Data Breach Response Policy

Effective Date [Version]:
January 10, 2024

Background and Purpose

CommonWell Health Alliance, Inc. ("Alliance") is committed to defining and promoting a national infrastructure with common standards and policies that promote a vendor-neutral platform to break down the technological and process barriers that currently inhibit effective health data exchange.

Alliance and its Authorized Users are committed to complying with all applicable laws and regulations. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Federal Agencies Serving as Authorized Users. Notwithstanding anything to the contrary in this Breach Incident Notification Policy ("Policy"), a federal agency that is serving as an Authorized User and is not otherwise subject to the HIPAA Rules is not required to comply with the HIPAA Privacy and Security Rules referenced in this Policy. The federal agency will comply with all privacy and security requirements imposed by applicable federal law.

Due to the above requirements, Alliance has adopted this Policy, however, nothing in this Policy shall be deemed to modify or replace any breach notification requirements under HIPAA, the FTC Rule, and/or other Applicable Law.

Definitions used in this Policy that are not defined elsewhere in the Policy are defined in the Definitions section.

Application

This Policy identifies the standards and requirements that are applicable to any party that accesses or uses the Services, including Authorized Users.

Federal Agencies Serving as Authorized Users. Notwithstanding anything to the contrary in this Policy, a federal agency that is serving as an Authorized User is not required to comply with this Policy. The federal agency will comply with the UC-CERT Federal Incident Reporting Guidelines as required by the Federal Information Security Modernization Act (FISMA), per 44 U.S.C. §§ 3553-54 and federal agency policy in accordance with the Office of Management and Budget guidance.

Terms and Conditions

1. General Obligations.

(a) Event Notification Obligations. As soon as reasonably practicable, but no later than five (5) business days (or such shorter period specified by the applicable Business Associate Agreement) after a Breach is Discovered and is likely to have an adverse impact on the Alliance Services or network or another Authorized User, Authorized User shall provide a notification to Alliance, Service Provider, and all Authorized Users that are likely impacted by the Breach. Authorized User shall supplement the information contained in the notification as it becomes available and cooperate with other Authorized Users and Alliance. For the purpose of this Policy, a Breach is treated as "discovered" or "learned"

by Authorized User on the first day the Breach is known, or would have been known with reasonable diligence, by any person (other than the person committing the Breach) who is a workforce member, officer *or agent* of the reporting party.

(b) Event Notifications Involving Federal Participants. Notwithstanding the foregoing, Authorized User agrees that: (a) within one (1) hour of learning that a Breach occurred and that such Breach may involve a Federal Participant, it shall alert the Federal Participant in accordance with the procedures and contacts provided by such Federal Participant, and; (b) that within twenty-four (24) hours after determining that a Breach has occurred and is likely to have an adverse impact on a Federal Participant(s), Authorized User shall provide a notification to all such Authorized Users that are likely impacted by the Breach, in accordance with the procedures and contacts provided by such Federal Participant. The Notification should include sufficient information for the Federal Participant to understand the nature of the Breach.

2. Presumption of a Breach. Except for the categories listed in Section 3 below, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a Breach unless Authorized Users can demonstrate that there is a low probability that the PHI has been compromised. In order to make this determination, the Privacy Officer will perform, and document the outcome of, a risk assessment taking into account at least the following 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.

3. Exceptions to the Definition of Breach. Incidents that fall into one of the following categories are not Breaches and, thus, are not required to be reported pursuant to this Policy (unless state law requires a report):

(a) Certain Unintentional Uses. Any unintentional acquisition, access, or use of PHI by Authorized Users or any individual acting under the authority of Authorized Users if: (i) the acquisition, access, or use was made in good faith and within the course and scope of authority; and (ii) the information is not further used or disclosed in a manner not permitted by the HIPAA Rules.

(b) Certain Inadvertent Disclosures. Any inadvertent disclosure by a person who is authorized to access PHI at Authorized User or a subcontractor of Authorized User if the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Rules.

(c) Incidents Involving no Ability to Retain PHI. A disclosure of PHI where Authorized User or its subcontractor has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office).

4. Content of Notice to Client(s). The notification to the Alliance and Service Provider will include, to the extent possible, the following information: (a) names of each individual

whose PHI was or is reasonably believed to have been affected by the Breach; and (b) any other available information to assist the Alliance and Service Provider with meeting its obligation to notify individuals (i.e., a description of the Breach, the date of the Breach, a list of individuals affected by the Breach, a description of the types of Unsecured PHI involved, and a description of actions being taken to mitigate harm and prevent further Breaches).

5. Other Notice to Alliance and Service Provider. Even if an incident is determined to not be a Breach, Authorized User will report any incident that constitutes a non-permitted use, disclosure or Security Incident to the affected Alliance and Service Provider(s) as specified in the applicable Business Associate Agreement(s). Clients may also perform their own Breach analysis.

6. Applicable law. Authorized User will comply with any applicable state law requirements that impose additional breach notification duties or more restrictive breach obligations (such state laws may apply to personal information that is not considered to be PHI).

7. Law Enforcement Delay for Notices to Client. Authorized User must delay notification to affected Alliance and Service Providers of a Breach if a law enforcement official states that notification would impede a criminal investigation or cause damage to national security as follows: (a) if the law enforcement statement is in writing, Authorized User will delay the notification or posting for the time period specified in the statement; or (b) if the law enforcement statement is made orally, Authorized User will delay the notification or posting for the time period requested or for 30 days, whichever time period is shorter. If the law enforcement official confirms an oral statement with a written request to delay notification or posting, Authorized User will delay the notification or posting for the time period specified in the written statement.

8. Notification of Individuals/HHS/Media (if requested by Alliance and Service Provider(s)). In the event of a Breach, Authorized User will cooperate with Alliance and Service Provider(s) in making required notices.

9. Other Policies. Authorized User will, to the extent applicable: (a) train its workforce members on this Policy; (b) accept complaints from individuals concerning its compliance with this Policy; (c) implement sanctions for violations of this Policy; (d) refrain from intimidating, threatening, coercing, discriminating against, or taking other retaliatory action against any individual for exercising his or her rights under this Policy or any other aspect of the HIPAA Rules; and (e) not require individuals to waive their rights under this Policy.

10. Documentation. Authorized User will document risk assessments performed pursuant to this Policy, incident reports, Breach notifications provided to Alliance and Service Providers and any other third party, and other documentation created pursuant to this Policy for at least 6 years from the date the documentation was created or was last in effect, whichever is later.

11. Definitions. In addition to terms defined elsewhere in this Policy, the following defined terms shall apply:

“Affiliated Networks” means networks that operate with or connect to the Services and/or network, including those currently existing and those that may come to exist in the future.

"Alliance Policies" means all policies approved by the Alliance relating to the Alliance or the Services, as updated from time to time.

"Alliance Specification" means each document designated a "CommonWell Health Alliance Specification" as finally adopted and approved by the Alliance. The most current version of the Alliance Specification may be obtained here: https://www.commonwellalliance.org/connect-to-the-network/use-cases-and-specifications/

"Applicable Laws" means all laws (including common law), statutes, rules, regulations, ordinances, formal written guidance, codes, permits and other authorizations and approvals having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including without limitation agreements and operating procedures required to operate with any government agency or government sponsored healthcare exchange.

"Authorized User" means a party that accesses or uses the Services in accordance with an authorized Use Case that has a written agreement directly an Authorized User or Alliance.

"Breach" has the meaning provided for in 45 CFR 164.402 (Definitions, effective March 26, 2013; 78 Federal Register 5695) or its successor.

"Breach of Confidentiality or Security" means an incident that is reasonably likely to adversely affect: (a) the viability, security, or reputation of the Services, or (b) the legal liability of Alliance, Service Provider, or any Member.

"Data" means the information and files that a Authorized User may receive from or deliver to Alliance, a Service Provider, or another Authorized User, through the Services, but not PHI.

"Downstream Authorized User" means a party with a written agreement directly with an Authorized User, and each subsequent Downstream Authorized User.

"Federal Participant" means those Authorized Users that are Federal agencies.

"Health Data" means health information, including information and PHI that is received, transmitted, stored or maintained through the Services.

"HIPAA" or "HIPAA Rules" means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations and rules.

"Individual User" means an individual that uses the Services on an individual basis, and where such individual is not an End User or Patient, such as a PHR user or Licensed User.

"Member" means legal entity that is a party to a valid Alliance Membership Agreement with Alliance.

"Privacy Officer" means Alliance's Privacy Officer who may be contacted at the following email: privacy@commonwellalliace.org.

"Protected Health Information" or "PHI" means will have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, as applied to the information

created, received, maintained or transmitted by Alliance on behalf of its Members. All references to PHI include Electronic PHI.

“Security Incident” will have the meaning given to such term in 45 C.F.R.

“Services” means the services approved and offered by or on behalf of the Alliance in accordance with an approved Alliance Use Case. Services may also include offerings from Affiliated Networks.

“Service Provider” means a party that Alliance has contracted with to provide the Services (or a subset of the Services).

“Use Case” means a use case approved by the Alliance, as further defined in the Alliance Specification, including a list of technical specifications, obligations, and events, necessary to implement a compliant implementation of such use case.