policy and procedure for use and disclosure of PHI as permitted by these Policies and Procedures.

5. Disclosure of PHI to Business Associates

Policy

The Privacy Officer and/or the Security Officer will identify individuals or entities that: 1) perform or assist with a specific function or activity and/or provide certain identified services for (or on behalf of) the Plan (other than other covered entities such as health insurance carriers); and 2) exchange individually identifying health information that is protected by the HIPAA Privacy and Security Rules with the Plan or on behalf of the Plan. These individuals or entities are Business Associates. The Privacy Officer will oversee determination of which individuals or entities fall within the definition of a Business Associate under HIPAA and enter into Business Associate Agreements on behalf of the Plan.

HIPAA Workforce Members may disclose PHI to the Plan's Business Associates and allow the Plan's Business Associates to create or receive PHI on behalf of the Plan. However, prior to disclosing PHI to a Business Associate or allowing a Business Associate to create or receive PHI on behalf of the Plan, the Plan must obtain written assurances, from the Business Associate through a contract or other agreement, that meet the applicable requirements of the Privacy and Security Regulations, that the Business Associate will appropriately safeguard the information. Before sharing PHI with outside organizations who meet the definition of a "Business Associate," contact the Privacy Officer and verify that a Business Associate contract is in place.

The Privacy Officer shall retain all Business Associate Agreements for at least six years after the date the applicable agreement is no longer in effect.

If the Plan learns that a Business Associate has materially violated the Business Associate Agreement in place with the Plan, the Plan will notify the Business Associate of the material violation. The Plan may provide an opportunity for the Business Associate to cure the material breach, or the Plan may terminate

the agreement between the parties, as governed by the applicable Business Associate Agreement between the Plan and the Business Associate.

Procedure

(a) Business Associate Agreement Provisions

Business Associate Agreements shall contain the following provisions:

- The permitted and required uses and disclosures of PHI by the Business Associate. Business Associates may not use or disclose PHI in a manner that the Plan may not use or disclose PHI under the Privacy Rule, except that a Business Associate may;
- Use or disclose PHI for the Business Associate's own proper management and administration as permitted by the Privacy Rule; and
- Provide data aggregation services to the Plan.
- Agreements that the Business Associate will:
 - Not use or further disclose the PHI other than as permitted by the Business Associate Agreement or as permitted by applicable law;
 - Use appropriate safeguards, including safeguards to protect electronic PHI to prevent further use or disclosure of the PHI except as allowed by the Business Associate Agreement;
 - Report to the Plan any use or disclosure (of which it is aware) not permitted by its Business Associate Agreement (including any breach of unsecured PHI);
 - Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to comply with the same restrictions and conditions that apply to the Business Associate;
 - Make available any PHI in accordance with an individual's request to access his or her own PHI;
 - Make available PHI for amendment or correction and incorporate any amendments to PHI in its records;
 - Make available any information required to provide an accounting of disclosures;
 - Carry out any obligations required by the HIPAA Privacy and Security Rules;
 - Make its internal practices, books, and records related to the use and disclosure of PHI received from, or created and received by the Business Associate on behalf of the Plan available to the Secretary of Health and Human Services in order for the Secretary to determine the Plan's compliance with the HIPAA Privacy or Security Rules;
 - At termination of the Business Associate Agreement, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of the Plan, that the Business Associate maintains in any form, and retain no copies of the information, or if return and destruction are not feasible, the Business Associate will extend the protections of the agreement and limit further uses and disclosures to those purposes that make return or destruction infeasible; and
 - Authorize termination of the contract if the Business Associate has violated the material terms of the Business Associate Agreement.

The Business Associate Agreement may contain the following provisions:

- The Business Associate may use PHI received in its capacity as a Business Associate from the Plan, if necessary for the following activities:
 - To carry out proper management and administration of the Business Associate;
 - To disclose PHI if:
 - The disclosure is required by law;
 - The Business Associate obtains reasonable assurance from the person to whom it is disclosed that the information will be held confidentially and used or further disclosed only as required by law; and

- The Business Associate notifies the Plan of any instances of which it learns that the confidentiality of any PHI has been breached.

(b) Disclosures to Business Associates

- Disclosures must be consistent with the terms of the Business Associate contract.
- Disclosures must comply with the Minimum Necessary Standard Rule. Recurring disclosures will be subject to the minimum-necessary standards set forth below, and each non-recurring disclosure must be approved by the Privacy Officer.
- Document disclosures, if necessary, in written or electronic format for the applicable six-year period.

(c) Material Breach or Violation of Business Associate Agreement

If a Plan representative learns of a material breach or a violation of a Business Associate Agreement, the representative shall notify the Privacy Officer as soon as practicable. The Privacy Officer will inform the Business Associate of the material breach or violation of the Business Associate Agreement and of any opportunity to cure. If the Business Associate does not satisfactorily cure the breach or violation (in the professional judgment of the Privacy Officer), the Privacy Officer will notify (in writing) the Business Associate of immediate termination of the Business Associate Agreement.

Documentation and correspondence related to a material breach of a Business Associate Agreement shall be retained for six years following the date the breach was discovered, the agreement was terminated, or the notice was sent to HHS, whichever is latest.

(d) Approval of Business Associate Agreement

All Business Associate Agreements must be signed and approved on behalf of the Plan by the Privacy Officer. If necessary, the Privacy Officer will retain the advice of legal counsel in drafting or executing a Business Associate Agreement.

6. Disclosures of PHI for Legal and Public Policy Purposes

Policy

PHI may be disclosed in the following situations without an individual's authorization, when specific requirements are satisfied. Permitted disclosures are disclosures:

- About victims of abuse, neglect or domestic violence;
- For judicial and administrative proceedings;
- For law enforcement purposes;
- For public health and health oversight activities;
- About decedents;
- For cadaveric organ, eye or tissue donation purposes;
- For certain limited research purposes;
- To avert a serious threat to public health or safety;
- For specialized government functions; and
- To the extent necessary to comply with laws relating to workers' compensation programs.

Procedure

Before making a permissible disclosure of PHI for legal and public policy purposes, take the following steps:

- Notify and obtain approval for the disclosure from the Privacy Officer.
- Verify the identity of the requestor
- If the individual's identity and authority is known, no further documentation is necessary.
- If the individual's identity and authority is not known, seek verification through one of the following:

- Signature on a written request with a copy of a government issued or photo identification issued by our organization; or
- Asking for known identifiers such as a combination of the Social Security number, birth date, maiden name, or driver's license number of the individual who is the subject of the PHI.
- If the individual is a Public Official
 - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status.
 - Make a copy of the identification provided and file it with the individual's Designated Record Set.
 - If the request is in writing, verify that the request is on the appropriate government letterhead.
 - If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
 - Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the individual's request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, contact the Privacy Officer.
- Obtain approval for the disclosure from the Privacy Officer.
- Retain all appropriate documents in written or electronic format for the applicable six-year period.
- Provide information in accordance with the Minimum Necessary Standard Rule.
- Document the disclosure in accordance using the **Protected Health Information Disclosure (FORM C)**.
- Make sure that the following specific requirements set forth below have been met:

(a) Disclosures about victims of abuse, neglect or domestic violence

Disclosures may be made about victims of abuse, neglect, or domestic violence if the following conditions are met:

- The individual, who is the subject of the PHI, agrees with the disclosure; or
- A statute or regulation expressly authorizes the disclosure, and the disclosure prevents harm to the individual (or other victim) or the individual who is the subject of the PHI, is incapacitated and unable to agree, and the information will not be used against the individual and is necessary for an imminent enforcement activity.

The individual must be promptly informed of the disclosure, unless prompt notification would place the individual at risk or if informing the individual would involve a personal representative who is believed to be responsible for the abuse, neglect, or violence.

Contact the Privacy Officer for a determination as to whether the disclosure concerns a victim of abuse, neglect, or domestic violence.

(b) For Judicial and Administrative Proceedings

Disclosure for purposes of judicial and administrative proceedings may be made if the following conditions are met:

- The Plan receives a court or administrative order; or
- The Plan receives a subpoena, discovery request, or other lawful process, not accompanied by a court or administrative order, which meets the standards of one of the following (items (1) through (11)) set forth below:

(1) Court or Administrative Order

If the Plan receives a court or administrative order, the following steps should be taken:

- Verify that the order is made by a court or an administrative agency.
- Release only the PHI expressly authorized by the order.

(2) Subpoena, discovery request, or other lawful process

If the Plan receives a subpoena, discovery request, or other lawful process without a court or administrative order, the following steps should be taken:

- Obtain satisfactory assurance from the party seeking the information that either of the following have occurred:
- The individual who is the subject of the request has been notified of the request, or
- The party seeking the information has obtained a “qualified protective order” that meets the requirements of the Privacy Regulations.

A “qualified protective order” is a court or administrative agency order that: (1) prohibits the parties from using or disclosing PHI for any purpose other than use in the litigation or proceeding for which the PHI is requested; and (2) requires the PHI to be returned to the Plan or destroyed at the end of the litigation or proceeding.

Satisfactory assurance that the party seeking the information has notified the individual who is the subject of the request can be met by the following statements from the party seeking the information:

- The party seeking the disclosure made a good faith effort to provide written notice to the individual, who is the subject of the PHI, or, if that individual's location is unknown, that the party mailed a notice to that individual's last known address;
- The notice contained sufficient information about the litigation or proceeding for which the PHI is sought to allow the individual to object to the court or administrative agency; and
- The time allowed for the individual to raise objections to the court or administrative agency has passed, and objections were either not filed, or any objections were resolved by the court or administrative agency in a manner permitting the disclosures.

Satisfactory assurance that a qualified protective order exists may be met by receipt of a copy of an agreed qualified protective order or a qualified protective order signed by the appropriate court or administrative agency.

If the satisfactory assurances identified above are not met, the Plan will consult legal counsel for advice.

(3) To a Law Enforcement Official for Law Enforcement Purposes

Disclosures to law enforcement officials or for law enforcement purposes may be made under the following conditions:

- Pursuant to legal process (such as a court order or court ordered warrant, a subpoena or summons issued by a judicial officer, a grand jury subpoena, or certain requests from government administrative agencies) and as otherwise required by law, but only if the information sought is relevant and material, the request is specific and limited to amounts reasonably necessary, and it is not possible to use de-identified information.
- To provide information about a deceased individual upon suspicion that the individual's death resulted from criminal conduct, but only to alert law enforcement about the death.
- To provide information that constitutes evidence of criminal conduct that occurred on our premises.
- To provide information limited to information to identify or locate a suspect, fugitive, material witness, or missing person.

- Information disclosed to identify or locate a suspect, fugitive, material witness, or missing person must be limited to the following information:
 - Name and address;
 - Date and place of birth;
 - Social Security Number;
 - ABO blood type and RH factor;
 - Type of injury;
 - Date and time of treatment;
 - Date and time of death, if applicable; and
 - A description of any distinguishing physical characteristics such as height, weight, gender, race, hair color, eye color, absence or presence of facial hair, scars, and tattoos.
- Unless PHI is disclosed to a law enforcement official to identify or locate a suspect, fugitive, material witness or missing person, PHI may NOT be disclosed that is related to an individual's DNA or DNA analysis, dental records, blood type, samples, or analysis of body fluids or tissue.
- Information about a suspected victim of a crime (1) if the individual agrees to disclosure; or (2) without agreement from the individual, if the information is not to be used against the victim, if need for information is urgent, if disclosure is in the best interest of the individual, or if the individual cannot agree because of incapacity or another emergency.
- Prior to releasing PHI to a law enforcement official about a suspected victim of a crime who has not agreed to the disclosure, the following steps must be taken:
 - Obtain a statement from the law enforcement official that: (1) the PHI is needed to determine whether a crime has occurred; (2) that the PHI will not be used against the victim; and (3) that immediate law enforcement action depends on the PHI and would be materially and adversely affected by waiting for the individual to agree to the disclosure; and
- Notify the Privacy Officer to determine whether the disclosure is in the individual's best interests in the professional judgment of the Plan.

The statement from the law enforcement official may be oral or written.

- PHI may be disclosed for law enforcement purposes for an individual who has died as a result of a suspected crime for the purpose of alerting a law enforcement official if the Plan has a suspicion that the death may have resulted from criminal activity. Contact the Privacy Officer for assistance.
- PHI may also be disclosed to a law enforcement official if the Plan believes that a crime has occurred on the Organization's premises. Contact the Privacy Officer for assistance.

(4) To Appropriate Public Health Authorities for Public Health Activities to the Extent Permitted by the Privacy Regulations.

PHI may be disclosed to the appropriate public health authorities for public health activities as permitted by the Privacy Regulations. Contact the Privacy Officer for guidance.

(5) To a Health Oversight Agency for Health Oversight Activities, as Authorized by Law.

PHI may be disclosed to a health oversight agency for health oversight activities if the following conditions are met:

- The requesting agency is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory (including American Samoa and the Northern Mariana Islands), or an Indian Tribe (or a person or contractor acting upon its authority) that is authorized by law to oversee one of the following:
- The public or private health care system;
- A government program or programs in which health information is necessary to determine eligibility or compliance; or
- A government program or programs to enforce civil rights laws for which health information is relevant.
- The PHI may only be used by the requesting agency for the following purposes:

- Audits;
- Civil or criminal investigations;
- Inspections;
- Licensure or disciplinary actions;
- Civil, administrative, or criminal proceedings; or
- Actions or other activities necessary for appropriate oversight of and by relevant agencies.

(6) To a Coroner or Medical Examiner about Decedents

PHI may be disclosed to a coroner or medical examiner to identify a deceased person, determine the cause of death, or for other duties as authorized by law. PHI may also be disclosed to a funeral director, under applicable state law, to allow the director to carry out duties related to the decedent.

(7) For Cadaveric Organ, Eye or Tissue Donation Purposes

PHI may be disclosed to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation or transplantation.

(8) For Certain Limited Research Purposes

PHI may be disclosed for certain limited research purposes provided that a waiver of the authorization required by the Privacy Regulations has been approved by an appropriate privacy board (as defined by Section 164.512(i)(1)(i) of the Privacy Regulations).

(9) In Emergency Situations

PHI may be disclosed to avert a serious threat to health or safety of an individual upon a belief in good faith that the use or disclosure is necessary to prevent a serious and imminent threat to the health or safety of a person or the public.

(10) For Specialized Government Functions

PHI may be disclosed for specialized government functions, including disclosures of an inmates' PHI to correctional institutions and disclosures of an individual's PHI to authorized federal officials, for the conduct of national security activities.

(11) For Workers' Compensation Programs

PHI may be disclosed for purposes of administering workers' compensation only to the extent necessary to comply with laws relating to workers' compensation or other similar programs.

7. Disclosures to Someone Involved in Individual's Care

Policy

If someone is obviously involved in an individual's care or the payment for that individual's care, PHI may be disclosed to that person, but that person must be a family member, other relative, close personal friend, or some other person identified by the individual as being involved in his or her care.

Procedure

If the individual is present, then the health plan may use or disclose PHI if: (1) the individual provides his or her agreement; (2) the individual has an opportunity to object and does not do so; or (3) from the circumstances, and based on professional judgment, an inference arises that the individual does not object to the disclosure or use.

If the individual is not present for the use or disclosure, or an opportunity to agree or object is not feasible due to an emergency or incapacity, the plan may disclose or use PHI if, in the exercise of professional

judgment, it is in the best interests of the individual. For example, if an individual is incapacitated and a spouse calls seeking assistance with payment of claims for the incapacitated individual, PHI may be disclosed to the spouse.

If uncertainty arises regarding whether the disclosure is appropriate, or if it is determined that disclosure is not appropriate, contact the Privacy Officer.

Any such disclosures must be limited according to the Minimum Necessary Standard Rule.

8. Disclosures by Whistleblowers

If a Workforce Member believes, in good faith, that the Plan has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or that the care, services, or conditions provided by the Plan potentially endangers a worker or the public, the Plan will evaluate whether any disclosure to a health oversight agency or public health authority or to an attorney retained by the Workforce Member falls within the exceptions for disclosures not otherwise permitted by the Privacy Rule and falls within the whistleblower disclosure exception under the Privacy Rule. If a disclosure, not otherwise permitted by the Privacy Rule, falls within the Whistleblower disclosure exception, the Plan will document the disclosure in using the **PROTECTED HEALTH INFORMATION DISCLOSURE (FORM C)**.

9. Complying With the “Minimum-Necessary Standard” for Routine Uses and Disclosures or PHI

Policy

The Plan and the Organization shall take reasonable efforts to limit PHI according to the Minimum Necessary Standard Rule to accomplish the intended purpose when using or disclosing PHI or requesting PHI from another covered entity or Business Associate. The Plan shall not use, disclose, or request an individual's entire medical record, even for purposes of payment or health care operations, unless the use, disclosure, or request is justified by the individual circumstances leading to the use, disclosure, or request.

The Plan will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Plan will comply with any future guidance on what constitutes the “minimum necessary” promulgated by the Secretary of Health and Human Services, which guidance shall override inconsistent policies and procedures established herein. References in this policy to the “minimum necessary” shall be interpreted in accordance with this paragraph.

However, the “minimum-necessary” standard does not apply to any of the following:

- Disclosures to or requests by a health care provider;
- Uses or disclosures made to the individual (as permitted by the Privacy Rule);
- Uses or disclosures made pursuant to a valid authorization;
- Disclosures made to the Secretary of the Department of Health and Human Services;
- Uses or disclosures required by law; and
- Uses or disclosures required to comply with the Privacy Regulations.

For all other recurrent uses and disclosures, the Organization and the Plan will apply the procedures set forth below.

Procedure

(1) Minimum Necessary When Disclosing PHI

For making *disclosures* of PHI:

Routine and Recurring Disclosure	Recipient(s)	Policy & Procedure
Health Plan Marketing	- Insurance Carriers - Third-Party Administrators - Brokers - Consultants - Plan Sponsor	Provide summary and de-identified information initially; provide minimum necessary PHI for accurate underwriting (genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy), premium rating, or other activities related to creation, renewal, or replacement of a contract for health benefits or health insurance; Provide PHI only at final negotiation if required.
Budgeting and Renewal	- Insurance Carriers - Third-Party Administrators - Brokers - Consultants	Provide summary and de-identified information initially; provide minimum necessary PHI for accurate underwriting (genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy).
Claim Issue Resolution	- Insurance Carriers - Consultants - Providers - Third-Party Administrators	Contact Carrier, Third-Party Administrator, or Consultant, on behalf of individual. Provide minimum necessary PHI to the third party for assistance with claim issue.
Compliance Issue Resolution	- Outside legal counsel - Brokers - Consultants	Provide minimum details of PHI necessary to secure legal counsel (but the Plan may reasonably rely on the representation of its counsel that the information requested is the minimum necessary for a stated purpose).
Claims Audit	- Brokers/Consultants; - Providers - Claims Review Specialists	Provide summary and de-identified information and PHI only if required
Billing Issue Resolution	- Insurance Carriers - Third-Party Administrators - Consultants - Providers	Provide summary and de-identified information and PHI only if required.
COBRA Rate or Funding Level Determination	- Insurance Carriers - Third-Party Administrators - Brokers - Consultants	Provide summary and de-identified information and PHI only if required.
Network Discount Evaluation	- Insurance Carriers - Brokers	Provide summary and de-identified information and PHI only if required.

	• Consultants	
Disruption Analysis	• Insurance Carriers • Brokers • Consultants	Provide summary and de-identified information and PHI only if required.
Strategic Planning	• Insurance Carriers • Third-Party Administrators • Brokers/Consultants • Plan Sponsor	Provide summary and de-identified information and PHI only if required.
Modifying, Amending, or Terminating the Group Health Plan	Plan Sponsor	Provide summary information.
Enrollment or Disenrollment Information	Plan Sponsor	Provide enrollment or disenrollment status information only.
Plan Administration	Plan Sponsor	To the extent necessary for plan administration so long as plan sponsor has amended its plan documents in accordance with the HIPAA Privacy Regulations.

For all other disclosures of PHI, contact the Privacy Officer, who will ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

(2) Minimum Necessary When Requesting PHI

For making *requests* for disclosure of PHI:

Routine and Recurring Requests	Disclosing Entity	Policy & Procedure
Health Plan Marketing	• Insurance Carriers • Third-Party Administrators; • Brokers/Consultants	Request summary and de-identified information and PHI only if needed.
Budgeting Underwriting and Experience Evaluation	• Insurance Carriers • Third-Party Administrators • Brokers/Consultants	Request summary and de-identified information and PHI only if needed (genetic information will not be used for underwriting purposes except for underwriting any applicable long-term care policy).
Claim Issue Resolution	• Insurance Carriers • Third-Party Administrators • Consultants • Providers	Request summary and de-identified information and PHI only if needed
Compliance Issue Resolution	• Outside legal counsel • Insurance Carriers • Third-Party Administrators • Brokers/Consultants	Request summary and de-identified information and PHI only if needed.

Routine and Recurring Requests	Disclosing Entity	Policy & Procedure
Claims Audit	- Insurance Carriers - Third-Party Administrators	Request summary and de-identified information and PHI only if needed.
Billing Issue Resolution	- Insurance Carriers - Third-Party Administrators - Consultants - Providers	Request summary and de-identified information and PHI only if needed.
COBRA rate or funding level determination	- Insurance Carriers - Third-Party Administrators	Request summary and de-identified information and PHI only if needed.
Network discount evaluation	- Insurance Carriers - Third-Party Administrators	Request summary and de-identified information and PHI only if needed.
Disruption Analysis	- Insurance Carriers - Third-Party Administrators	Request summary and de-identified information and PHI only if needed.
Strategic Planning	- Insurance Carriers - Third-Party Administrators; - Consultants/Brokers	Request summary and de-identified information and PHI only if needed.

For all other requests for PHI, contact the Privacy Officer, who will ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

(3) Minimum Necessary When Receiving or Disclosing PHI for Employment-Related Purposes

PHI should not be disclosed for employment-related purposes without a written authorization from the individual who is the subject of the PHI. For receiving PHI for employment-related purposes:

Routine and Recurring Disclosures and Requests	Recipient(s)/ Disclosing Entity	Policy & Procedure
Benefits inquiries and assisting with claims issues	- Insurance Carriers - Third-Party Administrators - Brokers/Consultants	Obtain written authorization for disclosure of PHI.
Obtaining a determination as to whether employee can perform essential functions and conclusions from fitness-for-duty exam	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; PHI obtained for performance of essential functions of a job or for a fitness-for-duty examination shall be filed in the applicable employee's medical file.
Obtaining results from drug-testing for employment-related reasons	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; drug testing results shall be filed in the applicable employee's medical file.

Routine and Recurring Disclosures and Requests	Recipient(s)/ Disclosing Entity	Policy & Procedure
Responding to a request for an accommodation under the Americans with Disabilities Act.	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; responses shall be filed in the applicable employee's medical file.
Responding to a request for a leave of absence under the Family and Medical Leave Act	Health care provider	Provide an authorization form for employee to complete and provide to health care provider; physician's certification shall be filed in the applicable employee's medical file.

10. Non-Routine Uses and Disclosures of PHI

The Plan will limit the use and disclosure for non-routine uses and disclosures to the minimum reasonably necessary to carry out the purpose for which a request is made. Non-routine questions for use or disclosure of PHI will be individually evaluated to determine the minimum reasonably necessary. If a HIPAA Workforce Member is uncertain whether an appropriate level of PHI constitutes what is reasonably necessary, that HIPAA Workforce Member should contact the Privacy Officer for assistance.

11. Disclosures of De-Identified Information

Policy

The Plan may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. The Plan can determine that information is de-identified: either by (1) professional statistical analysis conducted in accordance with the Privacy Regulations; or (2) removing 18 specific identifiers. These identifiers are as follows:

- Names;
- Geographic subdivisions smaller than State, including street address, city, county, precinct, zip code, and equivalent geocodes (special rules apply);
- All elements of dates (except year) relating directly to an individual (special rules apply);
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical Record Numbers;
- Health Plan beneficiary numbers;
- Account Numbers;
- Certificate/license numbers;
- Vehicle identification and serial numbers (including license plate numbers);
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (special rules apply).

Procedure

To use or disclose de-identified information, follow the following steps:

- Remove all identifiers listed above from information.
- Obtain approval from Privacy Officer for the disclosure. The Privacy Officer will verify that the information is de-identified.

The Plan may freely use and disclose de-identified information. De-identified information is not PHI.

D. Physical and Technical Security for PHI in Written, Electronic, and Oral Format.

Policy

The Plan has an obligation under both the Privacy and Security Rules to maintain the physical and technical security of the Plan's PHI regardless of whether that PHI is in written, electronic, or oral form. These policies and procedures are intended to meet the Privacy Rule requirements for security. The Plan's policies and procedures to comply with the Security Rule requirements for safeguarding electronic PHI are set forth in Section IV. Security Policies and Procedures.

The Organization and the Plan shall take reasonable measures to ensure that only designated HIPAA Workforce Members shall have access to PHI concerning individuals in the Plan.

The Privacy Officer and appropriate supervisors or managers shall determine the necessary level of access for each HIPAA Workforce Member. Each HIPAA Workforce Member shall be given physical access to PHI in accordance with his or her necessary level of access. Access should be limited sufficiently to afford Plan members as much privacy and security as possible without limiting access so as to interfere with Plan administration.

Procedures

1. PHI Storage and Access

a. Physical Security:

To maintain physical security of PHI, the Plan and the Organization will follow these safeguards in a reasonable manner:

- Maintenance of Primary Physical Security:
 - The Organization's offices where PHI is created, received, or maintained will maintain a secure area with a receptionist on duty and/or a locked door accessible only to HIPAA Workforce Members via an electronic card or code mechanism; and
 - Outside visitors will be escorted to their contact persons and not left unattended.
- Maintenance of Secondary Physical Security:
 - All files containing PHI, including electronic media, are to be kept in a separate file area of the where HIPAA Workforce Members create, receive, maintain, or transmit PHI, or an enclosed room or locked desk where access is limited to those HIPAA Workforce Members who have access per the terms of the Plan's Privacy Policy and Procedures.
 - HIPAA Workforce Members shall not leave files, electronic storage media, or documents containing PHI on desktops, countertops, or work tables unattended. Files or documents containing PHI may be kept at a HIPAA Workforce Member's desk provided that they are not left unattended on the HIPAA Workforce Member's desktop and are kept in locked drawers when not in use.

- Each HIPAA Workforce Member is expected to use reasonable efforts to protect PHI during and after work hours in areas under the HIPAA Workforce Member's control such as employee offices, workstations, desks, and filing areas.
- If a HIPAA Workforce Member leaves his or her desk for a short period of time, the HIPAA Workforce Member should conceal materials containing PHI to prevent accidental viewing.
- If a HIPAA Workforce Member leaves his or her desk for an extended period of time or at the end of the workday, the HIPAA Workforce Member should make certain that all materials containing PHI are placed in a secure location such as a locked desk drawer or filing cabinet.
- Documents containing PHI should not be left unattended on computers, copiers, fax machines, or printers.
- PHI should be protected in any form – electronic copy, hard copy, computer screen, or any other form of duplication for an original.
- Documents or electronic media containing PHI should not be deposited in trash cans, unsecured recycling bins, or other unsecured containers. PHI shall be destroyed in accordance with the Organization's document destruction policy.
- Where reasonable and appropriate, PHI will be secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. The amount of unsecured PHI maintained by the Plan should be limited.
- Acceptable means to render PHI unusable, unreadable, or indecipherable are encryption and destruction.
- The method to render PHI unusable, unreadable, or indecipherable shall be reviewed on an annual basis by the Security Officer to determine if the methodology or technology meets the current standards set by HHS.
- Verbal Security:
 - HIPAA Workforce Members shall take reasonable care in verbally discussing PHI to ensure that PHI is not discussed with any employee, individual, or third party who does not have access under the terms of the Plan's Privacy Policy.
 - When using the telephone to discuss PHI, HIPAA Workforce Members shall take reasonable care to make sure that the party to whom they are speaking has access to PHI and is either the individual who is the subject matter of the PHI, is the individual's personal representative, or is an individual, designated by a Business Associate, and insurance carrier, or a health care provider, to be contacted about PHI concerning individuals in the Plan.
 - PHI should not be discussed in public areas such as cubicles, elevators, and lunchrooms or at social gatherings.
- Security Maintenance:
 - The Privacy Officer and the Security Officer will monitor physical and verbal security and access to files containing PHI.
 - Supervisory and management personnel will review the location and placement of all computer displays, printers, copiers, and fax machines on a periodic basis to determine whether any changes should be made in order to comply with the Plan's Privacy Policies and Procedures and make any necessary changes.
 - If necessary, a risk and cost analysis shall be undertaken to determine whether physical changes are needed to improve security. Any such risk analysis shall be documented. All documentation should be forwarded to the Privacy Officer and shall be retained for six years.
 - HIPAA Workforce Members handling PHI shall report any violations of the Plan's Privacy Policy to the Privacy Officer as soon as possible, but no later than three business days after the incident occurs.
- Access to PHI:
 - Each HIPAA Workforce Member shall be advised of his or her level of access to PHI.
 - The Privacy Officer and appropriate supervisors or managers will make certain that physical access to PHI shall be limited to HIPAA Workforce Members. Necessary steps shall include making sure that only HIPAA Workforce Members have keys to filing cabinets containing documents with PHI and that only HIPAA Workforce Members have access to drawers or

work areas with materials containing PHI and workstations or electronic media containing PHI.

- Upon termination of a HIPAA Workforce Member's employment or other arrangement, or a change in assignments requiring a decreased level of access to PHI, the HIPAA Workforce Member's supervisor shall notify the IT department and the Privacy Officer. The Privacy Officer, or his or her designated representative, shall ensure that applicable access privileges are revoked or changed and that appropriate third parties are notified of the termination or decreased level of access to PHI. Relevant keys, cards, passwords, or electronic access should be returned or changed, as applicable. The Organization shall retain documentation of the termination or decrease in access.
- Destruction of PHI:
 - Discarded PHI shall be left completely inaccessible.
 - PHI in any form (hard copy, diskette, CD, etc.) shall not be discarded in ordinary trash.
 - Diskettes, CDs or other electronic media containing PHI must be erased or destroyed. Electronic media must be cleared, purged or destroyed consistent with NIST Special Publication 800-88 Rev 1, *Guidelines for Media Sanitization*, such that PHI cannot be retrieved.
 - Paper, film or other hard copy media is to be shredded or destroyed such that PHI cannot be read or otherwise cannot be reconstructed. Redaction is not an appropriate means of data destruction.
 - Photocopiers, multifunction machines, printers, scanners, or similar devices, with hard drives or other storage of information that are to be discarded, or leased machines that are to be returned must have the hard drives erased using NIST or Department of Defense standards before being disposed or returned.

b. Transmission Security:

The Plan shall implement such procedures and policies as necessary to comply with the HIPAA Security regulations. In addition to those safeguards, the Plan shall take the following steps:

- Incoming Mail:
 - Incoming mail containing PHI should be delivered unopened in its original sealed envelope to the person to whom it is addressed.
 - HIPAA Workforce Members should request that their business contacts – such as consultants and insurance carriers – clearly indicate the name of the specific person at the Organization and be labeled “confidential” on the envelope.
 - If a HIPAA Workforce Member receives PHI and the Workforce Member is not permitted access to PHI under this Privacy Policy, the HIPAA Workforce Member should redirect the incoming mail as soon as possible to an appropriate person with access to PHI.
- Outgoing Mail:
 - Outgoing mail containing PHI should be clearly addressed to a specific person and be labeled “confidential.”
 - If the outgoing mail contains PHI and is to be sent to an organization, it should be specifically addressed to a person at the organization who has access to PHI as per the organization's policies and procedures.
- Inbound Email:
 - HIPAA Workforce Members should exercise reasonable care to keep incoming e-mail messages secure and limit access by other HIPAA Workforce Members.
 - Substantive emails containing PHI may be printed out at a secure printer for hard copy storage in secured files maintained by any HIPAA Workforce Member.
 - HIPAA Workforce Members receiving PHI should request that persons sending emails limit the number of people that are copied on emails in order to limit the opportunity for inadvertent disclosure of PHI. The Privacy Officer will provide third-party administrators, carriers, and other service providers a list of individuals authorized to receive PHI on behalf of the Plan.

The Privacy Officer shall request that PHI sent via email to the Plan be sent to an individual identified on the applicable list.

- If a workforce member, who does not have access to PHI under this Policy, receives PHI, the workforce member should forward the email to someone who does have access under this Policy as soon as possible. The Workforce Member who improperly received the email should delete the email from his or her inbox, sent mail, and trash or deleted email folders after forwarding the email to the appropriate person.
- Outbound Email:
 - ePHI sent via email to an external party should be encrypted.
 - However, if it is not possible to encrypt an email, encrypted email sent externally from may be transmitted to outside contacts provided that any file attachments containing PHI are password protected or encrypted or are sent via a secure email process or an encrypted email and individually identifiable information is not contained in the subject line. The password may be communicated via phone, text, fax, or in a separate email significantly prior to or after the email containing the file with the PHI.
 - Email containing PHI sent internally in our offices may be transmitted provided that any individually identifiable information is not contained in the subject line.
- Incoming Faxes:
 - Facsimile (fax) machine transmissions containing PHI sent to a HIPAA Workforce Member shall be made using a fax machine dedicated for use by HIPAA Workforce Members.
- Outgoing Faxes:
 - When sending a fax, use a cover page containing the name of the recipient, the fax number, and the number of pages. Include a label stating that the fax is "confidential." Do not include any PHI on the cover page.
 - Faxes containing PHI sent from one HIPAA Workforce Member to another HIPAA Workforce Members shall be sent to a fax machine attended by the specific recipient. If necessary, the recipient should be telephoned prior to sending the fax.
 - If a workforce member receives PHI and the workforce member does not have access to the PHI, the workforce member should redirect the fax as soon as possible.
 - Faxes containing PHI sent to insurance carriers, consultants, brokers, other Business Associates, or entities for purposes of treatment, payment, or health care operations shall be sent to a specific person at the receiving organization and only to persons at that organization designated as having access to the Plan's PHI.
 - Cover sheets should be verified immediately before and after transmission of PHI to confirm that the information was sent to the correct fax number and was addressed to the correct recipient. If the PHI is not sent to the correct fax number, the sender should immediately send another fax to the number contacted in error with a reminder that the information sent is confidential and a request that the that the recipient contact the sender to arrange for proper destruction of the information. Any such error must be immediately reported to the Privacy Officer and recorded as an accidental disclosure of PHI.
 - The Privacy Officer will maintain all documentation regarding such an accidental disclosure for the applicable six-year period.
 - The accidental disclosure shall be subject to a breach risk assessment.
 - If necessary, the Privacy Officer shall contact legal counsel.
 - When sending flash drives/Diskettes/CDs and other portable electronic media such as DVDs, flash drives, thumb drives, hard drives, laptops, etc., follow the same policy for receiving and sending mail as described above. In addition, PHI sent on portable media must be encrypted, and the password must be sent separately.
- Internet:
 - Do not download PHI from, or upload PHI to, any web site or system via the internet other than for an insurance carrier or business associate unless the site is a secure site that can be accessed via a secure link (SSL). This means that the site can be accessed using a secure,

encrypted connection as required by the Privacy Regulations. When uncertain if a site is secure, check with IT.

- HIPAA Workforce Members may use the secure system of an insurance carrier, a service provider, or a Business Associate via their website to communicate PHI. In other words, the PHI must reside on a secure system belonging to the service provider, insurance carrier, or Business Associate.
- Take reasonable care to protect PHI from access by individuals who are not authorized to access it.

c. PHI Storage Related to Terminated Workforce Members

PHI for terminated Workforce Members shall be protected in the same manner that it was protected prior to the Workforce Member's termination of employment or other arrangement. The former Workforce Member's file PHI shall be retained for a period of six years following the date it was created or the date it was last in effect, whichever is later.

d. Securing Electronic PHI

When deemed appropriate by the Privacy Officer and the Security Officer, electronic PHI shall be encrypted by 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. Decryption tools must be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

- Data at rest: data that resides in databases, file systems, flash drives, memory, and any other structures storage system must be encrypted consistent with National Institute of Standards and Technology, or "NIST," Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.
- Data in motion: data that is moving through a network, including wireless transmission, whether by email or structured electronic interchange, must be encrypted consistent with NIST Special Publication 800-52 Rev 1, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77 Rev 1, *Guide to IPsec VPNs*; or 800-113, *Guide to SSL VPNs*, or others which are Federal Information Processing Standard 140-2 validated.

E. Data Breach Policy and Procedures

1. Breach of Information

Policy

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its Business Associates discovers a breach of unsecured PHI. In order to constitute a breach, which triggers the notification requirement, the following conditions must be met:

- *The information breached is PHI.* The breach notification requirement does not apply to information that is not PHI – such as de-identified information.
- *There has been an unauthorized acquisition, access, use or disclosure.* Unauthorized means acquisition, access, use or disclosure of PHI that compromises the privacy or security of that information. If there is no HIPAA privacy violation, there is no breach. Uses or disclosures involving more than the minimum necessary amount may qualify as a breach.
- *The use or disclosure compromised the security or privacy of the PHI.* An impermissible use or disclosure of PHI is presumed to be a breach unless there is a demonstration of a low probability that the PHI has been compromised. Notification to impacted individuals is necessary in all situations except when there is a demonstration of a low probability of harm or that an exception to the breach notification rule applies. In order to assess the probability that the PHI has been compromised, the

Privacy Officer will consider the following: (1) the nature and the extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the PHI was disclosed; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

The following shall not be considered breaches:

- Unintentional acquisition, access, or use of PHI by a HIPAA Workforce Member or individual acting under the authority of a covered entity or Business Associate, if the acquisition, access, or use was made in good faith, within the course and scope of employment or other professional relationship, and does not result in further use or disclosure. For example, if a billing employee opens an email with PHI mistakenly sent by a nurse, this would not be a breach if the billing employee realizes he is not the intended recipient, notifies the nurse of the mistake, and deletes the email.
- Inadvertent disclosure of PHI from a person who is authorized to access PHI at a facility operated by a covered entity or a Business Associate to another similarly situated person authorized to access PHI at the same facility if the information is not further acquired, accessed, used or disclosed without authorization. Inadvertent disclosures of PHI from a person who is authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the same covered entity or Business Associate are also exceptions.
- The unauthorized person to whom PHI has been disclosed would not reasonably have been able to retain the information. HHS gave two examples. In the first example, a health plan sends EOBs to the wrong person. The envelopes are returned by the post office unopened and marked undeliverable. In this case no breach occurred. If, however, any of the envelopes are not returned, this should be treated as a potential breach. In the second example, a nurse hands a patient someone else's discharge papers, but realizes her mistake and recovers the papers quickly. If the nurse can reasonably conclude that the patient could not have read the information, this would not be a breach.

All HIPAA Workforce Members are responsible for immediately reporting breaches or potential breaches of unsecured PHI. HIPAA Workforce Members may report breaches or potential breaches to their manager or the Privacy Officer. If a report is made to a manager, the manager shall immediately report the potential breach to the Privacy Officer.

Procedure

The Privacy Officer and/or the Plan's Security Officer shall be responsible for investigating all reported incidents of possible breaches in the security or privacy of PHI held by the Plan. After investigation and determination that an unauthorized use or disclosure of PHI occurred, the Privacy Officer and/or the Plan's Security Officer shall take necessary steps to investigate to determine if a breach has occurred, mitigate harm to the extent feasible, provide required notifications, and take steps to reduce the likelihood that similar breaches occur in the future.

The Privacy Officer shall maintain a Security Incident File. In the event of a PHI privacy or security violation, the following steps shall be taken:

(1) Report of Security Incident.

Any Workforce Member or other individual (such as a Business Associate) who becomes aware of a possible breach of the privacy or security of PHI maintained by the Plan shall report the security incident to the Privacy Officer.

The Privacy Officer shall then take the following steps:

- Ask the Workforce Member or other individual reporting the security incident to provide the details of the alleged breach in writing (use the Security Incident Report form).
- Review the written summary and determine if further investigation is necessary.

- Conduct an investigation. Determine the following:
- Whether a breach has occurred.
- If a breach occurred, what level of breach occurred:
 - Very serious – a large amount of data, or very sensitive data was improperly disclosed.
 - Serious – a large amount of data has potentially been improperly disclosed, but the likelihood of access is slight.
 - Important – protected participant data has been inappropriately released to a business partner.
 - Minor – protected participant data has been handled carelessly, but no exposure occurred.
- If a breach occurred, what level of culpability exists:
 - Very serious – Workforce Member or other individual engaged in malicious misconduct.
 - Serious – Workforce Member willfully ignored established policies and procedures.
 - Important – Workforce Member inadvertently failed to follow established policies and procedures.
 - Minor – Workforce Member made an error in judgment based on a misunderstanding of the policies or procedures.
- If a breach of privacy or security may have occurred, create a Security Incident File. The File shall contain the following:
 - **The Security Incident Report (FORM S).**
 - **The Security/Privacy Incident Review (FORM T).**
 - The original written summary of the alleged breach.
 - The intended course of action to investigate the alleged breach.
 - Documentation of the investigation, including any documentation related to any interviews.
 - All correspondence related to the alleged breach, including correspondence with legal counsel, if any, which shall be marked as “privileged and confidential.”
 - Documentation of the decision as to whether a breach occurred and any steps taken to resolve the issue.
 - Document any data or physical materials that may have been compromised, lost, destroyed, or stolen.
 - For serious and very serious situations, inclusion of outside legal counsel.
 - For serious and very serious situations, inclusion of professional, state and/or HIPAA oversight agencies such as the Office for Civil Rights.
- Develop an action plan, including the following:
 - Steps to be taken to determine the actual cause of the breach.
 - A determination of whether policies and procedures need to be changed to prevent future breaches, and if so, which policies and procedures.
- Steps to contact affected individuals whose PHI has been or is reasonably believed to have been compromised by the breach:
 - Provide notice (see **FORM U - Sample Breach Notice to Individual**), which must be written in plain language and contain the following:
 - A brief description of what happened, including the date of the breach, if known, and the date of the discovery of the breach;
 - A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 - Contact procedures for individuals to ask questions or learn additional information.
 - A toll-free number, an email address, web site, or postal address.
 - Provide notice to impacted individuals as soon as possible without unreasonable delay, but no later than 60 days after the date of discovery.

- Notice must be provided by first-class mail to the impacted individual at the last known address of the individual, unless only insufficient or out-of-date contact information exists that precludes notice to the individual. If only insufficient or out-of-date contact information exists, the following steps must be used:
 - If there are fewer than 10 individuals who cannot be contacted by first-class mail, then notice may be made using an alternative notice such as by email, by telephone, or by other appropriate method.
 - If there are 10 or more individuals who cannot be located by first-class mail, then an alternative notice must be posted on our website for at least 90 days in a conspicuous location, or it must be posted in a major print or broadcast media where the affected individuals most likely live. The notice must also include a toll-free number to call for more information. The toll-free number shall be active for at least 90 days.
 - If the Plan knows the individual is deceased and has the address of the next of kin or personal representative, the Plan may provide written notice by first-class mail to either the next of kin or the personal representative. If the Plan has insufficient or out-of-date contact information for the next of kin or personal representative for a deceased individual impacted by a Breach, the Plan is not required to provide substitute notice to the next of kin or personal representative of the deceased individual.
 - If a breach affects the protected health information of 500 or more individuals, the Privacy Officer shall notify HHS as required by HIPAA (within 60 days. Sixty days is an outer limit but may be a reasonable time for providing the notification of Breach depending upon the facts and circumstances. If a breach affects the protected health information of fewer than 500 individuals, the Privacy Officer shall log the breaches and report all breaches on an annual basis and no later than 60 days after the end of the calendar year in which the breaches were discovered. Instructions along with a list of the data elements required by HHS and the website address are contained in the Sample Notice to Secretary of HHS of Breach of Unsecured Protected Health Information (FORM Y).
 - If a breach of unsecured PHI involves more than 500 residents of a single state or jurisdiction, notification shall be provided to prominent media outlets serving the state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after Discovery of the Breach. (See **FORM V - Sample Press Release**.) Sixty days is an outer limit but may not be a reasonable time for providing the notification of Breach depending upon the facts and circumstances.
 - If a law enforcement agency requests that the notice to individuals and the media be delayed on the grounds that notice may impede a criminal investigation or national security, the notice must be delayed, but for no more than 30 days.
- Appropriate consequences for any responsible Workforce Member(s).
 - Determine if changes are necessary to policies and procedures to prevent future similar breach.
 - Include Action Plan in the Privacy Incident File.

(2) Concluding Investigation

Upon conclusion of investigation into a potential breach, the Privacy Officer shall take the following steps:

- Document the outcome of the investigation in the Privacy Incident File.
- Administer and document any necessary sanctions and disciplinary actions.
- Make changes, if necessary, to policies and procedures.

BREACH OF PRIVACY CHECKLIST

Activity	Date	By (Initials)
1. Receipt of Notice of Potential Breach		
2. Review by Privacy Officer of Written Report		
3. Creation of Privacy Incident File		
4. Development of Written Plan of Action		
5. Collection of Investigation Documentation Completed (e.g., all transcripts, correspondence with employees and with legal counsel, etc.)		
6. Completion of Investigation		
7. Documentation of Final Determination		
8. If breach has occurred complete items #8 through 10. If no breach, skip to #11		
9. Notification to Affected Persons that Privacy was Compromised		
10. Notification of Media (If Over 500 Members' Information Was Compromised)		
11. Notification to US Department of Health and Human Services		
12. Documentation of Resolution (including disciplinary actions as appropriate, or necessary changes to policies and procedures)		
13. Completion of Corrective/Disciplinary Actions		

Note: All correspondence should be in writing and transcripts made of all verbal conversations. Retain ALL documentation and correspondence in the incident file for 6 years following the completion of the investigation.

Signed:

Privacy or Security Officer

Date

IV. Security Policies and Procedures

A. Security Management Process

1. Risk Management

Policy

Our organization, on behalf of the Plan, will implement reasonable security measures necessary to reduce identifiable risks and vulnerabilities to reasonable and appropriate levels, including, but not limited to the creation, implementation, and maintenance of specific Security Policies and Procedures for any ePHI that it creates, receives, maintains, or transmits. The Plan must also rely upon its insurance carriers, third-party administrators, and other business associates to manage risks to ePHI by limiting vulnerabilities, based on risk assessments, to a reasonable and appropriate level. The Policies and Procedures are also intended to prevent, detect, contain, and correct security violations. The Security Officer and designated HIPAA Workforce Members shall create and maintain internal policies and/or procedures for the following:

- Sanctions;
- Information system activity review;
- Personnel security, including:
 - Screening personnel that work with ePHI;
 - Training employees with access to ePHI, and handling terminations of access to ePHI for employees upon termination of employment, job duties, or other relationship (as appropriate);
 - Appropriate supervision of employees with access to ePHI;
 - Limiting employee and business associate access to the minimum level of information necessary to accomplish established tasks;
 - Monitoring systems access to ePHI; and
 - Modifying employee's access to ePHI as necessary when a change in employment responsibilities or systems occurs.
- Information access management;
- Security awareness and training;
- Contingency planning;
- Facility access controls;
- Workstation use;
- Workstation security;
- Device and media controls;
- Access control;
- Authentication of persons or entities;
- Revision of Security Policies and Procedures;
- Investigation of alleged violations of this Policy or the HIPAA Security Regulations;
- Exchanging ePHI with Business Associates; and
- Other policies and procedures necessary to comply with HIPAA.

Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process.

Procedure

Our organization, on behalf of the Plan, will prioritize, evaluate, and implement appropriate risk-reducing controls recommended from the Plan's risk analysis process to ensure the confidentiality, integrity, and availability of ePHI. To manage risks, we shall follow the following process:

- Create, based upon our risk analysis, a prioritized list of action items.
- Evaluate any recommended remediation efforts and alternative solutions to determine what is reasonable and appropriate. We will also determine the feasibility (e.g., resource availability, user acceptable) and the effectiveness of the recommendations.
- Perform a cost-benefit analysis of each control option, considering the potential risk reduction of each control determined to be the most effective, and the cost of the that control.
- Using the information and evaluations from the first three steps, determine the best controls (administrative, physical, and/or technical safeguards) to reduce risk to a reasonable and appropriate level to protect the confidentiality, integrity, and availability e ePHI.
- Identify the individuals or teams who will implement each of the specific selected controls. We will also identify any necessary equipment, training, or other resources needed to implement those controls.
- Develop an implementation plan that will include the following:
 - The threat/vulnerability pairs with associated numerical risk assessment (0 through 16)
 - Prioritized list of action items
 - Recommended control for each threat/vulnerability pair
 - Individual or team responsible for implementation
 - Required resources for implementation
 - Target date for completion
 - Ongoing implementation requirements (e.g., annual review)
 - Monitor affected parts of the information system impacted by implemented controls.
 - Monitor to identify new risks or changes in operations or environment that may necessitate either additional or different controls or a new Risk Analysis and to determine whether implemented controls meet expectations for reducing risk.

The Plan acknowledges that it is not practical to eliminate all risk, but we will take steps to reduce risk to the confidentiality, integrity, and availability of ePHI to a reasonable and appropriate level.

2. Risk Analysis

Policy

It is our policy to conduct thorough and timely risk analyses of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI on behalf of the Plan and to develop strategies to efficiently and effectively mitigate the risks identified in the analysis process as an integral part of our information security efforts.

On behalf of the Plan, our organization implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

- Ensure the confidentiality, integrity, and availability of all ePHI the Plan creates, receives, maintains, and/or transmits,
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI,
- Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required, and
- Ensure compliance by HIPAA Workforce Members.

Such a review will be conducted every year. Any risk remaining (residual) after other risk controls have been applied, requires sign off by the HIPAA Security Officer.

All risk management efforts, including decisions made on what controls to put in place as well as those not put into place, will be documented and the documentation will be maintained for six years.

Procedure

The intent of completing a Risk Analysis is to determine potential threats and vulnerabilities related to ePHI and the likelihood and impact should they occur. On behalf of the Plan, our organization shall take the following steps:

- The Security Officer, the Privacy Officer, and other assigned workforce members will identify the areas in which ePHI is used, transmitted, or maintained by HIPAA Workforce Members on behalf of the Plan.
- The Security Officer, the Privacy Officer, and other assigned workforce members will identify and document potential threats.
- The Security Officer, the Privacy Officer, and other assigned workforce members will develop a list of technical and non-technical system vulnerabilities that could be exploited or triggered by potential threat sources.
- The Security Officer, the Privacy Officer, and other assigned workforce members will develop a list of current or planned controls (e.g., policies, procedures, training, technical safeguards, insurance, etc.).
- The Security Officer, the Privacy Officer, and other assigned workforce members will assign a numerical value for an overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source for each identified technical and non-technical system vulnerability identified in the steps above given the existing or planned security controls.
- The Security Officer, the Privacy Officer, and other assigned workforce members will assign a numerical value for the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors to consider include the importance of the data to the Plan; costs associated; loss of confidentiality, integrity, and availability of systems and data; and whether the data is replicated or duplicated in the hands of a third-party administrator or insurance carrier.
- The Security Officer, the Privacy Officer, and other assigned workforce members shall then establish a numerical risk score by multiplying the numerical likelihood determinations by the numerical impact score for each identified vulnerability.
- The Security Officer and assigned workforce members will identify controls that could reduce or eliminate the identified risks, as appropriate to our organization's operations on behalf of the Plan to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability.
- The results of the Risk Analysis will be documented and retained for at least six years.

3. Sanction Policy

If a Workforce Member fails to comply with the Plan's Security Policies and Procedures or the HIPAA Security Rule, the Workforce Member responsible for the violation will be dealt with according to our standard disciplinary practices. The disciplinary action will depend upon the severity and/or frequency of the violation. Disciplinary action may range from, but is not limited to, a verbal warning, a written warning, probation, or other disciplinary action up to and including termination of employment.

4. System Activity Review

Policy

Our organization, on behalf of the Plan, shall review logs of access and activity of ePHI applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance to safeguarding the privacy and security of ePHI. We intend to review information system access and activity (e.g., log-ins, and security incidents). A review may be done as a periodic event, as a result of an individual complaint, or when suspicion of employee wrongdoing arises.

Procedure

The Security Officer or designee assigned the task of generating reports for review activities to the individual responsible for the application, system, or network. The Security Officer will also assign the task of reviewing the logs to the individual responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task.

The Security Officer shall identify “trigger events” or criteria that raise awareness of questionable conditions of viewing of confidential information. Trigger events may include the following:

- Individual complaint
- Atypical patterns of activity
- Failed authentication attempts
- Activity post termination

The Security Officer will determine whether any trigger events requires further investigation or review.

Our organization may also engage the use of an automated process to monitor for security incidents and provide reports of potential incidents to the Security Officer or the Security Officer's designee. If the process is not automatically document, the Security Officer or the Security Officer's designee will document the review using **the SYSTEM ACTIVITY REVIEW form (FORM S-1)**.

B. Workforce Security

1. Authorization and Supervision

Policy

The Security Officer (or the Security Officer's designee) will authorize user access to systems containing ePHI based upon job responsibilities for individuals who work with ePHI or in locations where ePHI might be accessed.

Procedure

All requests for access to any of our information systems and applications must be accompanied with **FORM S-2 SYSTEM ACCESS REQUEST/CHANGE** approved by Human Resources unless requests for access or change may be submitted electronically to IT.

The Security Officer or the Security Officer's designee will maintain copies of **SYSTEM ACCESS REQUEST/CHANGE** forms, as applicable. Electronic requests for access or change will be maintained electronically. All applicable forms will be maintained for at least six years.

Individual supervisors will be held responsible for adequately supervising HIPAA Workforce Members to ensure appropriate access. The Security Officer, in coordination with the Privacy Officer, will verify and

document each HIPAA Workforce Member's level of access to ePHI. (Use **FORM S-3 SECURITY ACCESS REPORT**).

2. Workforce Clearance

Policy

The level of access granted to our information systems is based on the minimum necessary information (amount of data) access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations on behalf of the Plan.

Procedure

The Security Officer, in coordination with the Privacy Officer, will document based on job title (or job category) the level of access to ePHI by taking the following steps:

- Determining job description or classes of Workforce Members requiring access to ePHI;
- Determining the categories of ePHI available through information systems or information systems the Plan can access;
- Identifying categories of ePHI needed to perform the job functions for each role;
- Creating a mechanism to approve the minimum necessary access and any additional access to ePHI;
- Developing a method to monitor and/or audit established access and termination of access to ePHI; and
- Establishing a method to ensure security access changes for those who change positions and no longer meet clearance requirements.

(Use **FORM S-3 SECURITY ACCESS REPORT**.)

The level of access will be periodically reviewed upon a change in job role. When appropriate, job descriptions will be modified to include the minimum necessary level of user access to ePHI necessary to perform listed job functions.

3. Termination Procedures

Policy

If a Workforce Member with access to ePHI is terminated or has his or her job responsibilities revised to terminate access to ePHI, the former employee will be required to return all applicable physical security tokens, keys, access cards, etc. that could be used to gain access to ePHI. Electronic access to ePHI shall be terminated (e.g., remote access, email access). IT shall terminate the individual's access to systems containing or permitting access to ePHI on behalf of the Plan.

Procedure

Upon termination of the employment or revision of job responsibilities to end access to ePHI, the Security Officer or designee or the individual's supervisor will retrieve all applicable physical security tokens, keys, access cards, etc. that could be used to gain access to ePHI from the Workforce Member. Electronic access to ePHI shall be terminated (e.g., remote access, email access).

Termination of access for individuals involuntarily terminated from employment shall occur on date of termination. Termination of access for individuals voluntarily terminated from employment shall occur on last day of employment.

If a HIPAA Workforce Member has a change in ePHI access level due to a change in job position or job duties, the Security Officer (or designee) will reevaluate that individual's access and modify as necessary. The Security Officer will retain applicable termination documents for six years from the date of termination.

C. Information Access Management

1. Access Authorization

Policy

Access to ePHI shall be limited to the individuals identified on the **HIPAA WORKFORCE MEMBER DESIGNATION**.

Procedure

The Security Officer, the Privacy Officer, and/or appropriate supervisors or managers shall determine the necessary level of access for each HIPAA Workforce Member. Each HIPAA Workforce Member shall be given access to ePHI only to the extent that ePHI is necessary for a particular HIPAA Workforce Member to perform his or her job duties. Access should be limited sufficiently to afford Plan members as much privacy and security as possible without limiting access so as to interfere with the efficiency of Plan administration.

2. Access Establishment and Modification

Policy

The Security Officer and the Privacy Officer will periodically review the job responsibilities of all HIPAA Workforce Members to ensure that each HIPAA Workforce Member shall have appropriate access to workstations, transactions, programs, and processes involving the use or disclosure of ePHI required for each Workforce Member to do his or her job, but at no higher level of access than necessary.

HIPAA Workforce Members' access to ePHI will be limited to the minimum necessary level of information necessary to accomplish their job responsibilities.

Procedure

All requests for access to any of our information systems and applications must be accompanied with a **SYSTEM ACCESS REQUEST/CHANGE form (FORM S-2)** approved by Human Resources unless requests for access or change may be submitted electronically to IT.

The Security Officer or the Security Officer's designee will maintain copies of **SYSTEM ACCESS REQUEST/CHANGE** forms, as applicable. Electronic requests for access or change will be maintained electronically. All applicable forms will be maintained for at least six years.

Access to ePHI will be based upon job duties and limited administratively, technically, or physically to the minimum necessary to carry out job duties.

D. Security Awareness and Training

1. Protection from Malicious Software

Policy

Our organization, on behalf of the Plan, shall maintain systems and processes to guard against, detect, and report malicious software.

Procedure

Anti-virus software with current virus definition files will be installed on all desktops, laptops, and servers and will be programmed to conduct automatic virus scanning. Security patches and updates for computer operating systems and software will be installed to reduce known vulnerabilities. Workforce Members should not download software from the internet or installing software on desktops or laptops without approval from IT.

Workforce Members shall be reminded not to open email attachments from unknown or untrustworthy sources. If a virus is suspected or detected, the Security Officer (or the Security Officer's designee or IT) must be notified as soon as possible. Non-IT Workforce Members are not permitted to perform virus eradication without authorization and supervision. If a computer virus is suspected or identified, the infected machine and any others that may have been contaminated shall be isolated from the network, scanned, and repaired.

Training on protection from malicious software shall be included in our Security training.

2. Log-in Monitoring

Policy

To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately secured, our organization, on behalf of the Plan, will configure our information system or enable software to record failed login attempts to our information system and require automatic logout after five failed attempts.

Procedure

Our organization, on behalf of the Plan, shall take the following steps:

- Record failed login attempts to our information system.
- Require individuals who have incorrectly entered their usernames and passwords five or six times, depending on the system settings, to wait for the lockout duration (30 minutes) to expire. Alternatively, users can contact a System Administrator to reset their account. Additionally, users can use the self-service "Forgot Password" option to reset their password and regain access.
- Require individuals who believe that their usernames or passwords have been compromised to contact IT.

3. Security Training, Awareness, and Reminders

Policy

The Security Officer (or the Security Officer's designee) will train all HIPAA Workforce Members on password management, login monitoring, and protection from malicious software. Workforce Members who have access to PHI will receive the training necessary and appropriate to permit them to carry out

their functions within or on behalf of the Plan. New HIPAA Workforce Members will be trained within 30 days of joining our organization. Subsequent training will occur promptly after any material change in these policies and procedures for employees affected by the material change, and training will be conducted for all HIPAA Workforce Members on a periodic basis or when there is a change in processes or other requirements.

The Security Officer (or the Security Officer's designee) will send out periodic email alerts on any potential new risks (e.g., certain virus or worms, phishing scams, or changes to the Security policy) or reminders of important Security measures.

Procedure

The Security Officer will provide training through appropriate procedures such as small group training, webcasts, emails, newsletters, or other applicable methods. New HIPAA Workforce Members will be trained within 30 days of becoming a HIPAA Workforce Member. Subsequent training will occur promptly after any material change in these policies and procedures for employees affected by the material change.

Employees with access to ePHI shall be trained on proper uses and disclosures of ePHI stored in systems or applications, instructions on contacting a designated person or help desk when ePHI may have been altered or destroyed in error, reporting a Security Incident, how to guard against, detect, and report malicious software, password management, and how to report discrepancies related to log-in attempts.

Employees undergoing training will be required to document their participation in training sessions. Documentation shall include the date of the training, the employee's name, and the employee's signature. The Security Officer shall keep a record of training sessions for six years from the date of training.

The Security Officer (or the Security Officer's designee) will send out periodic email alerts on any potential new risks (e.g., certain virus or worms, phishing scams, or changes to the Security Policy).

4. Password Management

Policy

Our organization, on behalf of the Plan, shall require HIPAA Workforce Members to periodically change their passwords enabling them to access ePHI (e.g., user accounts, email, and screensaver protection) and to follow certain rules when creating or changing a password. Passwords shall be revoked upon termination of employment or changes in job duties resulting in a loss or decrease of access to ePHI.

HIPAA Workforce Members' passwords must meet our organization standards for complexity.

Procedure

Passwords must contain at least eight alphanumeric, upper- and lowercase non-sequential characters and contain at least three of the four categories: alphabet character, upper case letter, number, non alpha-numeric character. Passwords should not be based on personal information such as nicknames, family names, dates of birth, or other information that may be easily guessed. Passwords should be created that are easily remembered. Passwords should not be posted in a Workforce Member's work area. Passwords may not be shared with other Workforce Members other than information system personnel.

Workforce Members are required to change passwords every 90 days. The last five previously used passwords may not be used.

The Security Officer (or the Security Officer's designee) shall work with IT personnel to ensure that passwords are revoked as soon as possible for Workforce Members who terminate employment or no longer need access.

If a Workforce Member believes his or her password may have been compromised, the individual should immediately report the incident to the Security Officer or to IT as soon as practicable.

E. Security Incident Procedures

1. Response and Reporting

Policy

It is our policy to implement and follow a security incident response process to detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

Individuals needed and responsible to respond to a security incident may vary depending on the nature of the incident and may vary during the course of the investigation and remediation of the incident. Those individuals may include the following:

- HIPAA Security Officer
- HIPAA Privacy Officer
- Senior Management
- Information Technology Personnel
- Security Team Personnel
- Building and/or Facilities Management Personnel

Other Individuals which may be needed include representation from:

- Public Affairs
- Legal/Compliance Department
- Internal Audit/Risk Management
- Other workforce members involved in the incident or needed to fix/resolve the situation leading to the incident
- Third-Party Vendors (as necessary)

Procedure

Workforce Members must report suspected and known security incidents involving ePHI in one of the following ways:

- Report through technical means, such as through an IT Help Desk, an IT hotline number, or an email application (e.g., a phishing report button)
- Direct report to management, the Security Officer or Privacy Officer
- Report to an immediate supervisor, who shall report to IT, the Security Officer, or the Privacy Officer

If an individual other than the Security Officer or Privacy Officer receives the report, that individual shall immediately notify the Security Officer, the Privacy Officer, or both.

The Security Officer or the Privacy Officer will complete a **SECURITY INCIDENT REPORT (FORM S)**. Applicable documents shall be retained for a minimum of six years.

F. Contingency Plan

1. Data Backup Plan

Policy

Our organization creates a retrievable exact copy of ePHI before movement of equipment. We maintain a record of movements of hardware and electronic media containing ePHI and any person responsible therefore on behalf of the Plan. We will use these procedures to track the movement of hardware and electronic media containing ePHI in accordance with the standards set forth in the HIPAA Security Rule.

In addition, we will create backups of ePHI stored on network drives and periodically test those backups.

Procedure

ePHI should not be stored on any workstation's hard drive. All ePHI should be stored in a network folder or other part of the information system subject to automated backup (such as email). If any ePHI is saved onto the hard drive of a workstation or onto removable media, such as a flash drive, it shall be duplicated on a network folder dedicated to HIPAA Workforce Member usage prior to movement outside of our organization's facilities.

In addition, our organization, on behalf of the Plan, will conduct hourly snapshot data backups. We will conduct a full system backup daily. Backups shall be logged through an automated process.

For each backup created:

- The backup media will be to the cloud.
- The backup software will be AWS.
- The backup copy will be verified for data integrity using the backup software.
- The backup copy will be securely stored off site at geographically diverse sites. The organization's two primary data centers in the U.S. (Las Vegas and San Jose) are fully synchronized and located in separate disaster zones.

2. Disaster Recovery Plan

Policy

Our organization, on behalf of the Plan, shall establish procedures to restore loss of data, related to ePHI primarily maintained on our information system, within an established timeframe for recovery based upon the Plan's criticality analysis. The Security Officer shall have the primary responsibility for implementing procedures and processes regarding ePHI in the event of disaster recovery and shall delegate responsibilities as necessary to carry out data recovery. However, the Plan's ePHI is primarily maintained on third party vendor sites.

Procedure

The Security Officer and the Privacy Officer shall maintain the following files for purposes of disaster recovery:

- A list of personnel contact information
- A list of Plan Participant contact information
- A list of Business Associate and other vendor contact information
- Instructions to perform recovery operations in the event a disruption, compromise, or loss of ePHI occurs requiring data restoration

The Security Officer will establish an initial temporary operations site in the event of a disaster and obtain the latest backup from the secured offsite storage facility and make any necessary arrangements for compatible hardware.

The Security Officer will take necessary steps to protect the confidentiality of Plan Participant information at the temporary location and at the location of the disaster. The Security Officer will also assist in the planning for resumption of normal business operations and any contingency operations, including the following activities:

- Identifying and documenting contact information for ordering or acquiring alternative equipment, data center space, and personnel immediately following a disaster;
- Implementing a hot or cold site arrangement with an external provider and/or an internal source, as applicable, to meet business requirements; and
- Establishing specific tasks and responsibility of disaster team recovery members and documenting appropriate alternative responsibilities, where appropriate.

3. Emergency Mode Operation

Policy

The Health Plan relies on its third-party administrators, other business associates, or its insurers to manage risks to electronic PHI by limiting vulnerabilities, based on Risk Analyses, to a reasonable and appropriate level, taking into account the following:

- Their size, complexity, and capabilities;
- Their technical infrastructure, hardware, software, and security capabilities;
- The costs of security measures; and,
- The criticality of the electronic PHI potentially affected and the probability of the various risks.

Based on our assessments undertaken as the plan sponsor on behalf of the Plan, and those undertaken by our third-party administrators, other business associates, and/or insurers, we have made a reasoned, well-informed and good faith determination on the implementation of the HIPAA Security Rule that we may rely upon the security measures, other than the measures stated in our Security policies and procedures and our measures as a plan sponsor, our third-party administrators, other business associates, and/or insurers to protect against reasonably anticipated threats and vulnerabilities and to reduce risks to the confidentiality, integrity and availability of electronic PHI. Furthermore, because the Plan has delegated claims and other administration to third parties, it must rely upon those third parties in times of emergency and will coordinate emergency mode operations with those third parties to the extent practical and appropriate.

Procedure

In the event the plan must engage in emergency mode operations, those individuals identified on the **EMERGENCY MODE OPERATIONS TEAM (FORM S-4)** shall coordinate activities with our third-party administrators, other business associates, and/or insurers to assist their emergency mode operations as practical and appropriate.

4. Contingency Plan Testing and Revision Procedures

Policy

Our organization, on behalf of the Plan, will take reasonable and appropriate steps to perform periodic testing of the Plan's data backup plan and/or processes, and other applicable plans ("contingency plans") to assess its sufficiency and determine whether they are accurate and up to date, and by making

necessary revisions on a periodic basis. However, because the Plan has delegated claims and other administration to third parties, it must rely upon those third parties in times of emergency and will coordinate emergency mode operations with those third parties to the extent practical and appropriate.

Procedure

On at least an annual basis, the plan will test its data backup plan and/or processes.

5. Applications and Business Criticality Analysis

Policy

The Plan will create a documented process for defining and identifying the criticality of its information systems applications and the data contained within them in support of the Plan's other contingency plan components.

Procedure

The Plan has limited ePHI within its information systems that is not otherwise duplicated or otherwise created, received, or maintained by its third party partners, including its third-party administrators, other business associates, and/or insurers. However, to the extent that our organization, on behalf of the Plan, creates, receives, transmits, or maintains any ePHI, its email and internet access are its most critical portions of its information system for assisting third party partners in times of contingency operations. However, because the Plan has delegated claims and other administration to third parties, it must rely upon those third parties in times of contingency and has determined based upon a reasoned analysis that it may rely upon those third parties' determinations of critical applications and business operation on the Plan's behalf.

The Plan will periodically re-analyze and document the criticality of its ePHI and ePHI Systems. The purpose of the criticality analysis is to document the impact to the Plan's services, processes, and operating objectives if a disaster or other emergency causes ePHI Systems to become unavailable for a period of time. The criticality analysis will serve as the basis for the prioritization of data backup, disaster recovery, and emergency operations plans for ePHI and ePHI Systems.

G. Evaluation

Policy

Our Organization, on behalf of the Plan, will perform a periodic review (as necessary) to evaluate the extent to which its security safeguards meet the standards set forth in the HIPAA Security Rule. Such a review will be conducted every year.

Procedure

Periodically, the Security Officer will coordinate the resources necessary to evaluate the Plan's security environment and compliance with the HIPAA Security Rule. An Evaluation will also be performed whenever operational or environmental changes occur or a newly recognized risk arises affecting ePHI created, received, transmitted, or maintained by the Plan. The Security Officer may engage other Workforce Members or outside consultants to assist in the Evaluation process. The results of each Evaluation will be documented and retained for six years from the date the Evaluation was created or last in effect, whichever is later.

H. Facility Access Controls

1. Contingency Operations

Policy

If disaster recovery or emergency mode operations are implemented, only personnel who are permitted access (by the Security Officer) in either disaster recovery or emergency mode operation and whose identification has been validated may be permitted to access to ePHI and the physical environment housing ePHI during a disaster or emergency.

Procedure

Only the individuals identified on the **EMERGENCY MODE OPERATIONS TEAM** form (**FORM S-4**) are permitted access to areas housing ePHI when either emergency mode or disaster recovery operations are implemented. The identity of the above individuals will be verified through visual recognition.

2. Facility Security Plan

Policy

Our organization shall protect information assets containing ePHI and shall take measures to physically secure locations where ePHI is housed, including measures to safeguard building exteriors, interiors, and access, and implement safeguards to protect against tampering, theft, terrorist threats, bomb threats, intrusions, severe weather, and failure of services such as plumbing, water, and electricity that may impact the confidentiality, integrity, and accessibility of the Plan's ePHI.

Procedure

Each HIPAA Workforce Member shall be given physical access to the Company's electronic information systems and the facility or facilities in which ePHI is housed in accordance with his or her necessary level of access. Access should be limited sufficiently to afford Plan members as much privacy and security as possible without limiting access so as to interfere with the efficiency of Plan administration.

Our organization, on behalf of the plan, shall take measures to physically secure areas where ePHI is created, received, or maintained, including where appropriate locked doors, key card access, and on duty receptionists.

The Privacy Officer, or his or her designated representative, and the Security Officer shall ensure that applicable access privileges are revoked and that appropriate third parties are notified of the termination or decreased level of access to ePHI. Relevant keys, cards, passwords, or electronic access should be returned or changed, as applicable. Termination of access shall be documented.

3. Access Control and Validation Procedures

Policy

The Company implements policies and procedures to control and validate a person's physical access to highly sensitive and sensitive facilities that house ePHI Systems. Access is based on the person's role or function.

Procedure

Our organization, on behalf of the Plan, will identify all organizational or functional areas considered sensitive due to the nature of the ePHI that is stored or available within them. After identifying sensitive

areas, access rights to such areas should be given only to Workforce Members who have a need for specific physical access in order to accomplish a legitimate task.

HIPAA Workforce Members must immediately report to appropriate management the loss or theft of any device (e.g., card or token) that enables them to gain physical access to such facilities where ePHI is housed or accessed. All access rights to facilities where electronic systems containing ePHI are located or software programs that can access electronic systems containing ePHI must be regularly reviewed and revised as necessary.

4. Maintenance Records

Policy

The Privacy and/or Security Officer shall document repairs, changes, and modifications to the building exteriors, building interiors and physical systems which are related to security for facilities housing electronic systems containing ePHI.

Procedure

The Privacy and/or Security Officer shall maintain a written or electronic log to document changes to, or repair and maintenance of, physical security systems and measures for facilities housing electronic systems containing ePHI. (Use **FORM S-5 FACILITY MAINTENANCE**.) The Security Officer shall authorize any necessary repairs or modifications for the facilities housing electronic systems containing ePHI.

I. Workstation Use

Policy

HIPAA Workforce Members shall limit use of any electronic systems containing ePHI to the purpose for which they are intended.

Our organization maintains physical and technical safeguards for all workstations that access ePHI to restrict access to authorized users.

Procedure

Workstations should only be used for authorized business purposes.

When possible workstations should be placed in secure areas. Workstations should be logged off or locked when not in use. Users must take actions to prevent unauthorized viewing (e.g., privacy screens, minimizing sessions, closing laptops, etc.).

ePHI must be stored on network servers.

Laptops containing ePHI shall be secured by using cable locks or locking laptops in drawers or cabinets or in offices with locked doors when not in use. Laptops containing ePHI shall be encrypted. Workstations shall be positioned to prevent accidental screen viewing. Workstations shall be left on, but logged off, in order to facilitate after-hours updates.

K. Device and Media Control

1. Disposal

Policy

All electronic media that have contained ePHI and are slated for disposal shall either be scrubbed of all data prior to re-use or storage of non-PHI, or be thoroughly destroyed and rendered unusable for purposes of accessing or retrieving PHI.

All destruction/disposal of electronic media containing ePHI will be done in accordance with federal and state laws and regulations and pursuant to our standard retention policy/schedule, as applicable. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.

Procedure

Any media containing PHI should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Some appropriate methods for destroying/disposing of media include the following:

- Electronic Data/Hard Disk Drives, including drives found in printers or copiers.
- The method used for destruction, disposal, or reuse should destroy data permanently and irreversibly.
- Methods of reuse may include overwriting data with a series of characters or reformatting the disk (destroying everything on it) through degaussing or sanitization.
- Electronic Data/ Removable media or devices, including USB drives or SD cards.
- The method used for destruction, disposal, or reuse may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Removable media should be shredded or pulverized when no longer usable.
- Handheld devices including cell phones, smart phones, PDAs, tablets, and similar devices.
- Software capable of remote wiping should be enabled on all handheld devices that are capable of accessing parts of the information system containing ePHI, such as smart phones with access to our organization's email.
- Any removable media that is used by these devices should be handled as described above.
- Handheld devices no longer in use should be completely destroyed by recycling or by trash compacting.
- When destruction is conducted in-house, the Plan should maintain records of destruction/disposal.
- The record of destruction/disposal (such as a certification of destruction) should include the following:
 - Date of destruction/disposal
 - Method of destruction/disposal (e.g., degaussing)
 - Description of the destroyed/disposed record series or medium (e.g., flash drive containing large claim reports)
 - Dates of applicable ePHI (e.g., records from 1/1/2008 through 12/31/2008)
 - A statement that the PHI records were destroyed/disposed of in the normal course of business
 - Signatures of the individuals supervising and witnessing the destruction/disposal
- Use **FORM S-6 CERTIFICATE OF DESTRUCTION**.
- If the Plan contracts with a third party vendor for destruction/disposal services, the contract must meet all applicable Business Associate Agreement (BAA) standards under HIPAA. The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or other agreement should include, but not be limited, to the following:
 - The specific method of destruction/disposal
 - The time that will elapse between acquisition and destruction/disposal of data/media
 - Safeguards implemented by the third party vendor against unauthorized disclosures of PHI
 - Indemnification for the health plan from loss due to unauthorized disclosure of ePHI

- A requirement that the third party vendor will maintain liability insurance in specified amounts at all times the BAA or other agreement is in effect
- Provide proof of destruction/disposal (e.g., a certificate of destruction)
- The Security Officer will periodically reassess methods of destruction, disposal, and reuse, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.

2. Media Re-Use

Policy

All electronic media that have contained ePHI and are slated for re-use shall have the data securely overwritten or the data shall otherwise be rendered inaccessible, cleaned, or scrubbed.

Procedure

Any media containing PHI should be securely overwritten using a method that ensures the PHI could not be recovered or reconstructed. For example, the data may be overwritten through software utilities.

The Security Officer will periodically reassess methods of destruction, disposal, and reuse, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.

3. Accountability

Policy

The Security Officer shall maintain a record of hardware and electronic media containing ePHI, and the names and positions of the persons responsible for using them as a means of maintaining the confidentiality of ePHI.

Procedure

The Security Officer shall create and maintain a log of workstations (laptops and desktops), servers, and personal electronic devices (such as smart phones and tablets) containing ePHI, and the names and positions of the persons responsible for using them as a means of maintaining the confidentiality of ePHI. The log shall be updated each time a change in hardware or personnel occurs or the implementation of new electronic media (e.g., the purchase of a new laptop computer). The log may be maintained in a broader asset management process so long as the information may be extracted for all HIPAA Workforce Members.

4. Data Backup and Storage

Policy

Our organization, on behalf of the Plan, shall maintain processes and procedures to create and maintain retrievable exact copies of ePHI. The policy and procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all information systems used by the Plan.

Procedure

Our organization, on behalf of the Plan, shall take the following steps to create and maintain exact copies of ePHI:

- Perform snapshot backup of network-based ePHI on daily basis after close of business.
- Perform a full backup of network-based ePHI daily during non-regular business hours.
- The backup will be to the cloud.
- The software used to perform the backup will be AWS.
- Email containing ePHI shall be backed up continuously.
- Management is responsible for completing the backups and for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media, and for performing periodic testing of restored media.
- Data backup systems may be manual or automated.
- Automated systems should electronically capture back up locations, date/time, etc.
- If the process is manual, the individual responsible for conducting the backup should document the following:
 - Site/location name
 - Name of the system
 - Type of data
 - Date & time of backup
 - Where backup stored (or to whom it was provided)
 - Signature of individual that completed the back up
- All media used for backing up ePHI shall be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up (i.e., the media should be stored in a location that protects the backups from loss or environmental damage).
- If an off-site storage facility or backup service is used, a Business Associate Agreement must be used to ensure that the Business Associate will safeguard the ePHI in an appropriate manner.
- Stored data must be accessible and retrievable at all times.

L. Access Control

1. Unique User Identification

Policy

It is our policy to safeguard the confidentiality, integrity, and availability of ePHI within our information systems by controlling access to these systems/applications. Access to information systems by all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis.

Procedure

Each HIPAA Workforce Member shall have a unique user identification allowing access to our electronic information system and must use either a unique user name and/or number to access our information system.

2. Encryption and Decryption

Policy

Based on its Risk Analysis, our organization, on behalf of the Plan, shall determine when to implement encryption for ePHI and ePHI Systems and the type and quality of the encryption algorithm and cryptographic key length.

Procedure

Based on the results of the Risk Analysis, the Security Officer shall approve the encryption mechanism used. When encryption is used, our organization on behalf of the Plan shall:

- Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure;
- Implement a documented process for managing the cryptographic keys used to encrypt ePHI stored or maintained on ePHI System; and
- Periodically determine activation and deactivation dates for its cryptographic keys.

3. Emergency Access Procedure

Policy

In the event that emergency access to ePHI is necessary, the Security Officer (or his or her designated employee) shall determine who may be granted access.

Procedure

In order to gain access to ePHI in an emergency situation, an individual must contact the Security Officer, or his or her designated staff member.

4. Automatic Lockout

Policy

The Security Officer will determine when it is not reasonable or appropriate to implement electronic automatic logoff mechanisms on certain ePHI Systems and will approve equivalent alternative mechanisms (e.g., screen/session locking, screensaver implemented after period of time).

Procedure

When feasible, electronic sessions will be terminated and Workforce Members will be logged/locked out of our information system after no less than 15 minutes and no more than eight hours as configured under Administrative Settings > Security Policies, requiring the user to be identified and authenticated again in order to regain access and continue the session.

M. Person or Entity Authentication

Policy

Our organization, on behalf of the Plan, shall maintain procedures to verify that a person or entity seeking access to ePHI is the person or entity claimed.

Procedure

Users seeking access to the information systems network, including through remote access, must provide a unique user ID and password. All workforce members are assigned a unique User ID to access our organization's network and are responsible for creating and maintaining the confidentiality of the passwords associated with their unique User IDs.

N. Audit Controls (Activity Logs)

Policy

The Security Officer shall periodically conduct an audit or review of safeguards implemented to protect ePHI. The Security Officer shall implement and maintain necessary logs to document periodic review/auditing.

Procedure

The Security Officer shall implement and maintain one or more of the following (as necessary):

- A user access log
- A user activity log
- A log to monitor user access control configurations
- An administrator access log
- An administrator activity log
- A log of user privilege authorizations
- A log of software configuration changes
- A log of changes to operating and application software (including updates, upgrades, and patches)
- An exception report log (e.g., abnormal failed access attempts to our information system, etc.)
- A data backup and storage log
- A hardware user log

When not tracked electronically, the Security Officer or the Security Officer's designee will document the review using **FORM S-7 SYSTEM AUDIT LOG**.

O. Transmission Security

1. Integrity Controls

Policy

The Plan will take reasonable and appropriate steps to implement electronic mechanisms to prove that ePHI has not been altered or destroyed in an unauthorized manner, including: (1) which ePHI will be authenticated and (2) which electronic mechanisms would be reasonable and appropriate.

Procedure

The Security Officer will approve the electronic mechanisms that have been implemented to protect ePHI from unauthorized alteration or destruction and to authenticate the integrity of ePHI, such as use of methods of transmission of ePHI through our own organization's or a third-party administrator's, other business associates', or insurers' encrypted or secure email or secure third-party website. Where feasible and appropriate, our organization, on behalf of the Plan, will encrypt ePHI at rest.

In the event improper destruction or alteration of ePHI is detected, the Plan will activate its security incident procedures and take corrective action, including sanction workforce members, as necessary.

2. Encryption

Policy

Based on its Risk Analysis, our organization, on behalf of the Plan, shall determine when to implement encryption for ePHI and ePHI Systems and the type and quality of the encryption algorithm and cryptographic key length.

Procedure

Based on the results of the Risk Analysis, the Security Officer shall approve the encryption mechanism used. When encryption is used, our organization, on behalf of the Plan, shall:

- Protect its cryptographic keys against modification and destruction, and protect its private keys against unauthorized disclosure;
- Implement a documented process for managing the cryptographic keys used to encrypt ePHI stored or maintained on ePHI Systems; and
- Periodically determine activation and deactivation dates for its cryptographic keys.