HIPAA Privacy and Security Policy

[**Form Summary**: Use this HIPAA Privacy and Security Policy for a group health plan to satisfy the regulatory requirement that it set forth the written policies and procedures that it will follow to ensure its compliance with the privacy, security and breach notification requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 45 C.F.R. § 164.530(i). This form contains practical guidance and drafting notes.

For information on the HIPAA privacy rule, see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—What Safeguards, Policies, and Procedures Are Needed for Privacy Rule Compliance? [ADD LINK] For an additional discussion about HIPAA, see HIPAA Resource Kit [ADD LINK].]

HIPAA PRIVACY AND SECURITY POLICY

[date]:

_____

Table of Contents

A. Access to Protected Health Information and Requests for Amendment
B. Accounting
C. Requests for Request Confidential Communications
D. Requests for Restrictions on Uses and Disclosures of PHI
E. Requests for Amendment

HIPAA PRIVACY AND SECURITY POLICY
[Company name]
[Plan name]
Introduction

[Plan sponsor name] (the "Company") sponsors and is involved in [certain elements of] the [plan name(s)], a group health plan offering various benefits to participating employees and their dependents (the "Plan"). The various benefit plans comprising the Plan, along with the third-party administrators, insurers and managed care organizations involved with the Plan, constitute a single "organized health care arrangement", so that the policies set forth in this Policy apply to each such plan.

[Drafting Note to First Paragraph: The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of protected health information (PHI), and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. Most group health plans (other than hands-off plans (i.e., fully-insured plans not allowing PHI to flow to the plan sponsor except for summary health information and participation and enrollment data)) must satisfy the Privacy Rule standards listed below. 45 C.F.R. § 164.530(k). The group health plan must implement and maintain up-to-date written policies and procedures setting forth in detail privacy and security practices reasonably designed to ensure compliance with the Privacy Rule, taking into account the size and type of activities relating to PHI undertaken by the plan. The group health plan should change these policies as necessary to comply with legal changes. The privacy policies and procedures provide detailed instructions for those members of the employer's workforce tasked with handling PHI. 45 C.F.R. § 164.530(i). Customize the first paragraph further if the plan sponsor maintains other plans that are separate from the Plan but are subject to the HIPAA rules (i.e., they do not constitute "excepted benefits"). See ERISA § 732(b) (29 U.S.C. § 1191a(b)) and ACA and HIPAA Excepted Benefits [ADD LINK].]

[**Alternate First Paragraph (for Company with Affiliates That Participate in the Group Health Plan)**: [Plan sponsor 's name] (the "Company") sponsors for the Company and its Affiliated Group (as defined below)] a group health plan offering various benefits (the "Plan"). The various benefit plans comprising the Plan, which include [name of other Company-sponsored benefit plans subject to HIPAA] along with the third-party administrators, insurers and managed care organizations involved with the Plan, constitute a single "organized health care arrangement", so that the policies set forth in this Policy apply to each such plan or program. The term "Plan" used herein is intended to refer to all the underlying plans, referenced above, unless otherwise specifically delineated. References to Company obligations and procedures therefore encompass the Affiliate Group as well as the Company.]

[Drafting Note to Alternate First Paragraph (for Company with Affiliates That Participate in the Group Health Plan): Use this Alternate First Paragraph where the plan sponsor has an affiliated group that participates in the group health plan and any other benefit plan that is not an excepted benefit (like a stand-alone dental plan) under

ERISA § 732(b) (29 U.S.C. § 1191a(b)). For a discussion about excepted benefits, see ACA and HIPAA Excepted Benefits [ADD LINK].]]

Members of the Company's workforce may have access to the "protected health information" (as described below) of Plan participants (1) on behalf of the Plan itself, or (2) on behalf of the Company, for plan administrative functions. The Company intends to fully comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, as amended, as administered by the United States Department of Health and Human Services (HHS), including the HIPAA Privacy Rule and the HIPAA Security Rule (HIPAA Privacy Rule and HIPAA Security Rule, respectively). HIPAA restricts the Company's use and disclosure of "protected health information", as well as the use and disclosure of "protected health information" by its "business associates" and insurers.

[**Drafting Note to Second Paragraph:** The HIPAA Privacy Rule is set forth in 45 C.F.R. § 164.500-534. The HIPAA Security Rule is set forth in 45 C.F.R. § 164.306. The HIPAA Privacy Rule requires that a group health plan:

- Provide individuals with a notice of privacy practices. 45 C.F.R. § 164.520.
- Adopt appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and implement policies and procedures designed to comply with the Privacy Rule standards. 45 C.F.R. §§ 164.530(c)-(j).
- Designate a privacy officer to develop and implement the PHI policies and procedures. 45 C.F.R. § 164.530(a).
- Train workforce members on the PHI policies and procedures. 45 C.F.R. § 164.530(b).
- Use or disclose PHI only in accordance with the Privacy Rule standards. 45 C.F.R. §§ 164.502, 164.506, 164.508, 164.510, 164.512, 164.514.
- Ensure that all business associates are covered by a compliant business associate agreement. 45 C.F.R. § 164.504(e).
- Grant individuals the right to access their PHI, to amend incorrect PHI, and to receive an accounting of most PHI disclosures. 45 C.F.R. § 164.522, 45 C.F.R. § 164.524, 45 C.F.R. § 164.526, 45 C.F.R. § 164.528.

The HIPAA Security Rule generally requires covered entities and business associates to ensure the confidentiality, integrity, and availability of all electronic (ePHI) that they create, receive, maintain, or transmit. Specifically, they must:

- Protect against any reasonably anticipated threats or hazards to the security or integrity of any PHI that is maintained or transmitted in electronic form
- Protect against any reasonably anticipated unauthorized uses or disclosures of such information, and
- Ensure compliance with the Security Rule by its workforce.

45 C.F.R. § 164.306.]

"Protected health information" ("PHI") means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. PHI includes information concerning persons living or deceased. The Security Rule governs

electronically conveyed PHI, or "E-PHI." ("PHI" herein includes "E-PHI" unless "E-PHI" is specified.) Special aspects of Security Rule compliance are addressed at II-L, below.

PHI does NOT include individually identifiable health information which may be contained in employment records, such as sick leave, family leave, disability and other such records obtained from employees directly or from other sources than the Plan, in connection with those personnel matters. However, PHI from the above HIPAA group health plans may NOT be used in personnel matters, without written consent of the individual. Also, although PHI does not include individually identifiable health information that is generated and used in connection with other Company benefits outside the Plan, including LTD insurance and workers' compensation insurance, the Company may NOT utilize PHI from the above HIPAA plans in connection with administration of non-HIPAA benefits, EXCEPT for required workers compensation disclosures.

The Company has adopted this Privacy Policy and the Company's separate HIPAA Use and Disclosure Procedures regarding the use and disclosure of PHI and individuals' rights relating to their PHI. All members of the Company's workforce who have access to PHI must comply with this Privacy Policy and the Company's HIPAA Use and Disclosure Procedures. Individuals who would be considered part of the Company's workforce under HIPAA are employees, independent contractors, volunteers, trainees, and other persons whose work performance is under the direct control of the Company, whether or not they are paid by the Company. The term "employee" herein includes all of these types of workers.

As further set forth in the Use and Disclosure Procedures, the Company adopts as a policy that all claims and benefit issues arising in any of the Company's locations shall be referred to the Contact Person (or Privacy Official or Security Official where specifically designated in this Policy or the Use and Disclosure Procedures) for resolution. Therefore, any human resources personnel receiving inquiries regarding claims or benefits or any other questions regarding the Plan, the Notice of Privacy Practices or any related issue, shall not attempt to answer or address such inquiries, but shall refer such inquiries to a Contact Person, or Privacy or Security Official, as is specifically designated.

I. Plan Responsibilities as Covered Entity

A. Privacy Official and Contact Person

[Name and title] will be the Privacy Official for the Plan. The Privacy Official will be responsible for the administration of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's HIPAA Use and Disclosure Procedures.

The Privacy Official has designated [name and title], as the contact person ("Contact Person") for all regular and routine matters, as set forth herein. The Contact Person will serve as the person available to participants who have questions, concerns, or complaints about their PHI, as specified in the Notice of Privacy Practices and as further detailed in the Use and Disclosure Procedures.

[Drafting Note to A. Privacy Official and Contact Person: As discussed below in "E. Privacy Notice" the group health plan must appoint a privacy official who is responsible for the development and implementation of the Company's HIPAA privacy policies and procedures and designate a contact person or office for receiving complaints under the Privacy Rule. 45 C.F.R. § 164.530(a).]

B. Security Official and Contact Person

[**Drafting Note to B. Security Official and Contact Person Paragraph**: The Security Rule sets forth standards for the protection of ePHI in the following areas: (1) administrative safeguards, (2) physical safeguards, (3) technical safeguards, (4) organizational requirements, and (5) policies and procedures. One required implementation specification for administrative safeguards requires plans to designate a security official responsible for the development and implementation of the security rule policies and procedures 45 C.F.R. § 164.308(a)(2). For a board resolution to appoint a HIPAA Security Official (which also may be used to appoint a HIPAA Privacy Official) see Board Resolutions: HIPAA Privacy and Security Officer Appointment [ADD LINK].]]

[Name and title], will be the Security Official. The Security Official will serve as the person available for any issues of a technical nature specific to the HIPAA Security implementation specifications.

[**Drafting Note to B. Security Official and Contact Person First Paragraph**: Since HIPAA security deals with ePHI, you may suggest that the plan sponsor designate an individual (or position title) of an individual in its Information Technology (IT) group for this position. It can also be the Privacy Official.]

[Name and title], will serve as Contact Person for Privacy and Security Rule regular and routine matters.

[**Drafting Note to B. Security Official and Contact Person Second Paragraph**: In larger organizations, it's common to designate a contact person who is responsible for routine issues who is a different individual than the named Security Official.]

C. Persons with Access; Workforce Training.

It is the Company's policy to limit access to PHI to those who have need and to train employees who have access to PHI on its privacy and security policies and procedures. The Privacy Official, Security Official and Contact Person will develop training schedules and programs so that employees who have access to PHI (including E-PHI) receive the training necessary and appropriate to permit them to carry out their functions within Plan. Initially, the Company has determined that the following positions (and their incumbents) will have access to PHI and will receive training: (hereinafter "Persons With Access"): [list PWAs; use position titles with names]. The Security Official will arrange supplemental training of Persons with Access in elements of Security Rule compliance.

[Drafting Note to C. Persons with Access; Workforce Training: The HIPAA Privacy Rule requires a group health plan (or other covered entity) to train workforce members on the plan's PHI policies and procedures. 45 C.F.R. § 164.530(b). For a sample training presentation, see HIPAA Privacy and Security Training Presentation [ADD LINK].]

D. Technical and Physical Safeguards and Firewall

[**Drafting Note to D. Technical and Physical Safeguards and Firewall:** The Security Rule sets forth standards for the protection of ePHI in the following areas: (1) administrative safeguards, (2) physical safeguards, (3) technical safeguards, (4) organizational requirements, and (5) policies and procedures. Section D sets forth the second and third rung of these requirements within a HIPAA privacy and security policy. See 45 C.F.R. §§ 164.310(a)-(d),

164.312(a)-(e). For more information on the HIPAA Security Rule, see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—What Does the HIPAA Security Rule Require? [ADD LINK]]

An analysis of all the Company's information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. The analysis will examine the types of threats—internal or external, natural or manmade, electronic and non-electronic—that affect the ability to manage the information resource. The analysis will also document the existing vulnerabilities within each entity which potentially expose the information resource to the threats. Finally, the analysis will also include an evaluation of the information assets and the technology associated with i*ts collection, storage, dissemination and protection. From the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity and availability of the information will be determined*. Based on the periodic assessment, measures will be implemented that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities.

All computer equipment and network systems are assets of the Company and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based on the following:

- **Installed Software:** All software packages that reside on computers and networks within the Company must comply with applicable licensing agreements and restrictions and must comply with the Company's acquisition of software policies.
- **Virus Protection:** Virus checking systems approved by the Security Official and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.
- **Access Controls:** Physical and electronic access to PHI is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Security Official and approved by the Company. Mechanisms to control access to PHI include (but are not limited to) the following methods:
    1. **Authorization:** Access will be user-based access whereby users of a system gain access based upon the identity of the user.
    2. **Identification/Authentication:** Unique user identification (user id) and authentication is required for all systems that maintain or access PHI. Users will be held accountable for all actions performed on the system with their user id.
        a. Authentication shall be by **strictly** controlled passwords.
        b. The user must secure his/her authentication control (e.g. password) such that it is known only to that user and possibly a designated security manager.
        c. An automatic timeout re-authentication must be required after a certain period of no activity.
        d. The workstation must freeze after three unsuccessful attempts to gain access.
        e. The user must log off or secure the system when leaving it.
    3. **Transmission Security:** Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features will be implemented:
        a. Encryption shall be utilized for emails where electronic PHI is transmitted.
        b. Benefits personnel shall use facsimile or telephone contact with the third-party administrator to the Plan when dealing with electronic PHI in claims assistance.

4. **Remote Access:** Access into the Company's network from outside will be granted using the Company approved devices and pathways on an individual user and application basis. All remote access to systems which may access electronic PHI shall be made using a "virtual private network". All other network access options to these systems are strictly prohibited.
5. **Physical Access:** Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

   The following physical controls must be in place:
   a. Mainframe computer systems must be installed in an access-controlled area.
   b. File servers containing PHI must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
   c. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. The following policies regarding workstation use and physical safeguards are instituted:
      (1) Position workstations to minimize unauthorized viewing of protected health information.
      (2) Grant access to systems which may access electronic PHI only to those who need it in order to perform their job function.
      (3) Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to PHI.
      (4) Use automatic screen savers with passwords to protect unattended machines.
   d. Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.
      (1) Facility Security Plan—Procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
      (2) Access Control and Validation—Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.
      (3) Maintenance records—Procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

6. **Employee Hiring and Departures:**
   a. The Company shall maintain its existing clearance procedures regarding the hiring of employees.
   b. The Company shall maintain its existing procedures regarding departing employees, which include promptly deactivating system access and recovering ID cards, remote access devices and other access items.

7. **Security Updates:** The Company will provide periodic updates as appropriate, including security reminders regarding access security, virus protection and maintaining password protection.

- **Equipment and Media Controls:** The disposal of information must ensure the continued protection of PHI. The receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility shall be documented by Information Services personnel. The Company will maintain a record of the movements of hardware and electronic media and any person

responsible therefor. PHI must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PCs, etc.) unless the devices have the following minimum security requirements implemented:

a. Power-on passwords
b. Auto logoff or screen saver with password
c. Encryption of stored data or other acceptable safeguards approved by the Security Official
d. Mobile computing devices must never be left unattended in unsecured areas

- **Data Transfer/Printing:** PHI must be stored in a manner that is inaccessible to unauthorized individuals. PHI must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

- **Oral Communications:** Company staff should be aware of their surroundings when discussing PHI. This includes the use of cellular telephones in public areas. Company staff should not discuss PHI in public areas if the information can be overheard. Caution should be used when conducting conversations in: semi-private rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation.

- **Audit Controls:** Logs that record and examine activity in information systems that contain or use PHI will be maintained. Records of information system activity will be reviewed weekly and available for review should a security incident have occurred or be suspected.

- **Evaluation:** The Company shall undertake periodic technical and non-technical evaluations in response to environmental or operational changes affecting the security of electronic PHI to ensure its continued protection.

- **Contingency Plan:** Controls must ensure that the Company can recover from any damage to computer equipment or files within a reasonable period of time. The Company will create and maintain, for a specific period of time, retrievable exact copies of information. Certain backup data must be stored in an off-site location and protected from physical damage.

E. Privacy Notice

[**Drafting Note to E. Privacy Notice:** Individuals have a right under HIPAA to receive a written notice describing (1) the uses and disclosures of PHI that may be made by a group health plan or other covered entity, (2) the individuals' rights regarding PHI, and (3) the covered entity's legal duties with respect to PHI. 45 C.F.R. § 164.520(a)(1). The notice must be written in plain language and contain the elements set forth in the following subsections. HHS provides various forms of model notices for plans and for health care providers on its website. For a sample annotated HIPAA notice, see HIPAA Notices of Privacy Practices [ADD LINK]. For more information on the HIPAA Privacy Notice, see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—What are the Notice Obligations under the HIPAA Privacy Rule [ADD LINK].]

The Privacy Official will maintain the Plan's Notice of the Privacy Practices that describes the uses and disclosures of PHI that may be made by the Plan; the individual's rights with respect to use and disclosure of PHI; and the Plan's legal duties with respect to the PHI.

[**Drafting Note to E. Privacy Notice First Paragraph:** Just as group health plans must identify a Security Official, they also must identify a Privacy Official. The plan must appoint a privacy official who is responsible for the development and implementation of the privacy policies and procedures and designate a contact person or office for receiving complaints under the Privacy Rule. 45 C.F.R. § 164.530(a). For a board resolution to appoint a HIPAA Privacy Official (which also may be used to appoint a HIPAA Security Official) see Board Resolutions: HIPAA Privacy and Security Officer Appointment [ADD LINK].]]

The Notice informs participants that the Company and certain third parties as described therein (insurers and third-party administrators) will have access to PHI in connection with Plan administrative functions. The Notice also provides details of the Company's complaint procedures specifically for HIPAA Privacy and Security, the name and telephone number of the Privacy Official, Contact Person and Security Official for further information and assistance; and the date of the notice, among other elements.

The Notice of Privacy Practices was individually delivered to all participants no later than April 14, 2003. The Notice is delivered on an ongoing basis after April 14, 2003 at the time of an individual's enrollment in the Plan; and within 60 days after a material change to the Notice, including the addition of a Security Official. The Plan also calls for availability of the Notice at least once every three years.

F. Complaints

The Contact Person is responsible for administering a process for individuals to lodge complaints about the Plan's privacy and security procedures. A copy of the complaint procedure shall be provided to any participant upon request.

[**Drafting Note to F. Complaints:** The HIPAA Privacy Notice must set forth detailed information on how privacy complaints are handled, such as a claim of purported breach or unauthorized disclosure of an individual's PHI. The notice must include a statement that retaliation for making a complaint is prohibited. 45 C.F.R. § 164.520(b)(1)(vi), (vii). Individuals also can file a health information privacy or security complaint with HHS's Office for Civil Rights (OCR). The complaint must:

- Be filed in writing by mail, fax, e-mail, or via the OCR Complaint Portal
- Name the covered entity or business associate involved, and describe the acts or omissions, you believed violated the requirements of the Privacy, Security, or Breach Notification Rules
- Be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause"

An entity cannot retaliate against you for filing a complaint. You should notify OCR immediately in the event of any retaliatory action. For a further discussion on the HIPAA enforcement process, see HIPAA Enforcement and Penalties [ADD LINK TO TASK 2529].]

G. Sanctions for Violations of Privacy and Security Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy and Security Policy will be imposed in accordance with the Company's discipline policy.

H. Mitigation of Inadvertent Disclosures of Protected Health Information

The Company 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 this Policy. As a result, if an employee becomes aware of a disclosure of PHI that violates this Policy, either by an employee of the Plan or a third-party administrator or insurer, the employee may contact the Privacy Official so that the appropriate steps can be taken to mitigate the harm to the participant. (*See* "Use and Disclosure Procedures".)

I. Breach Notification Requirements

[Drafting Note to I. Breach Notification Requirements: see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—What Does the HIPAA Breach Notification Rule Require? [ADD LINK]

The Plan will comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") and its implementing regulations with respect to notifications in the event of a breach of unsecured PHI. As a result, if an employee becomes aware of a potential breach of unsecured PHI, the employee shall contact the Privacy Official. Promptly after a report of suspected breach of unsecured PHI, the Privacy Official shall direct and undertake an investigation and risk assessment to determine if a breach of unsecured PHI occurred and the scope of such breach. There is a reportable breach only if all of the following have occurred, as determined by the Privacy Official:

- There is a violation of the HIPAA Privacy Rules involving "unsecured" PHI.
- The violation involved unauthorized access, use, acquisition, or disclosure of unsecured PHI.
- The violation resulted in a compromise of the security or privacy of the PHI.
- No exception applies under applicable law.

If the Privacy Official determines that there is a low probability that the PHI was compromised, the Plan will document the determination in writing and keep the documentation on file.

The Plan shall, following the discovery of a breach of unsecured PHI that is required to be reported, notify each individual whose unsecured PHI has been, or is reasonably believed by the Plan to have been, accessed, acquired, used, or disclosed as a result of such breach as well as the Secretary of HHS.

[**Drafting Note to Third Paragraph of "I. Breach Notification Requirements":** The requirement derives from regulatory requirements. 45 C.F.R. § 164.404. For a sample letter to an individual reporting a breach of the individual's (or one or more individuals') PHI, see HIPAA Breach Notice (Individual) [ADD LINK].]

For a breach of unsecured PHI involving 500 or more residents of a state or jurisdiction, the Plan shall notify prominent media outlets serving the state or jurisdiction.

[**Drafting Note to Fourth Paragraph of "I. Breach Notification Requirements":** The requirement derives from regulatory requirements. 45 C.F.R. § 164.406. For a sample letter to the media reporting a breach of the individual's (or one or more individuals') PHI, see HIPAA Breach Notice (Media) [ADD LINK].]

For a breach of unsecured PHI involving 500 or more individuals, the Plan shall notify the Secretary of HHS contemporaneously with the notice to affected individuals and in the manner specified on the HHS website.

The above notices shall be provided without unreasonable delay and in no case later than 60 days after discovery of the breach and shall comply with the requirements of the HITECH Act and its implementing regulations with respect to the content and method of notification.

[**Drafting Note to Fifth Paragraph of Section I "Breach Notification Requirements":** The requirement derives from regulatory requirements. 45 C.F.R. § 164.408.

A business associate is required to do the same.

[**Drafting Note to Sixth Paragraph of Section I "Breach Notification Requirements":** A business associate is required to notify the plan without unreasonable delay and in no case later than 60 days after discovery of a breach. 45 C.F.R. § 164.410(b). The business associate agreement should be written to make this requirement clear and to indicate whether the covered entity or the business associate is primarily liable for the notification. You may wish to provide a right to review the communication before it is delivered to affected individuals.]

Breach Notification Definitions

- *Breach*. The acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA and its implementing regulations which compromises the security or privacy of the PHI. If an unauthorized use or disclosure of PHI occurs, the security or privacy of PHI is presumed to have been compromised unless the Plan demonstrates that there is a low probability that the PHI has been compromised. This determination is made through a risk assessment of at least the following factors:
  (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  (ii) The unauthorized person who used the PHI or to whom the disclosure was made;
  (iii) Whether the PHI was actually acquired or viewed; and
  (iv) The extent to which the risk to the PHI has been mitigated.

  A use or disclosure of PHI that does not include the identifiers listed at 45 CFR § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.
  Breach excludes:

  (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA and its implementing regulations.
  (ii) Any inadvertent disclosure by a Person with Access and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA and its implementing regulations.
  (iii) A disclosure of PHI where the Plan has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- *Unsecured PHI*. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS in the guidance issued under Section 13402(h)(2) of the HITECH Act on the HHS website.

J. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy and Security

No employee 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 HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

K. Plan Documents

The Plan Documents include provisions to incorporate descriptions, as set forth in the Use and Disclosure Procedures, of the permitted and required uses and disclosures of PHI by the Company for Plan administrative purposes. Specifically, the Plan Documents require the Company 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 the Company;
- not use or disclose PHI for employment-related actions or in connection with any other employee benefit plan (except those within the Company's "organized health care arrangement" or among the affiliated companies, required disclosures for workers' compensation purposes and the reallocation of employee claims from the Plan to workers' compensation, as appropriate);
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures;
- make the Company's internal practices and records relating to the use and disclosure of PHI received from the Plan available to HHS upon request; and
- if feasible, return or destroy all PHI received from the Plan that the Company 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.

The Plan Documents as amended also require the Company to (1) certify that the Plan Documents have been amended to include the above restrictions and that the Company agrees to those restrictions; (2) provide adequate firewalls; and (3) provide the administrative, physical and technical safeguards (including written policies and procedures) that reasonably protect the confidentiality, integrity and availability of electronic PHI it creates, receives, maintains, or transmits.

For these purposes, "Plan Documents" mean the documents of the Plan.

L. Documentation and Document Retention

The Plan's and the Company's privacy policies and procedures must be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must promptly be documented.

If a change in law impacts the Notice, the Notice must promptly be revised and made available to the necessary parties. Such change is effective only with respect to PHI created or received after the effective date of the Notice. The Plan and the Company shall document certain events and actions (including authorizations, requests for information, sanctions, complaints) relating to an individual's privacy rights, as further set forth in the Use and Disclosure Procedures. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years, beginning with documents created on or after April 14, 2003.

II. Policies on Use and Disclosure of PHI

[Drafting Note to Section II. Policies on Use and Disclosure of PHI: For a discussion on the permitted disclosures of PHI, see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—How Can PHI Be Used or Disclosed under the Privacy Rule? [ADD LINK]

A. Use and Disclosure Defined

The Company and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use*. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any Persons with Access of the Company, by the Insurers for the fully insured benefits as set forth in the Notice, or by a Business Associate (defined below) of the Plan.
- *Disclosure*. For information that is PHI, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons who are not Persons with Access of the Company.

B. Workforce Must Comply with Company's Policy and Procedures

HIPAA Use and Disclosure Procedures are set forth in a separate document.

[Drafting Note to Section II. Policies on Use and Disclosure of PHI, Subsection B. Workforce Must Comply with Company's Policy and Procedures: You can reference the HIPAA Use and Disclosure Procedures at HIPAA Use and Disclosure Procedures. [ADD LINK TO LEXIS FORM 49.02-3]

C. Access to PHI is Limited to Certain Employees

As set forth in Article II, above, only the Persons with Access shall have regular and recurring access to and use of PHI.

Persons with Access may use and disclose PHI for Plan administrative functions, and they may disclose PHI to other Persons with Access for Plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the Plan administrative function). Persons with Access may not generally disclose PHI to employees (other than other Persons with Access) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy and the Company's HIPAA Use and Disclosure Procedures.

D. Permitted Uses and Disclosures: Payment and Health Care Operations

[**Drafting Note to D. Permitted Uses and Disclosures: Payment and Health Care Operations:** Except with respect to uses or disclosures that require an authorization under 45 C.F.R. § 164.508(a)(2)-(4) or that are prohibited under 45 C.F.R. § 164.502(a)(5)(i), a covered entity may use or disclose PHI for treatment, payment, or health care operations. 45 C.F.R. § 164.506.]

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

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. Payment also includes: eligibility and coverage determinations, including coordination of benefits and adjudication or subrogation of health benefit claims; risk adjusting based on enrollee status and demographic characteristics; and billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity, administrator or insurer, for purposes of the other 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 participant and the PHI requested pertains to that relationship. (*See* Article X, *below,* regarding disclosures to "business associates".)

Health Care Operations. Health care operations means any of the following activities to the extent that they are related to Plan administration: conducting quality assessment and improvement activities; reviewing health plan performance; underwriting and premium rating; conducting or arranging for medical review, legal services and auditing functions; business planning and development; reallocating employee claims from the Plan to workers' compensation, as appropriate; and general administrative activities. Information may be disclosed to another health plan maintained by the Company [or a member of the Affiliate Group] for purposes of facilitating claims payments under that plan and shared between the constituent health plans comprising the Plan.

E. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Company's "non-health" benefits except required workers' compensation disclosures (*e.g.,* long-term disability, family and medical leave, life insurance,

etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required by applicable state law and particular requirements under HIPAA are met.

PHI may not be used or disclosed for personnel purposes or administration of benefits not within the Plan (except workers' compensation-required disclosures), unless the participant has provided an authorization for such uses and disclosure (as discussed in "Disclosures Pursuant to an Authorization.")

[Drafting Note to E. No Disclosure of PHI for Non-Health Plan Purposes: An employer can ask an employee for a doctor's note or other health information if they need the information for sick leave, workers' compensation, wellness programs, or health insurance. However, the employer cannot ask the health care provider directly for information about the employee without employee authorization unless other laws require them to do so. 45 C.F.R. §§ 160.103, 164.512(a), (b)(1)(v).]

F. Mandatory Disclosures of PHI to Individual and HHS

A participant's PHI must be disclosed as required by HIPAA in two situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Health Information and Requests for Amendment", below); and
- The disclosure is made to HHS for purposes of enforcing HIPAA.

G. Permissive Disclosures of PHI for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Company's HIPAA "Use and Disclosure Procedures" will describe specific requirements that must be met before these types of disclosures may be made, including prior approval of the Company's Privacy Official. The permissive disclosures are:

- about victims of abuse, neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- about crime on Company premises;
- for cadaveric organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

[Drafting Note to G. Permissive Disclosures of PHI for Legal and Public Policy Purposes: 45 C.F.R. § 164.512(b).]

H. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. The Contact Person will have a supply of the authorization form.

[Drafting Note to H. Disclosures of PHI Pursuant to an Authorization: Except as otherwise permitted or required by the HIPAA rules, a covered entity may not use or disclose PHI without a valid signed authorization. 45 C.F.R. §§ 164.502(a)(1)(iv), 164.508. For a discussion of those rules, see HIPAA Privacy, Security, Breach Notification and Other Administrative Simplification Rules—What Safeguards, Policies, and Procedures Are Needed for Privacy Rule Compliance? [ADD LINK]] For a sample authorization form, see HIPAA Authorization for PHI Use or Disclosure [ADD LINK].]

I. Complying with the "Minimum-Necessary" Standard

[**Drafting Note to I. Complying with the Minimum Necessary Standard**: "All covered entities and business associates must limit the PHI they use or disclose (or request to be used or disclosed) to the minimum amount necessary to accomplish the intended purpose. 45 C.F.R. §§ 164.502(b), 164.514(d). This minimum necessary standard does not apply to:

- Disclosures requested or authorized by the individual
- Disclosures required by law or to comply with the Privacy Rule –or–
- Uses or disclosures by a health care provider for treatment.

45 C.F.R. § 164.502(b)(2).

Compliance with the minimum necessary standard requires the covered entity or business associate to (1) identify those persons or classes of persons in its workforce who need access to PHI to carry out their duties, (2) identify the specific PHI needed by each such person or class and any conditions appropriate to their access of the relevant PHI, and (3) make reasonable efforts to limit the access of PHI to the appropriate workforce members accordingly. 45 C.F.R. § 164.514(d)(2).]

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure, as determined by the Privacy Official case-by-case, or, in the instance of routine and recurring disclosures, as set forth in the Uses and Disclosures Policy.

The "Minimum Necessary" Standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the DOL;
- uses or disclosures required by law;
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making routine and recurring disclosures of PHI, the Company's HIPAA "Use and Disclosure Procedures" will establish specific procedures. For routine and recurring disclosures

developing prospectively, the Privacy Official (or Contact Person if directed by the Privacy Official) will direct an analysis of such disclosures and further, specific standards will be developed.

All other disclosures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from [*list insurers and TPAs*] for purposes of claims, claims reports, stop loss insurance and other payment and health care operations, the Use and Disclosure Procedures will outline policies and procedures designed to limit the amount requested to the amount reasonably necessary to accomplish the purpose for which the disclosure is requested.
All other requests must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

J. Disclosures of PHI to Business Associates

Persons with Access may disclose PHI to the Plan's business associates and allow the Plan's business associates to create or receive PHI on its behalf. However, prior to doing so, the Plan must first obtain assurances from the business associate (in the form of business associate agreements) that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate", employees must contact the Contact Person and verify that a business associate agreement is in place.

[Drafting Note to J. Disclosure of PHI to Business Associates First Paragraph: For agency discussion on using business associates while complying with the HIPAA Privacy and Security Rules, see HSS, Business Associates.]

A "Business Associate" is an entity or person who:

- performs or assists in performing a Plan function or activity involving the use and disclosure of protected health information (including claims processing or administration; data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to the Plan, where the performance of such services involves giving the service provider access to protected health information.

[Drafting Note to J. Disclosures of PHI to Business Associates Second Paragraph: The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate. 45 C.F.R. §§ 164.502(e), 504(e), 532(d), (e). For a sample business associate agreement, see HIPAA Business Associate Agreement [ADD LINK]. For a separate business associate policy which you can append to the HIPAA Privacy and Security Policy, see HIPAA Business Associate Policy [ADD LINK].]

K. Disclosures of De-identified Information and Limited Data Sets

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. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers under HIPAA.

[Drafting Note to K. Disclosures of De-identified Information and Limited Data Sets: The specific identifiers relating to the individual (or relatives, employers, or household members of the individual), such as names; geographic location at or below the level identified by the first three digits of a five-digit ZIP code; age; dates of birth, death, and other identifying events; telephone numbers; Social Security numbers; biometric data; and email and internet protocol addresses. Alternatively, information determined by professional statistical analysis to be de-identified can qualify. In either case, there can be no reasonable basis to believe that the information could be used to identify the individual. 45 C.F.R. §§ 164.502(d), 164.514.]

L. Policies Specific to E-PHI/Security Rule

The Company has performed a risk analysis and assessment and developed a document called the HIPAA Security Risk Analysis and Assessment document, including recommended administrative, physical and technical safeguards that reasonably protect the confidentiality, integrity and availability of electronic PHI the Company creates, receives, maintains or transmits.

[List specific administrative, physical and technical safeguards as suggested by Security Rule Evaluation and Assessment document.]

[Drafting Note to L. Policies Specific to E-PHI/Security Rule: Plans must implement policies and procedures to prevent, detect, contain, and correct security violations as part of its administrative safeguards. 45 C.F.R. § 164.306. The four implementation specifications are all required: (1) risk analysis to identify risks to ePHI, (2) risk management to reduce identified vulnerabilities, (3) a sanctions policy to induce compliance by the workforce, and (4) periodic review of information system activity, such as audit logs, access reports, and security incident tracking. 45 C.F.R. § 164.308(a)(1); see also OCR, Risk Analyses vs. Gap Analyses—What Is the difference? for guidance on HIPAA risk analysis.]

III. Policies on Individual Rights

[**Drafting Note to III. Policies on Individual Rights:** Individuals have rights related to their PHI with a covered entity.
Specifically, the rights include the right to:

- Request restrictions on certain uses and disclosures of PHI (but not the right to compel the group health plan to agree to a requested restriction)
- Receive communications containing PHI in a manner reasonably requested to ensure confidentiality and safety
- Inspect and copy PHI
- Amend incorrect PHI
- Receive an accounting of certain disclosures of PHI –and–
- Obtain a paper copy of the notice from the group health plan upon request, even if the individual agreed to receive the notice electronically

45 C.F.R. §§ 164.522, 164.524, 164.528. These rights must be set forth in the privacy notice. 45 C.F.R. § 164.520(b)(1)(iv).]

A. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants in the Plan the right to access and obtain copies of their PHI that the Plan (or its business associates) maintains in designated record sets. HIPAA also provides that participants may request to have their PHI amended. The Plan will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants as set forth in the Notice of Privacy Practices.

A "Designated Record Set" is a group of records maintained by or for the Company that includes:

1. the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
2. other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

B. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
- as part of a limited data set; or
- for national security or law enforcement purposes.

The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Contact Person may impose reasonable production and mailing costs for subsequent accountings.

[Drafting Note to B. Accounting: The HIPAA Privacy rule grants individuals the right to request and receive an accounting of most PHI disclosures. 45 C.F.R. § 164.528.]

C. Requests for Requested Confidential Communications

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests shall be honored if, in the sole discretion of the Company, the requests are reasonable.

However, the Company shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Contact Person has responsibility for addressing requests for confidential communications.

[**Drafting Note to C. Requests for Requested Confidential Communications:** A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at **alternative** locations. 45 C.F.R. § 164.522.

D. Requests for Restrictions on Uses and Disclosures of PHI

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Contact Person is charged with responsibility for addressing requests for restrictions.

[**Drafting Note to D. Requests for Restrictions on Uses and Disclosure of PHI:** Individuals have a right to request that PHI not be used and disclosed for purposes of carrying out treatment, payment, or health care operations. Nevertheless, a group health plan generally does not need to agree to the request. One exception is that an individual who pays for a health care item or service outside of the plan can forbid PHI disclosures pertaining solely to that item or service. 45 C.F.R. § 164.522.]

E. Requests for Amendment

No third-party rights (including, but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Policy. The Company reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Company. This Policy does not address requirements under other Federal laws or under state laws.

[**Drafting Note to E. Requests for Amendment:** Covered entities and business associates must permit individuals to inspect any PHI relating to them that is maintained in the form of a designated record set. In addition, the covered entity responsible for incorrect PHI in a designated record set must make any amendments necessary to correct errors or omissions. 45 C.F.R. §§ 164.526.]