2019

Health Plan Participant Information Privacy and Security Program

Erie Insurance
9/30/2019

Contents

Preface

Purpose and Audience

This document describes ERIE's HIPAA Compliance Program and establishes policies and procedures for ensuring the protection of individually-identifiable health information held or under the control of ERIE's health plans.

Document Control

Program Owner	Employee Benefits Administration Committee
Legal Review	Counsel, Employment & Privacy Dept.

Program Overview

The Health Insurance Portability and Accountability Act (as amended) and the accompanying regulations (collectively, "HIPAA") require health plans to adopt policies and procedures designed to protect the security, privacy and confidentiality of plan participants' protected health information ("PHI"). Erie Indemnity Company ("ERIE" or the "Company") is the Plan Sponsor of the Erie Indemnity Company Health Protection Plan, the Erie Indemnity Company Dental Assistance Plan, the Erie Indemnity Company Vision Care Plan, the Erie Indemnity Company Pre-Tax Payment Plan and the Erie Indemnity Company Work Life Resources Program (the "ERIE Health Plans" or the "Plans"), which are subject to HIPAA. ERIE has delegated authority to administer the ERIE Health Plans to the Erie Indemnity Company Employee Benefits Administration Committee ("EBAC"), the Plan Administrator. ERIE and EBAC have adopted this Health Plan Participant Information Privacy and Security Program (the "Program") to establish and maintain policies, standards, procedures, controls and other Program components that achieve HIPAA's information privacy and security requirements and support the operations, mission, goals and objectives of the ERIE Health Plans.

Program Objective

The objective of ERIE's Health Plan Participant Information Privacy and Security Program is to ensure that the ERIE Health Plans collect, store, use and disclose PHI in a manner that is consistent with HIPAA and to maintain the confidentiality, integrity, and availability of PHI by protecting it against any reasonably anticipated threats, hazards, and/or inappropriate uses or disclosure.

Applicability

This Program is applicable to the ERIE Health Plans and the Company. It is overseen by EBAC, which by its Charter is responsible for administering the Plans and establishing rules, regulations and procedures as it deems necessary or appropriate to ensure the Plans operate in accordance with their plan documents and applicable law. Program requirements affect the actions and responsibilities of all persons who interact with ERIE Health Plans' information assets, including ERIE Employees and third party service providers.

Regulatory Framework

The Program is designed to comply with and account for applicable legal requirements and information security and privacy considerations. Specifically, the Program takes into account information security and privacy requirements prescribed principally by HIPAA, but is also designed to be consistent with other relevant laws and regulations, such as state data privacy and breach notification requirements.

Program Framework

The Program draws from industry best practices and the objectives set forth in the National Institutes of Standards and Technology's Special Publication 800-66, Revision 1: *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, and the resources available through the HIPAA Collective of Wisconsin, a not-for-profit corporation that assists HIPAA Covered Entities in implementing HIPAA's Privacy and Security Rule requirements.

The Program recognizes that while the ERIE Health Plans are separate legal entities from the Company, the ERIE Health Plans rely to a high degree on the personnel, information technology infrastructure and resources of ERIE, consistent with the parameters and obligations imposed on those entities by the Plans' governing documents, HIPAA, ERISA, and other applicable law. The Program recognizes that the information security and privacy requirements imposed by the Program will largely be implemented by the Company's various business units and functions. Company functional areas that assist with administering the ERIE Health Plans, include but are not limited to Human Resources, Compliance, Information Security, Office of the President, Law, Internal Audit, Crisis Prevention and Management, Enterprise Risk Management, and Sourcing and Vendor Management. The Program relies on the Company's risk-based approach to information security and oversight activities integrating people, processes, and technologies across multiple layers of its organization.

As a result, the Program incorporates by reference the Company's Corporate Information Security Program and the associated mandates, policies, procedures and controls to meet certain of HIPAA's requirements.

This Program must be periodically reviewed and updated to account for legal/regulatory, business or other changes that impact the Program and the obligations of the ERIE Health Plans.

Roles and Responsibilities

It is a fundamental premise of the Program that the ERIE functional areas involved in administering the ERIE Health Plans will collaborate with, advise and support each other and EBAC in carrying out the operations of the Program.

Additionally, because the ERIE Health Plans contract with various third parties to administer all or portions of the ERIE Health Plans, as Business Associates those third parties are obligated to comply with all HIPAA requirements applicable to Business Associates.

Erie Indemnity Company

The Erie Indemnity Company ("ERIE" or the "Company") is the Plan Sponsor of the ERIE Health Plans. As a separate legal entity from the ERIE Health Plans, the Company itself is not a covered entity directly subject to HIPAA. But because of the relationship between it and the Plans, the Company does have certain obligations with respect to PHI that it must uphold.

The ERIE Health Plans rely on ERIE Employees to perform certain administrative functions of the plans. These include, by way of example only:

- Performing day-to-day oversight and coordination with claims administrators and other business associates performing services for the ERIE Health Plans;
- Responding to participant questions or concerns;

- Reporting to the plans and applicable business associates on enrollment or status changes the Company receives from Employees and dependents; and
- Maintaining appropriate IT infrastructure and systems.

PHI may only be disclosed to the Company or employees of the Company according to the terms of the plan documents of the ERIE Health Plans, upon receipt from the Company of the required certifications and only as required for the Company's Employees to conduct the business of the ERIE Health Plans.

Employee Benefits Administration Committee

The Erie Indemnity Company Employee Benefits Administration Committee ("EBAC") is the Plan Administrator for the ERIE Health Plans and is responsible for the operation, administration and compliance of the Plans in accordance with its Charter. This includes matters of HIPAA compliance, and therefore responsibility for the oversight of the Program. EBAC appoints and oversees the HIPAA Privacy Officer and the HIPAA Security Official.

HIPAA Privacy Officer

The HIPAA Privacy Officer is appointed by EBAC and is responsible for overseeing compliance with the HIPAA Privacy Rule. The HIPAA Privacy Officer, in collaboration with the HIPAA Security Official and Company functional areas as appropriate, shall oversee all ongoing activities related to the development, implementation and maintenance of the information privacy policies, procedures, standards and notices required under HIPAA.

The HIPAA Privacy Officer is responsible for:

- Establishing and maintaining written policies, procedures and notices that place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
- Ensuring that appropriate training and education is provided to ERIE Employees whose job duties involve PHI.
- Coordinating with ERIE's Privacy Officer and Privacy Department to ensure alignment between ERIE's privacy policies, procedures and standards and those of this Program.
- Consistently enforcing the requirements of this Program and all related ERIE policies, standards and procedures.
- Maintaining a program for ERIE Employees and Plan participants to report complaints concerning the ERIE Health Plans' compliance with the law and applicable policies and procedures.
- Ensuring processes are in place to limit incidental uses and disclosures of PHI, and to mitigate the effects of an inappropriate use or disclosure of PHI in violation of HIPAA or applicable policies and procedures.
- Overseeing the incident response process and providing notice of HIPAA-related security incidents as required by applicable law.

HIPAA Security Official

The HIPAA Security Official is appointed by EBAC and is responsible for overseeing compliance with the

HIPAA-required safeguards on electronic PHI ("ePHI"). The HIPAA Security Official, in collaboration with the HIPAA Privacy Officer and Company functional areas as appropriate, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to the ERIE Health Plans' efforts to be compliant with the HIPAA Security Regulations.

The HIPAA Security Official is responsible for:

- Acting as a resource for EBAC and the ERIE Health Plans' on matters relating to information security.
- Taking direction from EBAC and/or ERIE on matters related to HIPAA compliance, and working closely with the HIPAA Privacy Officer to achieve the goals of this Program.
- Investigating and recommending secure solutions that implement the requirements of this Program and the related information security policy and standards.
- Assisting with the incident response process related to HIPAA-related security incidents
- Working and coordinating with ERIE's Chief Information Security Officer and Information Security department to ensure that ERIE information security related policies, procedures and controls relevant to the ERIE Health Plans continue to meet the requirements of the HIPAA Security Rule.

Definitions

HIPAA: Health Insurance Portability and Accountability Act of 1996. Implementing regulations, adopted by the United States Department of Health and Human Services in 2002, require health plans, health care providers and health care clearinghouses to take certain actions to protect the privacy and confidentiality of personally identifiable health information.

Covered Entity: A covered entity is a health plan, a health care clearinghouse or a health care provider that transmits PHI in electronic form in connection with designated transaction sets contained in HIPAA's Electronic Data Interchange Standards.

Business Associate: A business associate is a third party that performs a service on behalf of a covered entity. Examples of business associates of the ERIE Health Plans include their third party administrators.

Protected Health Information, or "PHI": Personally identifiable health information that is provided to one or more of the ERIE Health Plans by a plan participant, or otherwise received by one of the ERIE Health Plans, that relates to that person's past, present or future mental or physical health, the provision of health care to that person or the payment for health care. For example, a plan participant's "explanation of benefits" form received from a claims administrator is PHI because it arises out of a plan's obligation to pay for certain health care procedures covered by the plan. A completed short term disability form received from an employee's physician is not covered information because it was requested and received by ERIE in its capacity as employer, not in its capacity as administrator of the Health Plan.

This term does not include any information collected or maintained by the Company for purposes of enrolling Company employees and their dependents in the ERIE Health Plans, including but not limited to all information provided by Company employees during the annual open enrollment process or any other enrollment period. For example, the information entered into the Company's HRIS platform during an enrollment period, including benefit elections and personal information such as date of birth or Social Security Number, is not PHI.

Minimum Amount Necessary Rule: The term "minimum amount necessary" is a concept contained in the Privacy Rule that requires covered entities to disclose only the minimum amount of information that is necessary to respond to a request for PHI, or in conjunction with its use of PHI. For example, this policy requires that employees only be provided access to the PHI that is necessary for them to do their jobs.

Designated Record Set: A designated record set refers to a group of records maintained by or for a covered entity that are 1) medical records and billing records about an individual maintained by or for a health care provider; 2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or 3) information used in whole or in part by the covered entity to make decisions about an individual.

Permitted Uses and Disclosures of PHI

Permitted Disclosures for Treatment, Payment or Health Care Operations

PHI may be disclosed for the purposes of treatment, payment or health care operations without obtaining the consent of the individual to whom the PHI relates.

Treatment

"Treatment" means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

Payment

"Payment" involves the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and/or to obtain or provide reimbursement for the provision of health care.

Examples include:

- determining eligibility or coverage under a plan;
- adjusting claims;
- billing and collection activities;

- reviewing health care services for medical necessity, coverage, justification of charges, duplicate payments;
- utilization review activities.

Health Care Operations

"Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

Examples include:

- quality assessment and case management activities;
- reviewing the competency or qualifications of health care professionals;
- underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance;
- conducting audits, conducting and arranging for medical or legal review;
- fraud and abuse detection and compliance programs;
- cost management and planning analysis relating to managing and operating the entity;
- customer service;
- business management and general administrative activities.

Disclosure to the Plan Sponsor

The ERIE Health Plans, which are separate legal entities, may disclose PHI to ERIE, the Plan Sponsor of each of the ERIE Health Plans, to permit the Plan Sponsor to perform plan administration functions.

Exceptions

Use and disclosure of psychotherapy notes for treatment, payment and health care operations require the individual's written authorization. Uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI, will be made only with the individual's written authorization.

Responding to Subpoenas, Court Orders or Requests from Law Enforcement

Court Orders

The ERIE Health Plans may respond to a request for PHI pursuant to an order of court or administrative tribunal. We may only disclose information authorized by the order. All such requests should be reviewed by the Law Division before responding.

Subpoenas

The ERIE Health Plans may respond to a subpoena, discovery request or other legal process if we first determine that the party requesting the information has made a good faith attempt to provide written notice of the request to the subject; the written notice contains sufficient information about the litigation or proceeding to enable the subject to raise an objection; the time to raise objections to the court or tribunal has elapsed; and no objection has been filed.

If notice has not been provided to the subject of the request, the Plans may also disclose the requested information if the requestor obtains a qualified protective order from the court or tribunal. The Law Division should be contacted to determine whether a protective order satisfies the requirements of the HIPAA Privacy Rule.

Law Enforcement

The ERIE Health Plans may respond to requests for information from Law Enforcement if a response is required by law, or if it is in compliance with legal process such as a grand jury subpoena, an administrative subpoena or summons, or an authorized investigative demand. The information sought must be relevant and material to a legitimate law enforcement inquiry, the request must be limited in scope to accomplish the purpose for which it is requested. There must be a determination that de-identified information could not be reasonably used. All such requests must be in writing on the appropriate governmental/agency letterhead. If requests from law enforcement are made in person, proper identification such as a badge or other proof of identification should be requested. The Law Division should be consulted prior to providing a response to Law Enforcement requests.

Other Requests Which Do Not Require Prior Individual Authorization

Coroners, Medical Examiners, Funeral Directors and Organ Donors

The ERIE Health Plans may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, to determine cause of death, or for another lawful purpose. The Plans may also provide PHI to funeral directors consistent with state law.

Disclosures Made For Research Purposes

The ERIE Health Plans may disclose PHI to researchers only if a federally certified institutional review board or privacy board has reviewed the proposal and established protocols to protect the privacy of the information and has otherwise approved the research. Approval by the ERIE Health Plans' Privacy Officer must first be obtained prior to permitting disclosures for research purposes.

Disclosures Made to Prevent a Serious Threat to Health or Safety

Consistent with applicable law and ethical conduct, the ERIE Health Plans may disclose PHI if there is the basis a good faith belief that disclosure is necessary to prevent or lessen a serious and imminent threat

to the health or safety of a person or the public. Disclosure may not be made if the Plans learn of this potential harm through a request by the individual to initiate or be referred for treatment, therapy or counseling.

Disclosures Regarding Armed Forces Personnel and National Security and Intelligence Activities

The ERIE Health Plans may use or disclose PHI of members of the Armed Forces in accordance with information published by the Military in the Federal Register. The Plans may also disclose PHI to federal officials for intelligence, counter-intelligence and other national security activities authorized by the National Security Act.

Disclosures to Correctional Institutions

The ERIE Health Plans may disclose PHI to a correctional institution necessary for the provision of health care for the individual, the health and safety of such individual or other inmates or correctional officers.

Disclosures for Workers' Compensation

The ERIE Health Plans may disclose PHI as necessary to comply with workers' compensation laws. The Company Physician who provides service to individual employees at the request of ERIE may disclose the individual's PHI to the employer for purposes of evaluating workplace illnesses or injuries. The information disclosed must be limited to the provider's findings related to such work-related illness or injury. The physician must either provide written notice to the employee that the information will be provided to ERIE or post a notice in the health services area where the service is provided.

Disclosures to the Secretary of the Department of Health and Human Services

The ERIE Health Plans are required to disclose PHI to the Secretary of the Department of Health and Human Services in conjunction with an investigation of ERIE's compliance with the HIPAA Privacy Rule.

Accounting of Disclosures

Except for disclosures made for treatment, payment or health care operations, disclosures made to individuals about themselves, disclosures made to correctional facilities or for national security reasons, or any disclosures made prior to April 14, 2003, we must keep a written account of the disclosure. This written account must include the following:

- date of the disclosure;
- the name of the entity or person who received the protected health information;
- their address, if known;
- a brief description of the information disclosed;
- a brief description of the purpose of the disclosure;

- if the disclosure is to the same individual on multiple occasions, the accounting may include the first and last disclosure and a description of the frequency with which disclosures were made;
- written accounts must be maintained in the plan participant's benefits file for six years.

Requests Requiring Individual Authorization

If a request for PHI is not for the purpose of treatment, payment or health care operations, and also does not fall under one of the other categories of disclosures described above, the individual's authorization must be obtained before the PHI may be disclosed. All authorizations must be in writing using the ERIE Health Plans' "Authorization for the Disclosure of Health Information" form.

If PHI is disclosed pursuant to an authorization form, a copy of the completed form must be maintained in the Employee's benefits file. Such forms must be retained for a period of six years from the date the form was completed.

Plan Participant Rights

The Right to Request Restrictions on Our Use and Disclosure of PHI

Individuals have the right to request restrictions on the ERIE Health Plans' use and/or disclosure of their PHI. If the Plans receive such a request from a plan participant, the Plans will provide them with a copy of the form entitled, "Individual Request Not to Use or Disclose Health Information." No such request is effective unless approved by the ERIE Health Plans' Privacy Officer. Restrictions may be terminated at the request of the individual or the Plans. If the ERIE Health Plans terminate a requested and approved restriction, such termination shall be effective only with respect to PHI that is created or received after it has informed the individual of its termination of the restriction.

If the request pertains to the method of communication of PHI to an individual or the location to which information regarding the individual should be sent, the ERIE Health Plans must accept the request if the individual clearly states that the request has been made to prevent harm to the individual. If restrictions are accepted, they must be followed until terminated in accordance with this policy. Copies of all completed applications and accepted restrictions must be maintained in the plan participants' benefits file.

The Right of Individuals to Access Protected Health Information

An individual has a right to inspect or receive copies of his or her PHI that is contained in a "designated record set." This right does not extend to the following information:

- psychotherapy notes;
- information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding.

All requests should be in writing using the "Individual Request to Inspect Health Information Contained in a Designated Record Set" form. Following a review by the appropriate individual designated by the HIPAA Privacy Officer, a response to the request should be provided using the "Response to Request for Access to Health Plan Information" form. The form will indicate whether the request has been granted or denied.

A request may be denied without further review if the information requested was obtained from someone other than a health care provider and that individual was promised confidentiality.

Access may be denied for the following reasons:

- a licensed health care individual has determined that the release of the information would endanger the life or physical safety of the individual or another person;
- the protected health information makes reference to another person, and the release of the information would likely cause substantial harm to the other person;
- the request is made by the individual's personal representative and a licensed health care professional has determined that access by the personal representative is likely to cause substantial harm to the individual or another person.

Review of denial of access: If access is denied for the reasons set forth above, the ERIE Health Plans must ask a licensed health care professional who was not involved in the initial decision to make a determination regarding access. The individual must receive a prompt written response from the licensed heath care professional.

The Right of Individuals to Amend Protected Health Information

Individuals may request amendment of their PHI that is contained in a designated record set. All requests should be in writing using the form, "Individual Request to Correct or Amend a Record." Responses must be made within 60 days of the request. An extension of an additional 30 days may be taken if a written reason for the delay is provided to the requestor and a new response date is provided.

The ERIE Health Plans may deny requests for amendment for the following reasons:

- the information was not created by the ERIE Health Plans;
- the information is not part of a designated record set;
- the information is otherwise unavailable for inspection under the rules regarding rights of access;
- the information is already accurate and complete.

The ERIE Health Plans' written denial must provide the following information:

- indicate the basis for the denial, using the reasons set forth above;
- advise the individual of his/her right to disagree with the denial and explain how they may file such a statement;

- advise the individual that if he/she does not file a statement of disagreement, he/she may request to have the ERIE Health Plans attach the request for amendment to any future disclosures of PHI that concern the request for amendment; (If a statement of disagreement is provided, it must be either linked to or included with the designated record set.)
- inform the individual how he/she may file a complaint pursuant to the ERIE Health Plans' Complaint procedures.

If the ERIE Health Plans accept the amendment, they must do the following:

- make the appropriate amendment to the record by, at the very least, identifying the records that are affected and providing a link to the corrected information;
- inform the individual that the amendment is accepted and obtain the individual's agreement to notify others of the amendment, if others need to be notified;
- inform persons identified by the individual who need the amendment and determine which business associates, including any third party administrators, who need access to the amendment to prevent harm to the individual.

If the ERIE Health Plans receive information regarding an amendment from another covered entity, it must amend the PHI as requested by the covered entity.

The Right of Individuals to Request an Accounting of Disclosures of PHI

An individual may request an accounting of disclosures made by the ERIE Health Plans of his/her PHI for a period of up to six years of the date of the request. The accounting must include the following information:

- the date of the disclosure;
- the name of the entity or person who received the protected health information, and their address, if known;
- a brief description of the information disclosed;
- a brief description of the purpose of the disclosure;
- if the disclosure is to the same individual on multiple occasions, the accounting may include the first and last disclosure and a description of the frequency with which disclosures were made.

The ERIE Health Plans must provide the accounting within 60 days of its receipt of the request. An extension of 30 additional days may be taken so long as the individual is provided with a written description of the reasons for the delay and is provided with the date by which the accounting will be received.

Individuals are permitted one request for an accounting per year free of charge. The ERIE Health Plans may impose a cost-based fee for additional accounting requests. Individuals must be provided with advance notice of the fees and be given an opportunity to withdraw their request.

The ERIE Health Plans must document all accountings provided as well as the individual who responded to the request for accounting.

The ERIE Health Plans need not track the following disclosures. They do not have to be provided in any accounting:

- disclosures made to carry out treatment, payment or health care operations;
- disclosures made to individuals about themselves;
- disclosures to persons involved in the individual's care;
- disclosures made for national security or intelligence purposes;
- disclosures made to correctional facilities or to law enforcement;
- any disclosure made prior to April 14, 2003.

An individual may request an accounting of disclosures of any "electronic health record" (that is, an electronic record of health-related information about the individual that is created, gathered, managed and consulted by authorized health care clinicians and staff). Individuals must submit the request in writing and state a time period which may be no longer than three years prior to the date on which the accounting is requested. In the case of any electronic health record created on an individual's behalf on or before January 1, 2009, this paragraph shall apply to disclosures made on or after January 1, 2014. In the case of any electronic health record created on your behalf after January 1, 2009, this paragraph shall apply to disclosures made on or after the later of January 1, 2011 or the date the Plans acquired the electronic health record.

The Right of Individuals to Designate a Personal Representative

Individuals have the right to designate another individual to act as their personal representative with respect to their PHI. Individuals intending to designate a personal representative should complete the form, "Designation of Personal Representative." A personal representative stands in the shoes of the individual and may make decisions for the individual and exercise the individual's rights.

If the Individual is:	**The personal representative is:**
An adult, emancipated minor, or unmarried dependent between the ages of 19 and 25 enrolled full-time at an accredited school, college or university	A person with legal authority to make health care decisions on behalf of the individual (form required) Examples: Designated Personal Representative under HIPAA (form required) Health Care Power of Attorney (form required) Court appointed legal guardian (form required)
An unemancipated minor	A parent, guardian or other person acting in loco parentis with legal authority to make health care decisions on behalf of

	the minor child
Deceased	A person with legal authority to act on behalf of the decedent or the estate (not restricted to health care decisions) Examples: Executor of the estate, next of kin or other family member

Parents and unemancipated minors: In most cases, a parent will be considered the personal representative of his/her unemancipated child. The completion of a Designated Personal Representative Form is not required. The Privacy Rule permits a covered entity to disclose to a parent, or provide a parent with access to a minor child's protected health information when and to the extent that it is expressly permitted or required by state law.

Spouses and dependent college/university students: The Privacy Rule permits family members who are actively involved in the health care of another family member to receive PHI regarding that family member without being formally designated as that individual's personal representative if the family member orally consents to the involvement of their family member or circumstances suggest that such consent exists. For example, a woman may pick up a prescription from a pharmacy for her husband even though she has not been designated as his personal representative. The circumstances surrounding release of the prescription suggest its legitimacy. Similarly, if a Benefits Section employee receives a telephone call, e-mail or other communication from a plan participant seeking information about his or her spouse or about his or her son or daughter who is enrolled in college, the Benefits Section employee should advise the requester that she must receive permission from the individual to discuss his or her PHI with that family member. Permission may be obtained in the following ways:

- Oral Permission. Contact the individual by phone or e-mail to obtain permission to disclose his or her PHI to the family member. The individual's response should be documented in the benefits file.
- Written Permission. Have the individual complete a Designation of Personal Representative Form.
- Legal Status. If the individual has executed a power of attorney or other document, obtain a copy of the document. The document should be reviewed by the Law Division for legitimacy under state law before PHI is disclosed.

The Right of Individuals to Request Confidential Communications

Individuals have the right to request that the ERIE Benefit Plans communicate with them in confidence about their PHI by alternative means or to an alternative location. For example, individuals may ask that the ERIE Benefit Plans contact them only at their work address or via their work e-mail. Individuals must

make their request in writing, and must state that the information could endanger them if it is not communicated in confidence by the alternative means or to the alternative location they want.

The ERIE Benefit Plans must accommodate the request if it is reasonable, specifies the alternative means or location, and continues to permit the ERIE Benefit Plans to pay claims according to Plan terms, including issuance of explanations of benefits to the subscriber of the health plan in which the individuals participate.

Complaint Procedures

Complaints should be forwarded to the HIPAA Privacy Officer for review. The HIPAA Privacy Officer shall investigate the complaint and shall provide a timely written response to the complainant. There shall be no retaliation against any individual for filing a complaint.

Risk Assessment

Risk assessment is an ongoing and integral component of the Program and a part of many program requirements. In addition to the risk assessment activities required by the Company's Corporate Information Security and Cybersecurity Program, this Program requires periodic risk assessments of potential threats and vulnerabilities to the confidentiality, integrity and availability of the ePHI of the ERIE Health Plans and to develop strategies to efficiently and effectively mitigate the risks identified in the risk assessment process. The risk assessments required by this Program may to the extent practicable build upon the risk assessment activities conducted by the Company pursuant to its Corporate Information Security and Cybersecurity Program, provided all applicable requirements of HIPAA and this Program are met. Documentation of risk assessment activities must be maintained a minimum of six (6) years.

Business Associates

The ERIE Health Plans engage third parties to perform a number of plan-related administrative functions, and as necessary, provides third parties with access to its non-public personal information, including PHI, in the course of the third party's engagement. Third Parties performing services for the ERIE Health Plans are Business Associates, and must be vetted through the Company's third party assessment process and bound to the necessary contractual provisions, including a Business Associate Agreement conforming to the requirements of this Program and HIPAA, prior to engagement of the Business Associate and any information sharing. These steps are designed to protect the PHI and other restricted or confidential information to which Business Associates are provided access.

Prior to engaging a Business Associate and sharing any PHI, the Business Associate must be evaluated pursuant to ERIE's Third Party Risk Assessment process, and a Business Associate Agreement conforming to the requirements of HIPAA and this Program must be executed between the Business Associate and

the plan the Business Associate will perform services for. The requirements of this Program apply equally to Business Associates of the ERIE Health Plans.

Incident Response Procedure

This section sets forth the Program's incident response process for security incidents involving PHI. This process reflects the federal breach notification requirements imposed on the ERIE Health Plans in the event that an individual's "unsecured" protected health information (as defined under HIPAA and the HITECH Act) is acquired by an unauthorized party. To the extent a security incident involves ERIE's information systems or IT infrastructure, this process may occur in conjunction with other of ERIE's incident response procedures triggered

Determining whether a breach has occurred.

Under HIPAA, a breach is defined as an unauthorized acquisition, access, use or disclosure of "unsecured" PHI that compromises the information's security or privacy.

"Unsecured" PHI means protected health information in either paper or electronic form that is not secured by using a technology or methodology specified by HHS that renders the PHI unusable, unreadable or indecipherable to unauthorized persons. We require all PHI in the possession of the Plan Sponsor or the ERIE Health Plans to be secured according to the requirements of HHS.

Following a security incident, the HIPAA Privacy Officer shall conduct an analysis of whether a reportable breach has occurred. A reportable breach has occurred when:

1. Unsecured PHI is used or disclosed in an incident not otherwise permitted by HIPAA's Privacy Rules and this Policy. This means that there has been an acquisition, access or use of unsecured PHI that is **not** consistent with the uses and disclosures permitted under the HIPAA Privacy Rules, this policy document and the ERIE Health Plans' Privacy Notices. In other words, if the access, use or disclosure is in connection with or incident to an otherwise permissible use or disclosure, and occurs despite reasonable safeguards and proper minimum necessary procedures, a "breach" requiring notification has not occurred.

2. The security or privacy of the PHI is compromised and the breach does not fall into one of the three exceptions:

    a. Unintentional access. The PHI was unintentionally accessed by a workforce member or person acting under the authority of the Plan Sponsor or a business associate, where the PHI was acquired in good faith and within the scope of the employment (or other authority) and not further used or disclosed in violation of HIPAA.

    b. Inadvertent disclosure. The PHI was inadvertently disclosed by a person authorized to access PHI to another person within the same entity also authorized to access PHI, and the PHI is not further used or disclosed in violation of the privacy rules.

c. Unretainable PHI. The covered entity or business associate has a good-faith belief that the person to whom PHI was disclosed improperly would not reasonably have been able to retain it.

3. A low probability of compromise cannot be established. This means that we cannot determine that the impermissible use or disclosure of PHI has a low probability compromising the PHI. An acquisition, access, use or disclosure of PHI is presumed to be a breach unless we can demonstrate that there is a low probability that the PHI was compromised, based on a risk assessment that considers at least the following four factors:

   a. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   b. the unauthorized person who used the PHI or to whom the disclosure was made;
   c. whether the PHI was actually acquired or viewed; and
   d. the extent to which the risk to the PHI has been mitigated.

If an evaluation of these factors fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required.

Timeframe for Notification

If a breach has occurred under the definitions set forth in Section A, above, then notification must be made to affected individual(s) without unreasonable delay, but in no event not later than 60 calendar days after discovery of the breach. A breach is considered "discovered" by a covered entity as of the first day on which the breach is known to the covered entity or workforce member of the covered entity, or by exercising reasonable diligence, would have been known by the covered entity or workforce member of the covered entity. A "workforce member" of the Plan Sponsor or ERIE Health Plans includes any person identified by the ERIE Health Plans as being someone who may use PHI or to whom PHI may be disclosed.

Method and Manner of Notification

Contents of Notice.

The notice must be written in plain language and provide the following information:

- A brief description of what happened, including the date of the breach, and the date of discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (for example, an individual's full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website or postal address.

Manner of Notice.

The notification should be mailed by first-class mail to the individual's last known address, or via email if that individual has agreed to electronic notice, and such notice has not been withdrawn. If the covered entity knows that the individual is deceased, and has the address of the next of kin or personal representative of the individual, such notice should be mailed to the personal representative or next of kin.

Substitute Notice.

In the event where there is insufficient or out of date contact information, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided to a personal representative or next of kin, where there is insufficient or out-of-date contact information.

- If the insufficient or out of date contact information is for fewer than 10 individuals then substitute notice may be made by an alternative form of written notice, by telephone or other means.

- If the insufficient or out-of-date contact information involves 10 or more individuals, then the alternate form of notice shall:

    - be in the form of a conspicuous posting for a period of 90 days on the home page of the website of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

    - include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's PHI may be included in the breach.

Additional Notice in Urgent Situations.

In cases where the Plan Sponsor or the ERIE Health Plans determine that the need for notice is urgent because of a suspected possible imminent misuse of unsecured PHI, the covered entity may provide notice by telephone and other alternate means in addition to the required written notice.

Required Notification to the Media.

A breach of unsecured PHI affecting more than 500 individuals in a single state or jurisdiction requires notification to prominent media outlets within that state or jurisdiction. This notification shall be provided without unreasonable delay, and in no case later than 60 calendar days following discovery of a breach. The notice to the media shall contain the same information as the written notice and may be done in the form of a press release. Any required notice to the media shall be made in addition to (not in place of) the individual notice.

Notification to the Secretary of Health and Human Services.

For breaches involving more than 500 individuals, notice shall be made to the Secretary of Health and Human Services (HHS) in the manner provided on the HHS website. For breaches involving less than 500 individuals, the covered entity shall maintain a log of such breaches and not later than 60 calendar days following the end of each calendar year, provide the notification required to the Secretary of HHS in the manner provided on the HHS website.

Notification of Breaches by Business Associate.

A Business Associate is required to notify a covered entity in the event it has sustained a breach of PHI of the covered entity. The notice shall include the identity of the individuals whose information was subject to the breach. Upon receipt of notification of the breach from a business associate by the Plan Sponsor or the ERIE Health Plans, the Privacy Officer shall make a determination whether a breach has occurred and provide any notification to affected individuals required by this section.

Law Enforcement Delay.

If a law enforcement official states to a covered entity or business associate that a required notification, notice or posting would impede a criminal investigation or cause damage to national security, the covered entity or business associate shall delay such notification if the request for delay is in writing and includes a timetable for such delay. If the request for delay is made orally, the covered entity must document the request and include the identity of the official who made the request for delay and temporarily delay the notification for no longer than 30 days, unless the request for delay is subsequently made in writing as set forth above.

HIPAA Education and Awareness

Well-trained and aware ERIE Employees are essential to the privacy and security of the PHI of the ERIE Health Plans. This Program requires all individuals with access to PHI to receive training on the requirements of this Program and of HIPAA upon initial hire, periodically thereafter, and when there are changes to job functions, this Program, or applicable legal requirements. The HIPAA Privacy Officer shall work with the relevant ERIE functional areas (such as Law, Privacy and Compliance) to formulate the training and education activities required under the Program.

In addition, the HIPAA Privacy Officer and HIPAA Security Official shall receive, upon assuming their respective office(s), appropriate training to inform them of their responsibilities in those positions and the requirements of this Program, HIPAA, and other applicable legal requirements.

Any such training shall be documented, and such documentation shall be retained for a minimum of six (6) years.

Violations

ERIE Employees who violate the terms of this Program, or any of the related policies and procedures, shall be subject to disciplinary action, up to and including termination of employment.