HIPAA Privacy Policy

Table of Contents

HIPAA Privacy Policy for Self-Insured Plans

I. Introduction

Orange County Library System ("the Library") sponsors the following:

1. A self-insured group health plan: Health Insurance, administered through a third-party administrator (TPA) United HealthCare, and
2. A Flexible Spending Account (FSA), administered by Medcom a TPA.

For purposes of this Privacy Policy, the plans listed above are referred to collectively and singularly as the "Plan."

Members of the Library's workforce may have access to protected health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Library, for administrative functions of the Plan performed by the Library and other purposes permitted by The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rules. The Plan is administered by third-party administrators and has one or more Business Associates that perform functions for the Plan.

HIPAA and its implementing regulations restrict the Plan's and the Library's ability to use and disclose protected health information.

Protected Health Information. Protected health information 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. Protected health information includes information of persons living or deceased.

For purposes of this Policy, protected health information does not include the following, referred to in this Policy as "Exempt Information":

a. summary health information, as defined by HIPAA's privacy rules, that is disclosed to the Library solely for purposes of obtaining premium bids, or modifying, amending, or terminating the Plan;
b. enrollment and disenrollment information concerning the Plan that does not include any substantial clinical information;
c. protected health information disclosed to the Plan or the Library under a signed authorization that meets the requirements of the HIPAA privacy rules;
d. health information related to a person who has been deceased for more than 50 years;
e. information disclosed to the Library by an individual for functions that the Library performs in

its role as an employer and not as sponsor of the Plan or in providing administrative services to the Plan.

The Library may also provide information in the process of offering other plans such as dental insurance and other fully insured plans that are not subject to this Privacy Policy. This Privacy Policy will govern the circumstances, if any, that Plan protected health information may be shared with any such other plans.

It is the Library's policy that the Plan shall comply with HIPAA's requirements for the privacy of protected health information. To that end, all members of the Library's workforce who have access to protected health information must comply with this Privacy Policy. For purposes of this Policy and the Plan's more detailed Privacy Use and Disclosure Procedures, the Library's workforce includes individuals who would be considered part of the workforce under HIPAA, such as employees, volunteers, contractors, trainees, and other persons whose work performance is under the direct control of the Library, whether or not they are paid by the Library. The term "workforce member" includes all of these types of workers.

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 Library reserves the right to amend or change this Policy and to change third party administrators 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 Plan or the Library. This Policy does not address requirements under other federal laws or under state laws. To the extent this Policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

II. Plan's Responsibilities as Covered Entity

A. Privacy Official and Contact Person

The Human Resources Manager will be the Privacy Official for the Plan. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy of the Plan's protected health information, including but not limited to this Privacy Policy and the Plan's Privacy Use and Disclosure Procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their protected health information. The Privacy Official will coordinate the Plan's privacy activities with the Plan's Security Official.

The Privacy Official is responsible for ensuring that the Plan complies with all provisions of the HIPAA privacy rules, including the requirement that the Plan have a HIPAA-compliant Business Associate Contract in place with all Business Associates. The Privacy Official shall also be responsible for monitoring compliance by all Business Associates with the HIPAA privacy rules and the terms of their Business Associate Contracts.

B. Security Official and Contact Person

The Information Technology (I.T.) Director is the Security Official for the Plan. The Security Official is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy. The Security Official will coordinate the Plan's security activities with the Plan's Privacy Official.

C. Workforce Training

It is the Library's policy to train all members of its workforce who have access to protected health information for familiarity and compliance with the Plan's Policy and its Privacy Use and Disclosure Procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the necessary and appropriate training to permit them to carry out their Plan functions in compliance with HIPAA. Workforce training will be updated as necessary to reflect any changes in policies or procedures and to ensure that workforce members are appropriately aware of their obligations.

D. Safeguards and Firewall

The Library will establish on behalf of the Plan appropriate administrative, technical, and physical safeguards to prevent protected health information from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of protected health information. See the Plan's Privacy Use and Disclosure Procedures. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors and/or filing cabinets.

Firewalls will ensure that only authorized workforce members will have access to protected health information, that they will have access to only the minimum amount of protected health information necessary for the plan administrative functions they perform, and that they will not further use or disclose protected health information in violation of HIPAA's privacy rules.

E. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that complies with the HIPAA privacy rules and describes:

- the uses and disclosures of protected health information that may be made by the Plan;
- the rights of individuals under HIPAA privacy rules;
- the Plan's legal duties with respect to the protected health information; and
- other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Library will have access to protected health information in connection with its plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the effective date of the notice. The effective date will not be earlier than the date the notice is published.

The notice of privacy practices shall be posted on the Orange Peel, the Library's intranet. The notice also will be individually delivered:

- at the time of an individual's enrollment in the Plan;
- to a person requesting the notice; and
- to participants within 60 days after a material change to the notice. However, if the Plan posts its notice on the Plan's intranet and there is a material change to the notice, the Plan will prominently post the change or the revised notice on its website by the effective date of the change, and provide the change or information about the change and how to obtain the revised notice, in its next annual mailing to individuals covered by the Plan.

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

F. Complaints

The Privacy Official will be the Plan's contact person for receiving complaints. The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

G. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing protected health information in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Library's Progressive Discipline and Rules of Conduct, up to and including termination of employment. All Library workforce members with access to protected health information of the Plan must sign the Confidentiality Agreement after successfully completing training. A copy of the Agreement is attached to this policy as Appendix A.

H. Mitigation of Inadvertent Disclosures of Protected Health Information

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's protected health information in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if a workforce member or Business Associate becomes aware of an unauthorized use or disclosure of protected health information, either by a workforce member or a Business Associate, the workforce member or Business Associate must immediately contact the

Privacy Official so that appropriate steps to mitigate harm to the participant can be taken.

I. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

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

J. Plan Document

The Plan document shall include provisions to describe the permitted and required uses by, and disclosures to, the Library of protected health information for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Library to:

- not use or further disclose protected health information other than as permitted by the Plan documents or as required by law;
- ensure that any agents to whom it provides protected health information agree to the same restrictions and conditions that apply to the Library;
- not use or disclose protected health information for employment-related actions or for any other benefit or employee benefit plan of the Library;
- report to the Privacy or Security Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make protected health information available to Plan participants, consider their amendments, and, upon request, provide them with an accounting of protected health information disclosures in accordance with the HIPAA privacy rules;
- make the Library's internal practices and records relating to the use and disclosure of protected health information received from the Plan available to the Department of Health and Human Services (HHS) upon request; and
- if feasible, return or destroy all protected health information received from the Plan that the Library 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 document must also require the Library to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Library agrees to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

K. Documentation

The Plan's privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. 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), and the Plan's practices and processes. Any changes to policies or procedures must be promptly documented.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The Plan shall also document the dates, content, and attendance of workforce members at training sessions.

The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years.

III. Policies on Use and Disclosure of Protected Health Information

A. Use and Disclosure Defined

The Plan will use and disclose protected health information only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of protected health information by any Library workforce member or by a Business Associate of the Plan.
- *Disclosure.* The release, transfer, provision of access to, or divulging in any other manner of protected health information to persons who are not Library workforce members or to a person or entity who is not a Business Associate of the Plan.

B. Workforce Must Comply With Plan's Policy and Procedures

All members of the Library's workforce who have access to Plan protected health information must comply with this Policy and with the Plan's Privacy Use and Disclosure Procedures, which are set forth in a separate document.

C. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose Exempt Information to the Library. Exempt Information is not governed by this Policy, and the Library may use and disclose it for any lawful purpose.

The Plan may disclose protected health information to the following Library workforce members to perform Plan administrative functions ("workforce members with access"):

- Human Resources Department
- Finance Departments
- Administrative Team.

Workforce members with access may disclose protected health information to other workforce members

with access for plan administrative functions (but the protected health information disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Workforce members with access may not disclose protected health information to workforce members (other than workforce members with access) unless a valid, signed authorization is in place or the disclosure otherwise is in compliance with this Policy and the Plan's Privacy Use and Disclosure Procedures. Workforce members with access must take all appropriate steps to ensure that the protected health information is not disclosed, available, or used for employment purposes. For purposes of this Policy, "plan administrative functions" include the payment and health care operation activities described in section III.D of this Policy.

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

Protected health information may be disclosed for the Plan's own payment purposes, and protected health information 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, 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;
- 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; and
- any other payment activity permitted by the HIPAA privacy regulations.

Protected health information may be disclosed for purposes of the Plan's own health care operations. Protected health information may be disclosed to another covered entity 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 protected health information requested pertains to that relationship.

Health Care Operations. Health care operations mean any of the following activities:

- 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;
- business management and general administrative activities; and
- other health care operations permitted by the HIPAA privacy regulations.

E. No Disclosure of Protected Health Information for Non-Health Plan Purposes

Protected health information may not be used or disclosed for the payment or operations of the Library's "non-health" benefits (e.g., disability, workers' compensation, life insurance), 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 or allowed by applicable state law and all applicable requirements under HIPAA are met.

F. Mandatory Disclosures of Protected Health Information

A participant's protected health information must be disclosed, in accordance with Plan's Privacy Use and Disclosure Procedures, in the following situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows);
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

G. Other Permitted Disclosures of Protected Health Information

Protected health information may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Plan's Privacy Use and Disclosure Procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan's Privacy Official. Permitted are disclosures:

- about victims of abuse, neglect, or domestic violence;
- to a health care provider for treatment purposes;
- for judicial and administrative proceedings;
- for law-enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- 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.

H. Disclosures of Protected Health Information Pursuant to an Authorization

Protected health information 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.

I. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when protected health information is used, disclosed, or requested, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use, disclosure, or request.

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 HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing Protected Health Information. The Plan, when disclosing protected health information subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of protected health information that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures 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 Protected Health Information. The Plan, when requesting protected health information subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of protected health information necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures 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 Protected Health Information to Business Associates

Workforce members may disclose protected health information to the Plan's Business Associates and allow the Plan's Business Associates to create, receive, maintain, or transmit protected health information

on its behalf. However, prior to doing so, the Plan must first obtain assurances from the Business Associate, in the form of a business associate contract, that it will appropriately safeguard the information. The business associate contract will contain all of the requirements under HIPAA security regulations and specifically providing that the business associate will:

- implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that the business associate creates, receives, maintains, or transmits on behalf of the Plan;
- ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with all of the requirements of the HIPAA security regulations to protect the Contract protected health information;
- report to the Privacy Official any security incident or breach of unsecured protected health information of which the business associate becomes aware;
- take any contractually required steps with respect to breach notification requirements; and
- authorize termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.

Before sharing protected health information with outside consultants or contractors who meet the definition of a "Business Associate," workforce members must contact the Privacy Official and verify that a Business Associate contract is in place.

A Business Associate is an entity that:

- creates, receives, maintains, or transmits protected health information on behalf of the Plan (including for claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to or for the Plan, where the performance of such services involves giving the service provider access to protected health information.

K. Disclosures of De-Identified Information

The Plan may freely use and disclose information that has been "de-identified" in accordance with the HIPAA privacy regulations. 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.

L. Breach Notification Requirements

The Plan will comply with the Reportable Breach Notification Policy set forth in Appendix B of this Policy.

IV. Policies on Individual Rights

A. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their protected health information that the Plan (or its Business Associates) maintains in designated record sets. HIPAA also provides that participants may ask to have their protected health information amended. The Plan will provide access to protected health information, and it will consider requests for amendment that are submitted in writing by participants.

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

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

If information in one or more designated record sets is maintained electronically, and an individual requests an electronic copy of such information, the Plan will provide the individual with access to the requested information in the electronic form and format requested by the individual, if it is readily producible in such form and format; if the requested information is not readily producible in such form and format, the requested information will be produced, if possible, in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual are unable to agree on the form and format, the Plan will provide a paper copy of the information to the individual.

B. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own protected health information. 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 protected health information;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;

- as part of a limited data set;
- for specific national security or law-enforcement purposes; or
- disclosures that occurred prior to the compliance date.

The Plan shall

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 that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure. The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for subsequent accountings.

C. Requests for Alternative Communication Means or Locations

Participants may ask to receive communications regarding their protected health information by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. The Plan may, but need not, honor such requests. The decision to honor such a request shall be made by the Privacy Official. However, the Plan must accommodate such a request if the participant clearly states that the disclosure of all or part of the information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

D. Requests for Restrictions on Use and Disclosure of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's protected health information. The Plan may, but need not, honor such requests. However, the Plan will comply with a restriction request if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid in full by the individual or another person, other than the Plan. The decision to honor restriction requests shall be made by the Privacy Official.

Appendix A to Privacy Policy: Workforce Member Confidentiality Agreement

I, _____, have read and understand the Library's HIPAA Privacy Policy, for the protection of the privacy of protected health information, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have received training in the Library's HIPAA policies concerning protected health information use, disclosure, storage, and destruction as required by HIPAA.

In consideration of my employment or compensation by the Library, I hereby agree that I will not at any time-either during my employment or association with the Library or after my employment or association ends-use, access, or disclose protected health information to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities with the Library, as set forth in the Plan's privacy policies and procedures or as permitted under HIPAA. I understand that this obligation extends to any protected health information that I may acquire during the course of my employment or association with the Library, whether in oral, written, or electronic form and regardless of the manner in which access was obtained.

I understand and acknowledge my responsibility to apply the Library's policies and procedures during the course of my employment or association. I also understand that any unauthorized use or disclosure of protected health information will may in disciplinary action, up to and including the termination of employment or association with the Library and the imposition of civil penalties and criminal penalties under applicable federal and state law.

I understand that this obligation will survive the termination of my employment or end of my association with the Library, regardless of the reason for such termination.

Signed: _____ Date: _____ /_____ /_____

Appendix B to Privacy Policy: Reportable Breach Notification Policy

I. Introduction

This Reportable Breach Notification Policy is adopted by the Library as part of the Library's Privacy Policy and is intended to comply with the final HITECH regulations at 45 CFR §164.400 et seq. for breaches occurring on or after September 23, 2013 ("Breach Regulations").

Under the Breach Regulations, if a Reportable Breach of unsecured protected health information has occurred under the plan (the plan as defined in Section I of the Privacy Poliyc), the Library must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media.

II. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy and/or Security Official is responsible for reviewing the circumstances of possible breaches brought to his or her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations. All Business Associates, and all workforce members who have access to protected health information, are required to report to the Privacy and/or Security Official any incidents involving possible breaches.

Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the privacy rules is presumed to be a Reportable Breach, unless the Privacy or Security Official determines that there is a low probability that the privacy or security of the protected health information has been or will be compromised.

The determination of whether a Reportable Breach has occurred must include the following considerations:

- *Was there a violation of HIPAA Privacy Rules?* There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Library or a Business Associate of the Library. If not, then the notice requirements do not apply.
- *Was protected health information involved?* If not, then the notice requirements do not apply.
- *Was the protected health information secured?* For electronic protected health information to be "secured," it must have been encrypted to NIST standards or destroyed. For paper protected health information to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.

- *Was there unauthorized access, use, acquisition, or disclosure of protected health information?* The violation of HIPAA Privacy Rules must have involved one of these. If it did not, then the notice requirements do not apply.
- *Is there a low probability that privacy or security was compromised?* If the Privacy or Security Official determines that there is only a low probability of compromise, then the notice requirements do not apply.

To determine whether there is only a low probability that the privacy or security of the protected health information was compromised; the Privacy or Security Official must perform a risk assessment that considers at least the following factors:

- *The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.* For example, did the disclosure involve financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.
- *The unauthorized person who used the protected health information or to whom the disclosure was made.* For example, does the unauthorized recipient of the protected health information have obligations to protect the privacy and security of the protected health information, such as another entity subject to the HIPAA privacy and security rules or an entity required to comply with the Privacy Act of 1974 or the Federal Information Security Management Act of 2002, and would those obligations lower the probability that the recipient would use or further disclose the protected health information inappropriately? Also, was the protected health information impermissibly used within a covered entity or business associate, or was it disclosed outside a covered entity or business associate?
- *Whether the protected health information was actually acquired or viewed.* If there was only an opportunity to actually view the information, but the Privacy or Security Official determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer was lost or stolen and subsequently recovered, and the Privacy or Security Official was able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.
- *The extent to which the risk to the protected health information has been mitigated.* For example, if the Library can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the

information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

If the Privacy or Security Official determines that there is only a low probability that the privacy or security of the information was compromised, then the Library will document the determination in writing, keep the documentation on file, and not provide notifications. On the other hand, if the Privacy or Security Official is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Library will provide notifications. If an exception applies, then a Reportable Breach has not occurred, and the notice requirements are not applicable.

- *Exception 1:* A Reportable Breach does not occur if the breach involved an unintentional access, use, or acquisition of protected health information by a workforce member or Business Associate, if the unauthorized access, use, acquisition, or disclosure-(a) was in good faith; (b) was within the scope of authority of the workforce member or Business Associate; and (c) does not involve further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Library were to access the claim file of a participant whose name is similar to the name of the intended participant; but if the same employee intentionally looks up protected health information of his neighbor, the exception does not apply.
- *Exception 2:* A Reportable Breach has not occurred if the breach involved an inadvertent disclosure from one person authorized by the Library to have access to protected health information to another person at the same covered entity or Business Associate also authorized to have access to the protected health information, provided that there is no further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Library inadvertently emailed protected health information to the wrong co-worker; but if the same employee emailed the information to an unrelated third party, the exception likely does not apply.
- *Exception 3:* A Reportable Breach has not occurred if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the protected health information. For example, the exception may apply to an EOB mailed to the wrong person and returned to the Library unopened, or if a report containing protected health information is handed to the wrong person, but is immediately retrieved before the person can read it. However, the exception does not apply if an EOB was mailed to the wrong person and the unintended recipient opened the envelope before realizing the mistake.

III. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If a Reportable Breach has occurred, the Privacy or Security Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Library has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members are trained to notify the Privacy or Security Official or other responsible person immediately so the Plan can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Library, engage a third party (including a Business Associate) to assist with preparation and delivery of any required notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Library had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of-(1) the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and (2) the date that a workforce member or agent of the Library, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not impede the notice deadline.

There is an exception to the timing requirements if a law-enforcement official asks the Library to delay giving notices.

IV. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach relating to Library participants, the Business Associate must give notice to the Library. The Library is responsible for providing any required notices of a Reportable Breach to individuals, HHS, and (if necessary) the media. Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Library's notice obligations is the date that the Library receives notice from the Business Associate.

In its Business Associate contracts, the Library will require Business Associates to-

- report incidents involving breaches or possible breaches to the Privacy Official in a timely

manner;

- provide to the Library any and all information requested by the Library regarding the breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and
- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

V. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

A. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.
- If known, the date of the Reportable Breach and the Discovery Date.
- A description of the types of unsecured protected health information involved in the Reportable Breach (for example, full name, Social Security numbers, address, diagnosis, date of birth, account number, disability code, or other).
- The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services).
- A description of what the Library is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the Library is doing to mitigate harm to individuals.
- A description of what measures the Library is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

B. Types of Notice to Individuals

The Library will deliver individual notices using the following methods, depending on the circumstances of the breach and the Library's contact information for affected individuals.

Actual Notice will be given in all cases, unless the Library has insufficient or out-of-date addresses for the

affected individuals. Actual written notice-

- will be sent via first-class mail to last known address of the individual(s);
- may be sent via email instead, if the individual has agreed to receive electronic notices;
- will be sent to the parent on behalf of a minor child; and
- will be sent to the next-of-kin or personal representative of a deceased person, if the Library knows the individual is deceased and has the address of the next-of-kin or personal representative.

Substitute Notice will be given if the Library has insufficient or out-of-date addresses for the affected individuals.

- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.
- If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.

  Substitute notice via website. Conspicuous posting on the home page of the Library's intranet for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the intranet or via hyperlink.

  Substitute notice via media. Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. It may be necessary to give the substitute notice in both local media outlet(s) and statewide media outlet(s) and in more than one state.
- Substitute Notice is not required if the individual is deceased and the Library has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured protected health information may occur. Urgent notice must be given by telephone or other appropriate means.

- Example: Urgent notice is given to an individual by telephone. The Library must also send an individual notice via first-class mail.

VI. Notice to HHS

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on

the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will report to HHS the Reportable Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

VII. Notice to Media (Press Release)

Notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 residents of any one state or jurisdiction. For example:

- If a Reportable Breach affects 600 individuals who are residents of Oregon, notice to media is required.
- If a Reportable Breach affects 450 individuals who are residents of Oregon and 60 individuals who are residents of Idaho, notice to media is not required.

If notice to media is required, notice will be given to prominent media outlets serving the state or jurisdiction. For example:

- If a Reportable Breach involves residents of one city, the prominent media outlet would be the city's newspaper or TV station.
- If a Reportable Breach involves residents of various parts of the state, the prominent media outlet would be a statewide newspaper or TV station.
- If a Reportable Breach affects 600 individuals who are residents of Oregon, and 510 individuals who are residents of Washington, notice to media in both states is required.

If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for reporting this information to the Library's Administrative Team and the Public Relations Administrator is responsible for giving notice to media.