HIPAA Privacy Policy #27
Uses and Disclosures of Protected Health Information
Without Patient Authorization
to Business Associates

Effective Date: January 22, 2020	Refer to Privacy Rule Sections: 160.103; 164.308; 164.502; 164.504; 164.508; 164.528; 164.530
Authorized by: Equinox Board of Directors	Version #:

Policy: Equinox, Inc. may disclose Protected Health Information to a Business Associate and allow a Business Associate to create and receive Protected Health Information on Equinox, Inc.'s behalf without a patient's written Authorization according to the Procedures listed below. *45 C.F.R. §§ 164.502(a)(3), 164.502(e).*

Procedures:

1. Identify Business Associates: In general terms, a Business Associate is a person or entity that performs a service for Equinox, Inc., which involves the use of Protected Health Information. In more specific terms, a Business Associate is a person or entity (other than a member of Equinox, Inc.'s Workforce) that creates, receives, maintains, or transmits Protected Health Information in performing a function or service for, or on behalf of, Equinox, Inc. A subcontractor is a person (other than a member of the Business Associate's Workforce) to whom a Business Associate delegates a function, activity, or service. A subcontractor that creates, receives, maintains or transmits Protected Health Information on behalf of a Business Associate is also a Business Associate as defined in this section. *45 C.F.R. § 160.103(3)(iii)*.

    a. Examples of Business Associates: Business Associates include lawyers, malpractice insurers, e-prescribing gateways, health information organizations, billing companies, consultants, copy services, and any other person who may provide services that inherently involve the use of Protected Health Information. *45 C.F.R. § 160.103(3).*

    b. Who are not Business Associates?: A person or entity is not a business associate if the person or entity performs a service for Equinox, Inc. which involves incidental access to Protected Health Information. For example, the United States Postal Service may carry Protected Health Information for Equinox, Inc., but it would not normally have access to the Protected Health Information. Additionally, a janitorial service is not typically a Business Associate because its services would not involve the use of Protected Health Information except in unusual or unintended circumstances. *45 C.F.R. § 160.103.*

2. Enter into Business Associate Agreements: In order to share Protected Health Information with a Business Associate, and in order to allow a Business Associate to receive Protected Health Information on our behalf, Equinox, Inc. must enter into a written agreement with the Business Associate, in which the Business Associate agrees to appropriately safeguard the information. A subcontractor that has been designated as a Business Associate need not enter an Agreement with

Equinox, Inc. However, the subcontractor must enter a written agreement with the Business Associate agreeing to abide by the same restrictions relating to Protected Health Information that apply to the Business Associate. *45 C.F.R. §§ 164.504(e)(1), 164.504(e)(5), 164.308(b)(1).*

3. Limits of a Business Associates' Use of Protected Health Information: A Business Associate may only use or disclose Protected Health Information if the use or disclosure is permitted or required under its Business Associate Agreement or is required by law. Equinox, Inc. cannot permit a Business Associate to use or disclose Protected Health Information if such use or disclosure by Equinox, Inc. itself would violate HIPAA or New York law, except as necessary for proper management and administration of the Business Associate or to provide data aggregation services with respect to health care operations of Equinox, Inc. *45 C.F.R. §§ 164.502(a)(3)-(4), 164.504(e)(2)(i).*

4. Ensure Proper Format of Agreement: Equinox, Inc. must ensure that all Business Associate Agreements contain certain mandatory information and must substantially conform to Attachment 1, entitled "Sample Business Associate Agreement Provisions." If a Business Associate refuses to sign Equinox, Inc.'s Business Associate Agreement, and/or requires Equinox, Inc. to sign an alternate agreement, Equinox, Inc. must forward the alternate agreement to the Privacy Officer. The Privacy Officer should consult with legal counsel, as necessary, if there is any uncertainty about whether an alternate agreement complies with HIPAA and protects Equinox, Inc.'s interests. *45 C.F.R. § 164.504(e)(1), (2).*

5. Identify and Respond to Breach by Business Associates: If Equinox, Inc. discovers that a Business Associate has failed to meet its responsibilities under a Business Associate Agreement, Equinox, Inc. must take the following immediate action: *45 C.F.R. § 164.504(e)(1)(i)–(iii); § 164.530(f)* (general duty of mitigation).

    a. Notify Privacy Officer: Such instances must be brought to the Privacy Officer's attention immediately.

    b. Send Notice to Business Associate: The Privacy Officer must notify Business Associates in writing of the perceived breach.

    c. Afford Opportunity to Correct Behavior: The written notice should afford the Business Associate a reasonable opportunity to correct any breach that is not serious. (A serious breach, for example, would exist where the Business Associate has sold Protected Health Information or used Protected Health Information for malicious purposes). Generally, thirty (30) days is a reasonable opportunity to correct a breach.

    d. Terminate Relationship if Breach is Serious or Uncorrected: If the breach is serious or if the Business Associate fails to correct its behavior after being given a reasonable opportunity, then the Privacy Officer should terminate the Business Associate Agreement and the underlying business relationship with the Business Associate.

6. Minimum Necessary: When making a disclosure pursuant to this Policy, Equinox, Inc. may only disclose the minimum amount of information necessary for the purpose of the disclosure. Additionally, a Business Associate may not disclose more than the minimum amount of information necessary for the purpose of their disclosure. *See* Equinox, Inc.'s Policy No. 7 entitled "Minimum Necessary Uses, Disclosures and Requests of Protected Health Information." *45 C.F.R. § 164.502(b)(1).*

7. Log of Disclosures: Equinox, Inc. is not required to log disclosures of records created in hard copy paper format made pursuant to this Policy in the patient's Log for Accounting of Disclosures (*See* Equinox, Inc.'s Policy No. 32 entitled "Accounting of Disclosures").[1] However, disclosures of Protected Health Information to carry out treatment, payment and health care operations made through an electronic health record are not exempt from the accounting requirement and must be included in the patient's Log for Accounting of Disclosures. **New York law additionally requires Equinox, Inc. to make a notation in a patient's file or record of the purpose for every disclosure to a third party (including disclosures made under this Policy), except disclosures to practitioners under contract with Equinox, Inc. and certain government agencies.** ***45 C.F.R. § 164.528(a); N.Y. Public Health Law § 18(6).***

8. Special Protection for Highly Sensitive Protected Health Information: In accordance with certain Federal and New York State laws, Equinox, Inc. must provide greater privacy protections to highly sensitive Protected Health Information, which includes information that relates to HIV, Mental Health, Psychotherapy Notes, Alcohol and Substance Abuse Treatment, and Genetics. The Privacy Officer, and legal counsel when appropriate, should be consulted prior to the disclosure of such information. *See* Equinox, Inc.'s Policy No. 14 entitled "Uses and Disclosures of Highly Sensitive Protected Health Information."

1 Section 13405(c) of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, enacted in 2009, requires the Department of Health and Human Services ("HHS") to revise the HIPAA Privacy Rule to require Covered Entities to account for disclosures of Protected Health Information to carry out treatment, payment and healthcare operations if such disclosures are through an electronic health record. In May 2010, HHS issued a Request for Information in the Federal Register seeking comments from the public on the interests of various constituencies concerning this new accounting requirement. HHS is still working on preparing guidance on this issue, and the Privacy Rule does not currently contain a requirement that Covered Entities account for disclosures of electronic health records containing Protected Health Information to carry out treatment, payment and health care operations.

Attachment 1

Business Associate Contracts

SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS[2]

(Published January 25, 2013)

Introduction

A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to

2 Reprinted from www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

1. Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

a. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

b. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

c. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations and Activities of Business Associate

Business Associate agrees to:

a. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

b. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

c. Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

d. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

e. Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

f. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

g. Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

h. To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

i Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate

a. Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

b. Business associate may use or disclose protected health information as required by law.

c. Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

d. Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

e. [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

f. [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

g. [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

4. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

a. [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

b. [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

c. [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

5. Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

5. Term and Termination

a. Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

b. Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

c. Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and

5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

d. Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

6. Miscellaneous [Optional]

a. [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

b. [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

c. [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.