Privacy and Security Policies and Procedures

Table of Contents

Privacy and Security Policies and Procedures

Privacy Policies and Procedures

Security Policies

Glossary

Revision History

Privacy Policies and Procedures

Authorized User Access

Privacy Policy and Procedure
Policy No. P01

1 Policy Statement

HEALTHeNET Data Suppliers/Data Recipients must comply with applicable law and HEALTHeNET Policies and Procedures and promulgate the internal policies required for such compliance in order to provide essential privacy protections for patients. Authorized Users will be permitted access to patient protected health information ("PHI") only for purposes consistent with the HEALTHeNET *Services and Network Agreement*.

2 Scope

This policy applies to all Data Suppliers/Data Recipients that have registered with and are participating in HEALTHeNET that may provide, make available or access health information through HEALTHeNET. This policy also applies to all HEALTHeNET personnel who access health information through HEALTHeNET.

3 Procedure

3.1 Requirements for Data Supplier's/Data Recipient's Authorized Users

At the time that a Data Supplier/Data Recipient identifies an Authorized User to HEALTHeNET, the Data Supplier/Data Recipient must confirm to HEALTHeNET, if requested, that the Authorized User:

1. Will be permitted to use HEALTHeNET's on-line community health information network ("Network") only as reasonably necessary for the performance of the Data Supplier's/Data Recipient's activities as indicated in the Data Supplier's/Data Recipient's HEALTHeNET Agreement;
2. Has had his or her identity verified by the Data Supplier/Data Recipient;
3. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized User;
4. Has acknowledged that his or her failure to comply with HEALTHeNET Policies and Procedures may result in the withdrawal of privileges to use the Network and may constitute cause for disciplinary action by the Data Supplier/Data Recipient; and
5. Has complied with other requirements described in HEALTHeNET Policies and Procedures.

3.2 Requirements for HEALTHeNET's Personnel

HEALTHeNET will require that each person utilizing the Network on behalf of HEALTHeNET:

1. Has completed a training program provided or approved by HEALTHeNET;
2. Has had his or her identity verified by HEALTHeNET;

3. Will be permitted to use the Network only as reasonably necessary for the performance of HEALTHeNET's activities;
4. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized Users;
5. Has acknowledged that his or her failure to comply with HEALTHeNET Policies and Procedures may result in the withdrawal of privileges to use the Network and may constitute cause for disciplinary action by HEALTHeNET;
6. Has complied with other requirements described in HEALTHeNET Policies and Procedures.

3.3 Access Limited to Minimum Amount of Information

HEALTHeNET and Data Suppliers/Data Recipients must ensure that reasonable efforts are made to access the minimum amount of information necessary to accomplish the intended purpose for which the information is accessed.

4 References

- 45 C.F.R. § 164.514(d)(2)(i).
- HEALTHeNET Policy P03, *Sanctions for Failure to Comply with HEALTHeNET Privacy and Security Policies and Procedures.*

1 Policy Statement

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes provisions for protecting the privacy and security of patient protected health information ("PHI"). HIPAA regulations require Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information. As a Business Associate of the Covered Entities supplying and/or receiving data in HEALTHeNET, it is the policy of HEALTHeNET to comply with those requirements in accordance with the procedures set forth herein. As a business conducting business in New York State, HEALTHeNET will also comply with the New York State Information Security Breach and Notification Act.

2 Scope

HEALTHeNET and its Data Suppliers/Data Recipients including but not limited to those who Access the HEALTHeNET System and/or Transmit PHI contained therein, as well as those who maintain the HEALTHeNET hardware and software.

3 Procedure

HEALTHeNET will use appropriate administrative, technical, and physical safeguards to prevent a breach of unsecured PHI.

3.1 Reporting Requirements

A. HEALTHeNET personnel and HEALTHeNET Data Suppliers/Data Recipients, who discover, believe, or suspect that unsecured PHI has been Accessed, Used, Transmitted or Disclosed in a way that may violate the HIPAA Privacy or Security Rules, must immediately report such information to the HEALTHeNET Privacy Officer/designee.

B. The HEALTHeNET Privacy Officer/designee will report the breach or suspected breach to the effected Data Supplier(s), verbally, within 24 hours of HEALTHeNET becoming aware of such breach followed by written notice within 72 hours of verbal notification.

1. HEALTHeNET will include in the report, or provide to the Data Supplier(s) as promptly thereafter as the information becomes available, the following:
   i. Identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, Accessed, Transmitted, acquired, Used or Disclosed;
   ii. A brief description of what happened, including the date of the breach and the date of the discovery of the breach.

2. HEALTHeNET will not contact any individuals suspected to be affected by the breach without prior written approval of the effected Data Supplier(s).

C. HEALTHeNET and/or Data Supplier(s)/Data Recipient(s) where breach occurred will:
   1. Investigate the scope and magnitude of the breach;
   2. Identify the root cause of the breach;
   3. Mitigate, to the extent possible, damages caused by the breach;
   4. If applicable, request the party who received such information to return and/or destroy the impermissibly disclosed information;
   5. Apply sanctions to their respective staff members involved in the breach, as appropriate in accordance with their respective Privacy and Security policies and procedures and HEALTHeNET Policy P03, *Sanctions for Failure to Comply with HEALTHeNET Privacy and Security Policies and Procedures.*

CI. If applicable, HEALTHeNET will report security breaches as required by the New York State Information Security Breach and Notification Act.

CII. HEALTHeNET will notify the HEALTHeNET Operating Committee and the HEALTHeNET Board of Directors of the breach.

4 References

- 45 C.F.R. Subpart D.
- HEALTHeNET Policy P03, *Sanctions for Failure to Comply with HEALTHeNET Privacy and Security Policies and Procedures.*
- HEALTHeNET: *Terms and Conditions for Data Supplier Services and Network Agreement, Exhibit A.*
- HEALTHeNET: *Terms and Conditions for Data Recipient Services and Data Use Agreement, Exhibit A.*

Sanctions for Failure to Comply with HEALTHeNET Privacy and Security Policies and Procedures

Privacy Policy and Procedure
Policy No. P03

1 Policy Statement

HEALTHeNET and each Data Supplier/Data Recipient shall implement system procedures to discipline and hold Authorized Users, workforce members, agents and contractors accountable for ensuring that they do not Use, Transmit, Disclose or Access patient protected health information ("PHI") except as permitted by the HEALTHeNET Privacy and Security Policies and Procedures and that they comply with these policies and procedures.

2 Scope

This policy applies to HEALTHeNET and all Data Suppliers/Data Recipients that have registered with and are participating in HEALTHeNET that may Transmit, make available or Access health information through HEALTHeNET.

3 Procedure

A. Any breach of patient PHI reported by HEALTHeNET to a HEALTHeNET Data Supplier/Data Recipient (see HEALTHeNET Policy P02, *Breach Response*) will be handled according to the Data Supplier's/Data Recipient's HIPAA Privacy and Security Policies.

B. Any breach reported to HEALTHeNET by a Data Supplier/Data Recipient (see HEALTHeNET Policy P02, *Breach Response*) will be handled according to HEALTHeNET's Privacy and Security Policies and Procedures.

C. HEALTHeNET will impose sanctions on HEALTHeNET personnel who are determined to have failed to adhere to HEALTHeNET Privacy and Security Policies and Procedures.

D. HEALTHeNET Data Suppliers/Data Recipients are solely responsible for all acts and omissions of the Authorized Users of their workforce. HEALTHeNET will impose sanctions on a Data Supplier/Data Recipient whose Authorized Users fail to adhere to HEALTHeNET Privacy and Security Policies and Procedures.

E. When determining the type of sanction to apply, HEALTHeNET and/or the Data Supplier/Data Recipient will consider the following factors:
   1. whether the violation was a first time or repeat offense;
   2. the level of culpability of the Data Supplier/Data Recipient or Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently;
   3. whether the violation may constitute a crime under state or federal law; and
   4. whether there is a reasonable expectation that the violation did or may result in harm to a patient or other person.

F. Sanctions will include, but do not necessarily have to be limited to, the following:
   1. requiring an Authorized User to undergo additional training with respect to participation in HEALTHeNET;
   2. temporarily restricting an Authorized User's Access to HEALTHeNET;
   3. terminating the Access of an Authorized User to HEALTHeNET; and
   4. suspending or terminating a Data Supplier's/Data Recipient's participation in HEALTHeNET.

G. Any Sanction involving the termination of a Data Supplier Services and Network Agreement or a Data Recipient Services and Data Use Agreement resulting from a failure to comply with HEALTHeNET Policies and Procedures, must first be presented to the HEALTHeNET Operating Committee for review and approval.

4 References

- HEALTHeNET Policy P02, *Breach Response.*

Security Policies

1 Introduction

HEALTHeNET and HEALTHeLINK are affiliated organizations established as the result of collaboration and funding from the region's major hospital systems and health plans.

Both HEALTHeNET and HEALTHeLINK are business associates, as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), of the covered entities that provide and access HEALTHeNET and HEALTHeLINK data. As a business associate, both organizations are required to comply with the HIPAA Security Rule that requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

HEALTHeNET is committed to the continuous improvement in planning, implementation, monitoring, and changes to the Information Security Management System (ISMS).

2 Scope

A singular Information Technology department is responsible for the security of the systems that contain the electronic data of both HEALTHeNET and HEALTHeLINK. The security policies and procedures that apply to HEALTHeLINK will also apply to HEALTHeNET.

3 Reference

Please refer to HEALTHeLINK Privacy and Security Policies and Procedures available online at HEALTHeLINK's website. In each instance where the term "HEALTHeLINK" appears, the term "HEALTHeNET" should be used in its stead.

Glossary

Please refer to the glossary in the current HEALTHeLINK Privacy and Security Policies and Procedures available online at HEALTHeLINK's website.

Revision History

Privacy Policies and Procedures

Authorized User Access
Policy P01

Effective Date: 08/15/19

Review Dates: 07/25/19, 05/26/22, 05/25/23, 11/21/24

Revision Effective Dates: 06/30/23, 12/23/24

Breach Response
Policy P02

Effective Date: 08/15/19

Review Dates: 07/25/19, 05/26/22, 05/25/23, 11/21/24

Revision Effective Dates:

Sanctions for Failure to Comply with HEALTHeNET Privacy and Security Policies and Procedures
Policy P03

Effective Date: 08/15/19

Review Dates: 07/25/19, 05/26/22, 05/25/23, 11/21/24

Revision Effective Dates: 06/27/22

Security Policies

Preamble (S01)

Effective Date: 08/15/19

Review Dates: 07/25/19, 05/25/23

Revision Effective Dates: 06/30/23