Data Privacy and Security Policy and Statement of Information Handling Practices

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.

We are committed to supporting a robust privacy and security standard for all data exchanges through the Alliance Services. As such, the Services and Alliance Specifications are designed with privacy as a key consideration.

Definitions used in this Data Privacy and Security Policy and Statement of Information Handling Practices (the "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.

Compliance with Laws

This Policy does not supersede or replace any Applicable Laws, including HIPAA, or any federal or state laws or regulations applicable to Alliance, or any Authorized Users. In their use of the Services, Authorized Users represent and warrant that they shall remain compliant with all Applicable Laws related to the use of the Services. All Covered Entities are required to enter into Business Associate Agreements with other Covered Entities as required by law.

Use and Disclosure of Health Information

Authorized Users shall request, access, use, and disclose Health Data made available through the Services only in accordance with all Applicable Laws.

Health Data shall be used by or on behalf of Authorized Users only as necessary to provide or receive the benefit of the Services, including to carry out the following related to the Services: (a) submitting requests for Health Data relating to individual patients, (b) identifying whether other Authorized Users maintain Health Data relating to those patients, (c) requesting such Health Data from Authorized Users maintaining it, (d) transmitting requested Health Data to the requesting Authorized Users, or (e) as otherwise specifically approved by Alliance in accordance with an authorized Use Case, and for no other purposes.

In addition, Alliance or Service Provider may de-identify PHI, as defined in 45 CFR § 164.514(b)(1) and 164.514(b)(2), and store Health Data and de-identified PHI for the sole purposes of providing the Services in accordance with the terms of the applicable service agreement between Alliance and Service Provider, and for no other purpose.

Patient Consents and Notification

Authorized Users are required to obtain all necessary patient consents and authorizations required under Applicable Law. Patient consents must be: (a) made with full transparency and education, (b) made only after the patient has had sufficient time to review any applicable educational material, (c) commensurate with the circumstances for which the Health Data is exchanged, (d) not used for discriminatory purposes or as a condition for receiving medical treatment, (e) consistent with patient expectations, and (f) revocable at any time.

Identity Management and Authentication

Each Authorized Users is fully responsible for all uses of any applicable Login Credentials issued to it or created by it or its users, and for authentication and identity management of each user accessing the Services on behalf of Authorized Users, and for ensuring that such Login Credentials are unique to each user, and that such credentials remain secure. Authorized Users are required to ensure that each of its users accessing Health Data using the Services is properly identified, authenticated and authorized under Applicable Law to access such Health Data.

System and Network Security Requirements

Authorized Users are required to maintain a secure information technology environment and to use appropriate technical, administrative and physical safeguards to prevent the use or disclosure of PHI other than as permitted hereunder, including appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of PHI accessed or disclosed through the Services. Authorized Users representing Business Associates or Covered Entities are required to develop, implement, maintain and use the safeguards identified in HIPAA Security Rule, 45 C.F.R. Part 160 and 164, Subparts A and C.

Adopters are required to: (a) connect via secure web services connections or through virtual private network (VPN) connection between its local area network (LAN) and the Services, (b) implement, use and maintain commercially reasonable firewall technology, (c) implement, maintain and assume all costs for a business class virus protection solution on the Authorized User's network and computers, and (d) monitor and investigate potential or actual fraudulent activity that involves the Services.

Information Blocking

Authorized User agrees to comply with all Information Blocking regulations and shall not conduct practices that constitute information blocking under Section 4004 of the Cures Act,

including where no applicable exception applies: (a) practices that restrict authorized access, exchange or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health information technologies (health IT); (b) implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging or using EHI; (c) implementing health IT in ways that are likely to: (i) restrict the access, exchange or use of EHI with respect to exporting complete information sets or in transitioning between health IT systems; or (ii) lead to fraud, waste or abuse, or impede innovations and advancements in health information access, exchange and use, including care delivery enabled by health IT.

Breach and Notification

Unless Applicable Laws require earlier notice, Authorized Users are required to report any Breach or Breach of Confidentiality and Security involving the Services in accordance with the Alliance Breach Notification Policy available at www.commonwellalliance.org/commonwell-breach-incident-notification-policy.

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 the Alliance Breach Notification Policy referenced in 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.

Prohibited Uses

Authorized Users shall not use the Services to conduct any business or activity, or solicit the performance of any activity, which is prohibited by or would violate any Applicable Laws, or for purposes that may create civil or criminal liability, including: (a) uses which are defamatory, deceptive, obscene, or otherwise inappropriate; (b) uses that violate or infringe upon the rights of any other person, such as unauthorized distribution of copyrighted material; (c) "spamming," sending unsolicited bulk e-mail or other messages using the Services or sending unsolicited advertising or similar conduct; (d) threats to or harassment of another; (e) impersonating another person or other misrepresentation of source; (f) copying, selling, reselling or exploiting any portion of the Services, including Health Data, except as expressly permitted by Alliance in accordance with an approved Use Case; and (g) assisting or permitting any persons in engaging in any of the activities described in this paragraph. Authorized Users shall not expose or introduce or facilitate the exposure or introduction of any Malicious Code into the Services, or any Alliance system or network, or the systems or networks of any Authorized Users, Alliance Member or Alliance Service Provider. .

Definitions

In addition to terms defined above, capitalized terms in this Policy have the following meanings:

"Alliance Policies" means all policies approved by the Alliance relating to the Alliance or the Services.

"Alliance Specification" means each document designated as a "CommonWell Health Alliance Specification" as finally adopted and approved by the Alliance.

"Applicable Laws" means all applicable federal, state, and local laws, including but not limited to privacy laws, HIPAA, and those concerning the use of PHI related to minors, personally identifiable information, and sensitive personal information.

"Authorized User" means an individual or legal entity that accesses or uses the Services in accordance with an authorized Use Case, and where such entity has an agreement directly with Alliance, another Authorized User, or Downstream Authorized User.

"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 or any Authorized User.

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

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

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

"Login Credential" means unique user identification and password combination, as well as any other applicable security measures that are required by Service Provider to allow Authorized User or its representatives to gain access to the Services.

"Malicious Code" means any viruses, worms, unauthorized cookies, trojans, malicious software, malware or other program, script, routine, subroutine or data that may disrupt, or is designed to disrupt, the proper operation of software, hardware, networks or systems.

"Member" means a person or legal entity that is a member of Alliance.

"Protected Health Information" or "PHI" has the meaning set forth in 45 C.F.R. 160.103, as applied to the information created, received, transmitted or maintained through the Services.

“Service Provider” means a service provider that provides services relating to the Services, on behalf of Alliance.

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

“Use Case” means a use case approved by 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.

Effective Date: *November 12, 2020*