Georgia Health Information Network, Inc.
GeorgiaConnX Network Operating Policies

Version History

Effective Date: September 30, 2021	**Revision Date:** September 21, 2021
Originating Work Unit: TBD	**Revision Number:** 1

Contents

GaHIN-2001 Identity Verification Policy

Purpose of Policy

The purpose of this policy is to ensure that only specifically authorized individuals gain access to the Network.

Policy Scope

This policy applies to the Network Facilitator, Vendor, Network Participants, and Member Affiliates.

Policy Statement

1. Access to the Network shall be restricted to Authorized Users.
2. The following shall be designated as Authorized Users:
    a. Workforce members of any Network Participant or Member Affiliate.
    b. Workforce members of the Network Facilitator.
    c. Others as required by law and designated by Network Facilitator.
3. Network Participants and Member Affiliates shall be responsible for verifying the identities of Authorized Users. A Network Participant that is a Health Information Organization may delegate this responsibility to its Member Affiliates.
4. Such identity verification shall be conducted through a review of documentation (government-issued identification card, Social Security card, Member Affiliate provider number (if applicable), or other documentation) in accordance with the Network Participant's policies and procedures.
5. Network Participants and Member Affiliates shall use a multi-factor authentication solution of their choosing that provides a time-based one-time password to access the clinical viewer web portal (e.g., Google Authenticator, Duo, and Authy).
6. For access to GaHIN through a Member's direct connection within the Member's software application, the authentication is handled by the exchange of certificates between GaHIN or its authorized designee, and the Member's software product.
    a. Any additional user authentication shall be managed at the Member level and shall be specific to that application.
    b. For Single Sign On connections, the authentication shall be managed at the Member level through provision of the user account creation in the Member's application and then shall be managed by those Member's applications which may have their own requirements.
7. An Authorized User shall utilize both aspects of his or her authentication information prior to being granted access to the Network and accessing Health Data through the Network.
8. The vendor shall perform initial authentication of Authorized Users in accordance with the documentation and verification requirements set forth in the *Digital Certificate Policy*. On subsequent access to the Network, Authorized Users shall be prompted to authenticate their identity.

9. All Network Participants and Member Affiliates shall ensure that Health Data is requested and viewed only by Authorized Users with the legal authority to have such access.
10. All Network Participants and Member Affiliates shall update the Network Facilitator if an Authorized User's status must be terminated or amended, as necessary.
11. Network Participants, Member Affiliates, and Business Associates shall educate and oversee Authorized Users to ensure that this policy is consistently followed.
12. All violations of this policy shall be promptly reported to the Network Facilitator so that appropriate safeguards can be taken to eliminate or mitigate the possibility of access to the Network by any unauthorized individual.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

HIPAA Privacy and Security Rule 45 C.F.R. § 164.530 Administrative Requirements

Related Documents

- Digital Certificate Policy

GaHIN-2002 Notice of Privacy Practices Policy and Opt-Out Notifications

Purpose of Policy

The purpose of this policy is to ensure that all Network Participants and Member Affiliates develop, maintain, and appropriately distribute a Notice of Privacy Practices (NPP) consistent with applicable federal and state laws.

Policy Scope

This policy applies to the Network Participants and Member Affiliates.

Policy Statement

Notice of Privacy Practices

1. Each Network Participant and Member Affiliate shall develop, distribute, and maintain a NPP that complies with all applicable laws, including HIPAA and HITECH, and this policy.
2. Each Network Participant and Member Affiliate shall make its NPP available to a patient prior to sending, uploading, and otherwise distributing any of the patient's Health Data through the Network.
3. For Network Participants and Member Affiliates who are health care providers, the NPP shall be:
    a. Provided to a patient at the first date of service by the health care provider.
    b. Made available to the public upon request.
    c. Made available electronically through the Network Participant's or the Member Affiliate's website, if possible.
    d. Made available at the Network Participant's or the Member Affiliate's treatment location.
    e. Posted in a clear and prominent location where it is reasonable to expect patients seeking treatment services to be able to access the NPP.

Opt-Out Notice

1. Each Network Participant and Member Affiliate shall include a notice of the patient's right to Opt-Out of having his or her Health Data exchanged via the Network in the NPP.
2. Consistent with 21st Century Cures Act Information Blocking requirements, Network Participants and Member Affiliates shall not improperly encourage or induce patients to opt out and must implement their practices in a consistent and non-discriminatory manner.
3. The Opt-Out notice shall include the following:
    a. An explanation of the function of a Health Information Exchange (Network) and the potential benefits and risks of participating in the Network.
    b. A description of the types of Health Data that may be, and may not be, exchanged via the Network.

c. A description of the permitted purposes for disclosure of the patient's Heath Data via the Network.

d. An identification of who and/or what entities have access to the patient's Health Data via the Network.

e. An explanation of the patient's right not to share Health Data through the Network by completing and submitting an Opt-Out form.

f. An explanation that a Network Participant or Member Affiliate is authorized to disclose the patient's Health Data via the Network unless and until the patient elects to Opt-Out by completing and submitting an Opt-Out form.

g. An explanation of how the patient's Health Data will be handled if they exercise their right to Opt-Out.

h. A statement that an Opt-Out decision remains in effect until the patient notifies the health care provider of their intent to participate in the Network.

4. In accordance with the 21st Century Cures Act Information Blocking requirements, the opt-out notice must present all information accurately, and must not omit important information nor present information in a way that is likely to improperly influence the patient's decision about how to exercise his or her opt-out right.

Right to Opt-Out

1. Patients of a Network Participant or Member Affiliate who is a health care provider shall be automatically enrolled in the Network without a written HIPAA authorization.
2. A patient shall be deemed to have given his or her consent to participate until and unless the patient affirmatively exercises their right to Opt-Out of the Network.
3. If a patient does not Opt-Out of the Network, his or her Health Data shall be disclosed in response to a specific request by a Network Participant or a Member Affiliate for permitted purposes, subject to the *Restrictions of Sensitive Health Information Policy*.
4. A patient may Opt-Out of having their Health Data disclosed through the Network at any time, even after enrollment in the Network.
5. A patient may revoke his or her decision to Opt-Out at any time, provided that such revocation shall not preclude any Network Participant that has accessed Health Data via the Network prior to such revocation, and incorporated such Health Data into its records, from retaining such information in its records.
6. The patient's choice to Opt-Out of the Network or to revoke a prior decision to Opt-Out of the Network shall be provided in writing through the Network Participant's or Member Affiliate's patient consent process.
7. Each Network Participant and Member Affiliate shall document and maintain for a period of six years all patient decisions to Opt-Out or to revoke a prior decision to Opt-Out.
8. If a patient exercises their right to Opt-Out, Network Participants and Member Affiliates shall sequester his or her Health Data and shall ensure that the patient's Health Data is not disclosed through the Network.

9. If a patient exercises their right to Opt-Out, Network Participants and Member Affiliates shall submit the patient's personal demographic information to the Network Facilitator for use in the Master Patient Index in accordance with the *Master Patient Index Policy*.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

HIPAA Privacy and Security Rule 45 C.F.R. § 164.520

21st Century Cures Act, Information Blocking Regulations 45 C.F.R. § 171.202

Related Documents

- *Master Patient Index Policy*
- *Opt-Out Policy*
- *Restrictions on Sensitive Health Information Policy*

GaHIN-2003 Minimum Necessary and User Authorization

Purpose of Policy

To ensure that reasonable efforts are made to limit the Health Data transmitted via the Network to the minimum amount necessary to accomplish the intended purpose for which the Health Data is accessed, thereby allowing Patients to have confidence in the privacy of their Health Data as it moves among Network Participants and Member Affiliates via the Network.

Policy Scope

This Policy applies to all Network Participants and Member Affiliates.

Policy Statement

Each Network Participant and Member Affiliate shall have reasonable Minimum Necessary policies and procedures to limit how much Health Data is used, disclosed, and requested for certain purposes. These Minimum Necessary policies and procedures should limit who has access to Health Data and under what conditions based on job responsibilities and the nature of the business.

1. Uses
    a. Use of Health Data must be limited to the minimum amount necessary to accomplish a specified Permitted Purpose.
    b. Each Network Participant and Member Affiliate shall share Health Data obtained through the Network and allow access to such information by only those Workforce members, agents, and contractors who need the information in connection with their job function or duties.
2. Disclosures
    a. Each Network Participant and Member Affiliate shall disclose through the Network only the minimum amount of Health Data as is necessary for the purpose of the disclosure.
    b. Disclosures to a Health Care Provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.
3. Requests
    a. Each Network Participant and Member Affiliate shall request only the minimum amount of Health Data necessary for the intended purpose of the request.
    b. This Policy does not apply to requests by Health Care Providers for treatment purposes. To the extent that Health Data is disclosed for Treatment and some other purpose, this Policy applies.
4. Role-Based Access Standards
    a. Each Network Participant and Member Affiliate shall implement a role-based access system, whereby Authorized Users may include only those members of the Network Participant's or Member Affiliate's Workforce who require access to the Network to facilitate the use and disclosure of Health Data for a Permitted Purpose as part of their job responsibilities. Network Participants and Member Affiliates shall establish and implement policies and procedures that:

        i. Establish categories of Authorized Users;

ii. Define the purposes for which Authorized Users in those categories may access Health Data via the Network; and
iii. Define the types of Health Data that Authorized Users within such categories may access (e.g., demographic data only, clinical data).

b. The purposes for which an Authorized User may access Health Data via the Network and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized User's job function and relationship to the patient.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

HIPAA Privacy Rule 45 C.F.R. §§ 164.502, 164.514

Related Documents

GaHIN-2004 Accounting of Disclosures Policy

Purpose of Policy

The purpose of this policy is to ensure that all Network Participants and Member Affiliates develop and maintain processes through which patients may obtain a record of Protected Health Information (PHI) disclosures upon request.

Policy Scope

This policy applies to all Network Participants and Member Affiliates.

Policy Statement

1. Patients shall have the right to request and obtain an Accounting of Disclosures of their PHI accessed through the Network in accordance with applicable law, including HIPAA and HITECH.
2. Network Participants and Member Affiliates shall provide a formal process through which patients are able to request an Accounting of Disclosures from the Network Participant or Member Affiliate originating the PHI.
3. Network Participants and Member Affiliates shall, upon request, provide a patient with a record of the entities to which they have disclosed the patient's PHI.
4. Network Participants and Member Affiliates shall comply with the requirements of 45 C.F.R. § 164.528 when providing an Accounting of Disclosures to a requesting patient.
5. All requests for an Accounting of Disclosures made to the Network Facilitator shall be forwarded to the appropriate Network Participant or Member Affiliate within 10 business days.
6. The Network Facilitator shall not be obligated to, nor shall it directly respond to, Accounting of Disclosures requests received directly from a patient.
7. The Network Participant or Member Affiliate shall be solely responsible for providing the requested Accounting of Disclosures to the patient in accordance with the HIPAA Regulations.
8. To the extent required by law, the Network Facilitator shall provide information in its possession necessary to enable Network Participants and Member Affiliates to provide a timely response to requests for an Accounting of Disclosures within the timeframe required by the *Member Agreement*.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

HIPAA 45 C.F.R. § 164.528 Accounting of disclosures of protected health information

Related Documents

Member Agreement

GaHIN-2005 Restrictions on Sensitive Health Information

Purpose of Policy

This policy defines how Network Participants and Member Affiliates may disclose Health Data that is subject to greater protection under federal and Georgia law ("Sensitive Health Information" or "SHI") through the Network.

Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of Health Data that may be considered particularly private or sensitive to a Patient.

These laws require strict compliance, and patient fears and concerns about their privacy must be given the utmost attention and respect.

Policy Scope

This Policy applies to all Network Participants and Member Affiliates.

Policy Statement

1. SHI shall include but is not limited to:
    a. Substance abuse records.
    b. Mental health and psychotherapy records.
    c. Genetic testing information.
    d. HIV/AIDS information.
    e. Developmental disability records.
2. The heightened legal requirements for this type of Health Data cannot be adequately addressed by an Opt-Out policy.
3. Depending upon the permitted purpose for which SHI is being sought, the law may require a patient to specifically authorize in writing a disclosure of his or her SHI by signing a document that contains certain elements.
4. Responsibility for restricting the transmission of SHI shall reside with Network Participants and Member Affiliates, consistent with the 21st Century Cures Act Information Blocking exceptions for actions required by law and for preconditions to disclosure.
5. The sending Network Participant or Member Affiliate shall obtain an appropriate consent in accordance with applicable law from the patient prior to disclosing or re-disclosing SHI through the Network.
6. Network Participants and Member Affiliates shall meet all other obligations with respect to such SHI as required by applicable law.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

The HIPAA Privacy Rule 45 C.F.R. § 164.528; 42 C.F.R. Part 2; 45 C.F.R. § 164.508(a)(2)

21st Century Cures Act, Information Blocking Rules 42 U.S.C. 300jj-52, 45 C.F.R. 171.202

O.C.G.A. §§ 26-5-17, 33-54-3, 33-54-6, 43-39-16, 37-3-166, 37-4-125

Related Documents

- *Permitted Purposes*

GaHIN-2006 Digital Certificate Policy

Purpose of Policy

This Policy governs the creation of Digital Certificates to identify Network Participants by name, address of place of business, or other disambiguating information and to enable the encrypted communication of information over the Network. Network Participants shall under the terms of the Member Agreement be obligated to verify identity of their Member Affiliates.

Policy Scope

This Policy applies to all Network Participants in the Network Facilitator's GeorgiaConnX Services.

Policy Statement

1. Documentation Requirements: Prior to the issuance of a Digital Certificate, the Applicant must provide the following documentation, in compliance with the requirements of these Guidelines:
   a. Subscription Agreement;
   b. Member Agreement;
   c. Such additional documentation as the Vendor requires from the Applicant to satisfy its obligations under these Guidelines pursuant to the Member Agreement.

2. Network Participant's Warranties and Representations:
   a. Network Participant represents and warrants, during the period when the Digital Certificate is valid, that the information contained in the Digital Certificate is accurate;
   b. Network Participant warrants that it will not install and use the Digital Certificate until it has reviewed and verified the accuracy of the data contained therein;
   c. Network Participant warrants that it will take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Digital Certificate (and any associated access information or device, e.g. password);
   d. Network Participant warrants that it will install the Digital Certificate only on the server accessible at a Domain Name listed in the Digital Certificate, and to use the Digital Certificate solely in compliance with all Applicable Law, solely for authorized company business, and solely in accordance with the Subscriber Agreement;
   e. Network Participant warrants that it will promptly cease using a Digital Certificate, and promptly request the Vendor to revoke the Digital Certificate, in the event that there is any actual or suspected misuse or compromise of the Network Participant's Private Key associated with the Public Key listed in the Digital Certificate;
   f. Network Participant warrants that it will promptly cease all use of the Private Key corresponding to the Public Key listed in a Digital Certificate upon expiration or revocation of that Digital Certificate.
   g. Network Participant warrants that it will verify the identity of all its Member Affiliates.

3. Time Cycle of Digital
    a. The identified time cycle for assigned Digital Certificates shall be one year from the date of issuance of the Digital Certificate.
    b. During annual renewal of a Digital Certificate, the Network Participant shall validate the information contained within the Digital Certificate.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

HIPAA Privacy Rule 45 C.F.R. Parts 160 and 164

Related Documents

N/A

GaHIN-2007 Breach Notification Policy

Purpose of Policy

The purpose of this policy is to establish a notification process in compliance with Federal and state laws protecting patients from the improper acquisition, access, use or disclosure of PHI by unauthorized persons and entities.

Policy Scope

This policy applies to Network Participants, Member Affiliates, and others with access to the Network including Authorized Contractors.

Policy Statement

This policy sets forth minimum standards that Network Participants, Member Affiliates, and others with access to the Network including Authorized Contractors, shall follow in the event of a Breach of Unsecured PHI.

Definitions

1. **Breach** shall be defined in accordance with 45 C.F.R. § 164.402, as may be amended, to be the unauthorized acquisition, access, use or disclosure of Protected Health Information in a manner not permitted under Subpart E of 45 C.F.R. § 164.402, when such information is exchanged via the Network. The notification process contemplated by Applicable Law applies only if the Breach involves Unsecured PHI. Unsecured PHI means that the PHI has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of encryption or other federally-approved technology.
2. **Unsecured PHI** shall be defined in accordance with 45 C.F.R. § 164.402, as may be amended.
3. **Adverse Security Event** shall be defined as the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content being transacted in a manner permitted by DURSA.
4. An Adverse Security Event shall not include any unintentional acquisition, access, disclosure, or use of Message Content by an individual acting under the authority of the Network Facilitator of the Network Facilitator or an Authorized Individual Contractor if:
    a. Such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the professional relationship of such individual; and
    b. Such unencrypted Message Content is not further acquired, accessed, disclosed, or used by such individual; or
5. An Adverse Security Event shall not include any acquisition, access, disclosure or use of information contained in, or available through, the Network Facilitator's system where such acquisition, access, disclosure, or use was not directly related to transacting Message Content.

Content of Breach Notifications

1. Notification of a Breach of Unsecured PHI shall include sufficient information for the recipient to understand the nature of the Breach; provided, however, that the notification shall not include any PHI.
2. Such notification shall include, to the extent available at the time of the notification, the following information:
    a. Brief description of the Breach.
    b. Description of the roles of the people involved in the Breach (e.g., employees, Network Facilitator, Vendor, Network Participants, Member Affiliates, unauthorized persons, etc.).
    c. A description of the type of PHI subject to the Breach.
    d. Network Participants and their respective Member Affiliates likely impacted by the Breach.
    e. Number of patients or records estimated to be impacted by the Breach.
    f. Actions taken by notifying party to mitigate the Breach.
    g. Current status of the Breach (i.e., under investigation or resolved).
    h. Corrective actions taken to prevent any similar or additional Breaches.
3. In addition, such notifications shall include the information necessary to comply with applicable state laws.
4. Such notifications shall be sent to the Network Facilitator's Privacy Officer and the Security Officer for response.

Network Participant Breach Notifications

1. Network Participant shall follow its policies and procedures to determine if an incident constitutes a Breach Notification Event.
10. Network Participants shall require their Member Affiliates to notify the Network Participant in the event a Member Affiliate determines that there has been a Breach of Health Data consisting of Unsecured PHI that is exchanged via the Network.
11. Network Participants shall notify the Vendor and the Network Facilitator of a Breach of Unsecured PHI by the Network Participant or its Member Affiliate without unreasonable delay, but no later than twenty-four (24) hours after confirming that a Breach has occurred.
12. Network Participant notification shall comply with HIPAA Regulations, HITECH, and applicable federal and state laws.
13. Network Participants shall provide the Vendor with a point of contact so individuals can ask questions or request additional information and shall promptly notify Vendor if the contact changes.
14. In the event of a Breach by a Network Participant or a Member Affiliate, the Vendor and Network Facilitator, in cooperation with each other, may conduct an investigation of such Breach, determine the extent of the Breach, determine corrective actions, and may apply such

sanctions on Network Participants as a result of such Breach as permitted by the applicable Member Agreement.

15. Network Participants and Member Affiliates shall cooperate in any investigation conducted by the Network Facilitator, Vendor, state, or federal government authorities.

Sanctions of Authorized Users

16. Vendor, Network Participants, and Member Affiliates shall apply appropriate sanctions to Authorized Users in the event of a Breach.
17. Such sanctions may include, but shall not be limited to, temporarily restricting an Authorized User's access to the Network, termination by a Network Participant of a Member Affiliate's access to the Network, or such other remedies as Vendor, Network Participant, or Member Affiliate may deem reasonably necessary in accordance with a risk analysis.

DURSA Adverse Event Notifications

The Network Facilitator participates in the eHealth Exchange, or the nationwide Health Information Exchange, and must comply with the Breach notification procedures outlined in the *Data Use and Reciprocal Support Agreement* (DURSA)[1].

1. Network Facilitator shall report an Adverse Security Event (Event) in accordance with *Section 14—Privacy and Security (Breach Notification)*:
    a. If the Event involves Federal data, Network Facilitator shall alert the Federal Participant within one (1) hour of learning that an Event occurred and shall provide notification to all DURSA participants that are likely impacted by the Event and the Coordinating Committee within twenty-four (24) hours.
    b. If the Event does <u>not</u> involve Federal data, Network Facilitator shall provide notification to the DURSA Coordinating Committee and all DURSA Participants that are likely impacted by the Event as soon as reasonably practicable, but no later than five (5) business days.
2. The notification shall include sufficient information for the Coordinating Committee to understand the nature of the Event; provided, however, that the notification shall not include any PHI:
    a. One or two sentence description of the Event.
    b. Description of the roles of the people involved in the Event (e.g., employees, Network Facilitator, Vendor, Network Participants, Member Affiliates, unauthorized persons, etc.).
    c. The type of Message Content involved in the Event.
    d. DURSA Participants likely impacted by the Event.
    e. Number of individuals or records estimated to be impacted by the Event.
    f. Actions taken by the Network Facilitator to mitigate any unauthorized access to, use or disclosure of PHI because of the Event.
    g. Current status of the Event (under investigation or resolved).

[1] https://ehealthexchange.org/dursa/

h. Corrective action taken and steps planned to be taken to prevent a similar Event.

3. Network Facilitator shall supplement the information contained in the notification as it becomes available and shall cooperate with other DURSA Participants and the Coordinating Committee.
4. If the Coordinating Committee determines that non-impacted DURSA Participants would benefit from a summary of the notification or that a summary of the notification would enhance the security of the Network, then the Coordinating Committee may provide, in a timely manner, a summary that does not identify any of the individuals involved in the Event.
5. DURSA *Section 14—Privacy and Security (Breach Notification)* shall not be deemed to supersede the Network Facilitator's obligations (if any) under applicable laws.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

Data Use and Reciprocal Support Agreement (DURSA)[2] *Section 14—Privacy and Security (Breach Notification)*

HIPAA Privacy and Security Rule 45 C.F.R. § 164.400 – 164.414

[2] https://ehealthexchange.org/dursa/

GaHIN-2008 Information Blocking Policy

Purpose of Policy

This Policy addresses the Information Blocking provisions of the 21st Century Cures Act (Cures Act) and implementing regulations.

Policy Scope

This Policy applies to the Georgia Health Information Network, Inc. (GaHIN) and its affiliated entities.

Policy Statement

GaHIN and its HIPAA covered components are committed to making electronic health information (EHI) available and usable for authorized and permitted purposes as required by law. To that end, GaHIN has adopted this Policy to deter Information Blocking.

Regulatory Standards

The Cures Act and implementing regulations set forth standards relating to Information Blocking.

Information Blocking encompasses practices that an Actor knows, or that should know, is likely interfere with, prevent, or materially discourage the access, exchange, or use of EHI. Information Blocking does not include practices that are required by law or covered by one of the eight exceptions outlined below.

The Information Blocking exceptions fall into two categories: (1) Exceptions that involve not fulfilling a request to access, exchange, or use EHI; and (2) Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI. A practice that falls under an exception would not constitute Information Blocking; however, a practice would not constitute Information Blocking merely because it does not meet an exception or does not meet every element of an exception.

If GaHIN determines that an Information Blocking exception applies, then it should document the applicability of such exception and only engage in activities that could constitute Information Blocking with respect to the specific EHI to which the exception applies.

Exceptions that Involve Not Fulfilling Requests

1. **Preventing Harm** – Allows an Actor to take reasonable and necessary steps to prevent harm to a patient or another person when a patient's treating practitioner determines that disclosure poses a risk of harm to the patient or a third party, or when the Actor reasonably believes that disclosure poses a risk of harm caused by misidentified, mismatched, corrupt, or otherwise erroneous data in the EHI.

   Example: Treating provider determines that disclosure poses risk of harm to patient or third party, or EHI is incomplete, inaccurate, or otherwise erroneous, posing a risk of harm.

2. **Privacy –** Allows an Actor to deny a request to access, exchange, or use EHI to protect an individual's privacy, including where: (i) the requestor does not meet a precondition to disclosure under federal or state law, such as obtaining a valid consent for Sensitive Health Information; (ii) the patient is requesting a copy of his or her own EHI that contains Psychotherapy Notes or EHI that an Actor compiled in reasonable anticipation of, or for use in, litigation; and (iii) the patient requests that an Actor deny third parties access to his or her EHI.

   Example: Requestor has not met a precondition to disclosure (e.g., missing HIPAA authorization). A patient, or his or her personal representative, requests Psychotherapy Notes or EHI compiled in anticipation of litigation. A patient has requested that an Actor not disclosure his or her information on a Health Information Exchange.

3. **Security –** Allows an Actor to deny a request to access, exchange, or use EHI to protect the security of the EHI. This exception applies if the Actor either: (i) takes steps pursuant to its written Security Policy; or (ii) makes a case-by-case determination, based on specific facts and circumstances, that the practice is necessary to mitigate the security risk to EHI and there are no reasonable and available alternatives that address the security risk in a manner that is less likely to interfere with the access, exchange, or use of EHI.

   Example: Actions including direct responses to a known security incident or be directly related to the need to verify an individual's identity before granting access to EHI.

4. **Infeasibility –** Allows an Actor to deny a request to access, exchange, or use EHI if responding to the request is infeasible, including: (i) due to a natural disaster or other uncontrollable situation; (ii) because the Actor cannot separate disclosable from non-disclosable EHI; and (iii) in situations where responding to the request is infeasible under the particular circumstances of a request.

   Example: Cannot fulfil request because of a disaster or other uncontrollable situation, or cannot separate disclosable from non-disclosable EHI.

5. **Health IT Performance –** Allows an Actor to take reasonable and necessary measures to make its health IT temporarily unavailable or to degrade the performance of its health IT to benefit the overall performance of the health IT, as well as to stop a third-party application that is negatively impacting health IT performance.

   Example: Cannot fulfil request due to the EHI platform being slowed or shut down for maintenance.

Exceptions that Involve Procedures for Fulfilling Requests

6. **Content and Manner –** Allows an Actor to transmit EHI in a manner different than requested when it is technically unable to fulfil the request or cannot reach agreeable terms with the requestor. The Actor's point of contact, or a designee, is responsible for contacting and negotiating with the requestor, as well as describing how the Actor will fulfil the request if it cannot fulfil the request in the manner requested. Any fees charged pursuant to the Content and Manner exception will be consistent with the Actor's HIPAA fee policies.
7. **Fees –** Allows an Actor to charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI. This exception does not apply to fees charged to individuals or their personal representatives more than the fees permitted under HIPAA (45 CFR 164.524(c)(4)), or for accessing EHI using a provider's online portal or personal health applications. An Actor may not charge a fee to patients or personal representatives who request electronic access to EHI, including via online portal. An Actor may charge fees to a patient or their personal representative who requests other forms of access.
8. **Licensing –** Allows an Actor to license interoperability elements for EHI to be accessed, exchanged, or used. This exception will not apply to an Actor unless it plans to license interoperability elements for EHI.

Definitions

For a complete list of definitions, refer to the *Glossary*.

Authoritative References

The 21st Century Cures Act and Implementing Regulations, 45 CFR Part 170, 45 CFR Part 171

Related Documents

N/A

GaHIN Glossary

A

Accounting of Disclosures shall have the meaning set forth at 45 CFR § 164.528. Network Participants or Member Affiliates make the determination whether to disclose health data and log the disclosure if required to do so under the HIPAA Regulations. The Network Participant or Member Affiliate whose Accounting of Disclosures is being sought by a patient is the only organization that can logically evaluate and provide a full Accounting of Disclosures of a patient's health data that is PHI.

Acknowledgement shall have the meaning set forth at 45 CFR § 164.520.

Adverse Security Event shall be defined as the unauthorized acquisition, access, disclosure, or use of unencrypted Message Content being transacted in a manner permitted by DURSA. An Adverse Security Event does not include the following:

1. Any unintentional acquisition, access, disclosure, or use of Message Content by an individual acting under the authority of the Network Facilitator if:
    a. Such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the professional relationship of such individual; and
    b. Such unencrypted Message Content is not further acquired, accessed, disclosed, or used by such individual; or
2. Any acquisition, access, disclosure or use of information contained in, or available through, the Network Facilitator's system where such acquisition, access, disclosure, or use was not directly related to transacting Message Content.

Agreement shall mean a Member Agreement.

Applicable Law shall be defined as all applicable statutes, rules, and regulations of the State of Georgia, as well as all applicable federal statutes, rules, and regulations, including without limitation, HIPAA, HITECH, the Minimum Necessary Standard, and 42 C.F.R. Part 2 ("Confidentiality of Alcohol and Drug Abuse Patient Records").

Authorized User means a member of the Workforce of a Network Participant or a Member Affiliate who has been designated by that Network Participant or Member Affiliate to access the Network pursuant to the concept of role-based access control. An Authorized User may also be a member of Network Facilitator's or Vendor's Workforce; or a member of the Workforce of a Business Associate of Network Facilitator or Vendor.

B

Breach shall be defined to be the unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted under Subpart E of 45 C.F.R. § 164.402, as may be amended, which compromises the security or privacy of the PHI, when such information is exchanged via the Network. A Breach is also defined as a DURSA Breach.

> **DURSA Breach** is a subset of Breach and shall mean the unauthorized acquisition, access, disclosure, or use of Message Content (which includes Protected Health Information, de-identified data, individually identifiable information, pseudonymized data, metadata, schema, and digital credentials) while sending, requesting, receiving, responding to, or otherwise

exchanging or disclosing Health Data via the eHealth Exchange, or the nationwide health information network. "DURSA Breach" does not include the following: (1) any unintentional acquisition, access, disclosure, or use of Message Content by an employee or individual acting under the authority of a Network Participant or Member Affiliate if: (a) such acquisition, access, disclosure or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Network Participant or Member Affiliate; and (b) such Message Content is not further acquired, accessed, disclosed, or used by such employee or individual; or (2) any acquisition, access, disclosure or use of information contained in or available through the Network Participant's systems where such acquisition, access, disclosure or use was not directly related to sending, requesting, receiving, responding to, or otherwise exchanging or disclosing Message Content via the eHealth Exchange.

The term Breach does not include the following:

1. Any unintentional acquisition, access, disclosure, or use of health data through the Network by an employee or individual acting under the authority of Vendor, Participant, or Participant User if:
    a. Such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with Vendor, the Participant, or Participant User; and
    b. Such Health Data is not further acquired, accessed, used, or disclosed by such employee or individual; or
2. Any acquisition, access, disclosure or use of information contained in or available through the Participant's System where such acquisition, access, disclosure, or use was not directly related to transmission of health data through the Network.

Business Associate shall have the meaning set forth at 45 C.F.R. § 160.103.

Business Associate Agreement means a contract between a Covered Entity under HIPAA and a Business Associate, or between Business Associates, which obligates the Business Associate to maintain the privacy and security of Protected Health Information in accordance with the requirements of the HIPAA Regulations.

C

Common Network Resource shall mean software, utilities and automated tools made available for use in connection with the Network and which have been designated as a "Common Network Resource" by Vendor.

Covered Entity shall have the meaning given to it in the HIPAA Privacy and Security Rules, as amended.

D

De-identification shall mean the process of anonymizing data so that the risk of re-identifying an individual is minimized to an acceptable level in accordance with 45 CFR 164.514.

Designated Record Set shall have the meaning set forth at 45 C.F.R. § 164.501. The Network Participants or Member Affiliates are the originators of health data containing PHI and maintain the designated record sets in which PHI resides.

Direct Secure Messaging Service shall mean the SMTP Service and the XDR Service.

DURSA shall mean the *Data Use and Reciprocal Support Agreement* entered into by the Network Facilitator[3].

E

Electronic Health Information (EHI) shall mean electronic PHI as defined in 45 CFR 160.103, to the extent it would be included in a Designated Record Set, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103.

G

GaHIN: see Network Facilitator.

H

Health Care Operations shall have the meaning set forth at 45 C.F.R. § 164.501.

Health Care Provider shall have the meaning set forth at 45 C.F.R. § 160.103.

Health Care Provider Health Data shall mean only that Health Data that is, or could reasonably be expected to be, useful for Treatment, Payment, and Health Care Operations, all in accordance with HIPAA Regulations.

Health Data shall be defined as any electronic healthcare information which is requested, disclosed, stored on, made available on, or sent by a Participant through the Network. Health Data shall include, but may not be limited to, Health Care Provider Health Data, Health Plan Health Data, HIO Health Data, Protected Health Information, Individually Identifiable Health Information, Health Information, de-identified data, limited data sets, pseudonymized data, metadata, and schema.

Health Information shall be defined as any information, including genetic information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

18. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Information Exchange means a system for the electronic transfer of Protected Health Information between participating organizations for a permissible purpose based upon the requirements of federal and state law.

Health Information Organization (HIO) shall mean an organization that oversees and governs the exchange of health-related information, other than the Network Facilitator.

[3] https://ehealthexchange.org/dursa/

Health Plan shall have the meaning set forth at 45 C.F.R. § 160.103.

Health Plan Health Data shall mean that Health Data that includes admission, discharge, and transfer data of Patients covered by the Health Plan requesting such data and such other Health Data as approved in writing by a majority of the Network Participants, in accordance with HIPAA Regulations, including the Minimum Necessary Standard.

HIO Health Data shall mean that Health Data that is, or could reasonably be expected to be, useful for Treatment, Payment, or Health Care Operations, all in accordance with HIPAA Regulations.

HIPAA shall mean the Health Insurance Portability and Accountability Act of 1996, as amended by HITECH, as currently in effect and as may be amended, modified, or renumbered.

HIPAA Regulations shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160, 162 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) of the American Recovery and Reinvestment Act of 2009, as in effect on the date of the Agreement and as may be amended, modified, or renumbered.

HITECH shall mean the Health Information Technology for Economic and Clinical Health Act of 2009 (which is part of the American Recovery and Reinvestment Act of 2009 (45 C.F.R. Part 495)), as amended, and any of its implementing regulations.

I

Individual shall be defined as a person who is the subject of PHI and shall include a person who qualifies as a personal representative.

Individually Identifiable Health Information shall have the meaning set forth at 45 C.F.R. § 160.103.

Limited Data Set shall mean a data set with fewer identifiers deleted than a “safe harbor” de-identified data set. The Limited Data Set allows the inclusion of all dates, 5-digit ZIP codes, and city as indirect identifiers. A limited data set can only be used for research, public health, or operations. Its use or disclosure may be further limited by the purpose statements in the Data Use Agreement. HIPAA defined sixteen identifiers that must be deleted in order for the information to be considered a limited data set.

M

Master Patient Index (MPI) means the index wherein Personal Demographic Information of Patients is securely maintained by the Network to record their decision to Opt-Out of the Network. For those Patients who have not elected to Opt-Out, the Master Patient Index shall be used to match the Patients with any inquiries seeking the exchange of Protected Health Information for a Permitted Purpose. The Network shall maintain Personal Demographic Information regarding all potential individual Patients in this Master Patient Index, even if the decision is made to Opt-Out, in order to minimize the possibility of improperly matching Patients.

Member Affiliates shall mean those persons who have been authorized by a Network Participant to access Health Data through the Network and in a manner defined by such Network Participant, in compliance with the terms and conditions of the Member Agreement and Applicable Law.

Member Agreement shall mean that certain agreement entered into by and between the Network Facilitator for statewide health information exchange services, and Network Participant, as may be amended and/or restated from time to time.

Message Content shall mean an electronic transmission of information contained within a message or accompanying a message as specified by DURSA. This information includes, but is not limited to, Protected Health Information (PHI), de-identified data (as defined in the HIPAA Regulations at 45 C.F.R. § 164.514), individually identifiable information, pseudonymized data, metadata, digital credentials, and schema.

Minimum Necessary Standard shall mean the "minimum necessary standard" as set forth in 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d), as the same may be amended from time to time.

N

Network shall mean the network that allows for the exchange of Health Data and/or information between and among Network Participants and Participant Users as described in the Member Agreement.

Network Facilitator shall mean the Georgia Health Information Network, Inc. (GaHIN).

Network Participant shall mean any organization that (i) is a Health Care Provider, Health Plan, State Agency, or Health Information Organization; (ii) meets the requirements for participation in the Network as contained in the Network Operating Policies and Technical Requirements; and (iii) has entered into an Agreement.

Notice or **Notify** shall mean a written communication, unless otherwise specified in the Agreement, sent to the appropriate Party's representative at the address listed in the Member Agreement.

Notice of Privacy Practices shall have the meaning set forth at 45 CFR § 164.520.

O

O.C.G.A. shall mean the Official Code of Georgia Annotated.

Opt-Out means a process under which any Patient who does not wish to have his or her Health Data exchanged with other Network Participants through the Network may affirmatively express his or her decision not to participate.

P

Patient means the individual whose Personal Demographic Information or Protected Health Information is subject to electronic storage and transfer by the Network. "Patient" includes a personal representative who has the authority to authorize the disclosure of a Patient's Protected Health Information pursuant to 45 C.F.R. § 164.502(g) and any other Applicable Law.

Payment shall have the meaning given such term at 45 C.F.R. § 164.501.

Personal Demographic Information means information which may be used to individually identify a Patient, and may include, but not be limited to, name, address, Social Security number, date of birth, telephone number, and driver's license number.

PHI: See Protected Health Information.

Protected Health Information (PHI) shall mean individually identifiable health information:

1. Except as provided in paragraph (of this definition, that is:
    a. Transmitted by electronic media;
    b. Maintained in electronic media; or
    c. Transmitted or maintained in any other form or medium.
2. Protected health information excludes individually identifiable health information:
    c. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
    d. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
    e. In employment records held by a covered entity in its role as employer; and
    f. Regarding a person who has been deceased for more than 50 years.

R

Required By Law shall have the meaning set forth at 45 C.F.R. § 164.103.

S

Sensitive Health Information shall mean drug and alcohol records as defined by 42 C.F.R. Part 2; genetic information as defined by O.C.G.A. § 33-54-2; mental health records as defined by 45 C.F.R. § 164.508(a)(2) and 45 C.F.R. § 164.501 and O.C.G.A. §§ 43-39-16, 37-3-166, 37-1-1; HIV/AIDS information as defined by O.C.G.A. §§ 31-22-9.1, 24-12-20, and 24-12-21; and mental retardation records as defined by O.C.G.A. §§ 37-4-125 and 37-1-1(8). Sensitive Health Information may also be referred to as SHI.

Services shall mean the provision and use of the Network and all related services, including, without limitation, the Direct Secure Messaging Service, currently offered by GaHIN under the name "GeorgiaDirect".

State Agency shall have the meaning set forth in O.C.G.A. § 50-5-82(a).

Suspected Breach shall refer to the point at which either the Network Facilitator, Vendor, Network Participant, or Member Affiliate discovers information that leads it to reasonably believe that a Breach may have occurred.

System shall mean software, portal, platform, or other electronic medium controlled by a Participant through which the Participant sends, receives, discloses or uses Health Data through or from the Network. For the purposes of this definition, it shall not matter whether the Participant controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.

T

Treatment shall have the meaning set forth at 45 CFR § 164.501 of the HIPAA Regulations.

U

Unsecured PHI shall be defined in accordance with 45 C.F.R. § 164.402, as may be amended.

W

Workforce has the same meaning as the term is defined in 45 C.F.R. Part 160, as may be amended.

X

XDR Service shall mean the encrypted secure direct messaging service provided by Vendor utilizing the Cross-enterprise Document Reliable Interchange ("**XDR**") integration profile in the Network that allows exchange of Health Data in CCDA format between and among Participants and Participant Users through the Network.