**HIPAA Privacy Policy #39**
**Breach Notification**

| | |
|---|---|
| Effective Date:<br>January 22, 2020 | Refer to Privacy Rule Sections: 160.103; 164.314; 164.402; 164.404; 164.406; 164.408; 164.410; 164.412; 164.520 |
| Authorized by:<br>Equinox Board of Directors | Version #: |

**Policy**: This Policy describes Equinox, Inc. responsibilities that relate to a breach of Protected Health Information. Equinox, Inc. must provide breach notification in all situations except those in which Equinox, Inc. has determined that there is a low probability that the Protected Health Information has been compromised (or one of the other exceptions outlined in Section 2 "Procedures/Responsibilities" applies). The Privacy Officer is responsible for determining if a Privacy Incident constitutes a privacy violation or breach by conducting an investigation and risk assessment to determine the probability that protected heath information has been compromised by utilizing the Attachment 1 form entitled "Breach Notification Risk Assessment Tool" for guidance in analyzing each suspected breach. Equinox, Inc. personnel should consult with the Privacy Officer who may consult with legal counsel. Equinox, Inc. must notify the affected parties of a breach of Protected Health Information in accordance with the Procedures listed below.

**Procedures / Responsibilities**:

1. What is a Breach? A breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not otherwise permitted under the law. The permitted acquisitions, accesses, uses, and disclosures are discussed throughout this Privacy Policy. *45 C.F.R. § 164.402.*

2. Questions to Consider in Determining Whether a Breach Occurred:

    a. Is the Data Protected Health Information? Protected Health Information is defined as individually identifiable health information that is transmitted by electronic media, maintained in electronic media; or transmitted or maintained in any other form or medium. If the information acquired, accessed, used or disclosed is not Protected Health Information, there is no breach. *45 C.F.R. § 160.103*.

    b. Is the Data Unsecured Protected Health Information? Protected Health Information that is rendered unusable, unreadable, or indecipherable to unauthorized parties through the use of technology or methodology is secured Protected Health Information" and not subject to the breach notification requirements. Incidents of disclosure of secured Protected Health Information need not be reported according to the requirements of this Policy, but should be documented by Equinox, Inc..

    c. Does the Incident Fall Under an Exception to a Breach? If the incident falls into one of the following exceptions, it is not considered a "breach":

        i. Unintentional access to Protected Health Information by an employee in good faith in the course of that employee performing their job, and such access does not result in further impermissible use.

ii. Inadvertent disclosure of Protected Health Information by a person authorized to access Protected Health Information to another employee authorized to access Protected Health Information at the same covered Entity or Business Associate, and the Protected Health Information is not further used or disclosed in a manner not permitted by the Privacy Rule.

iii. When Protected Health Information is improperly disclosed but Equinox, Inc. believes in good faith that the recipient will be unable to retain the information.

3. Risk Assessment Factors: When Equinox, Inc. knows, or believes that a breach may have occurred, the following information should be gathered to determine what notification is required:

a. The Nature and Extent of the Protected Health Information Involved: This includes the types of identifiers and likelihood of re-identification such as Social Security numbers, credit cards, financial data, clinical data, diagnosis, treatment, medications, behavioral health, or substance abuse.

b. The Unauthorized Person to Whom the Protected Health Information was Disclosed: Questions to consider are whether the person has any additional obligations to protect privacy, such as a business associate or another covered entity, or if the information is not immediately identifiable, if the unauthorized person has the ability to re-identify, or has the ability to re-identify the Protected Health Information with the affected patients.

c. Whether the Protected Health Information was Actually Acquired or Viewed: If the information was not actually acquired or viewed, no breach occurred.

d. The Extent to Which the Risk to Protected Health Information has been Mitigated: Was the person who received the Protected Health Information willing and able to limit its further use or disclosure? What level of effort has been expended to lessen the harm of this breach, or to prevent future related issues?

4. Discovery of a Breach: Discovery of breach of a patient's Protected Health Information occurs when either Equinox, Inc. knows, or should have known through exercising reasonable diligence that a breach has occurred. *45 C.F.R. § 164.404(a)(2).*

5. Notification Timeframe: Notification must be given to the appropriate party, based on the circumstances of the breach, within sixty (60) calendar days of the discovery of the breach. *45 C.F.R. § 164.404(b).*

6. Federal Notification Requirements: In the event of a breach of Protected Health Information, The Procedure Will Vary Based On The Nature And Volume Of The Breach:

a. All Protected Health Information Breaches: Each individual patient whose Protected Health Information was breached requires notification that complies with Section (e) of this Policy. *45 C.F.R. § 164.404(c).*

b. Breaches of More than 500 Patients:

i. Media Notification: In addition to the required notification to the individuals, Equinox, Inc. must notify "prominent" media outlets serving the jurisdiction of the breach. This provision only applies to Protected Health Information breaches of

more than 500 patients within the same jurisdictions. The prominence of the media outlet will depend on the jurisdiction of the breach, but at the minimum should include a general interest newspaper of daily circulation within the affected jurisdiction. *45 C.F.R. § 164.406(a).*

ii. Notification to the Secretary: In addition to the individual and media notifications, Equinox, Inc. must notify the Secretary of Health and Human Services (HHS) of a breach of more than 500 patients within 60 calendar days from the discovery of the breach. This notification must include the information in Section (e) of this Policy. The form for this required notification to the Secretary can be accessed via the HHS website at:https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true. *45 C.F.R. § 164.408(b)*.

c. Breaches of Less than 500 Patients:

i. Maintain a Log: If a breach of unsecured Protected Health Information affects fewer than 500 individuals, Equinox, Inc. must maintain a log that documents the extent and circumstances of the breach. This log should be maintained over the calendar year. *45 C.F.R. § 164.408(c).*

ii. Notification to the Secretary: Equinox, Inc. must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. Equinox, Inc. may report all of its breaches affecting fewer than 500 individuals on one date, but Equinox, Inc. must complete a separate notice for each breach incident. The form for this required notification to the Secretary can be accessed via the HHS website at:
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.
*45 C.F.R. § 164.408(c).*

d. Unknown Amount of Affected Patients: If the number of individuals affected by a breach is uncertain at the time of submission, Equinox, Inc. should provide an estimate, and, if it discovers additional information, submit updates as information becomes available. It is important to update any documentation to the appropriate parties (individuals, media, Secretary) as the information becomes available to Equinox, Inc..

e. Required Content of Notification: Each notification of the breach required under this Policy must include the following information:

i. A brief description of what happened in the breach, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of Protected Health Information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

v. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, website, or postal address. *45 C.F.R. § 164.404(c).*

f. Law Enforcement Delay: Notification pursuant to this Section can be delayed if a law enforcement officer states that notification would impede a criminal investigation or cause damage to national security. The law enforcement's statement to Equinox, Inc. can be made orally or in writing.

i. If Statement is in Writing: The written notice should specify the time for which a delay in notification is required. *45 C.F.R. § 164.412(a).*

ii. If Statement is Given Orally: Equinox, Inc. or business associate should document the statement, including the identity of the official making the statement, and limit the delay in the notification for no longer than 30 days. *45 C.F.R. § 164.412(b).*

g. Business Associates: All of the breach notification requirements and procedures referenced in this Policy Section apply to the Business Associates of Equinox, Inc. . *45 C.F.R. § 164.410.*

7. New York Breach Notification Requirements:

a. Notification Requirements: Any resident of New York State whose computerized Private Information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization must be notified of such breach of their Private Information ("Private Information Breach"). *N.Y. General Business § 899-aa(2).*

i. Notice to affected persons under New York Private Information Breach notification requirements is not required if the exposure of Private Information was an inadvertent disclosure by persons authorized to access Private Information, and Equinox, Inc. reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials. Such a determination must be documented in writing and maintained for at least five (5) years. If the incident affects over five- hundred (500) residents of New York, Equinox, Inc. shall provide the written determination to the State Attorney General within ten (10) days after the determination.

b. Private Information: Private Information shall mean a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or any unencrypted information concerning a natural person whose name, number, personal mark, or other identifier, in combination with any one of the following:

i. Social security number;

ii. Driver's license number or non-driver identification card number;

iii. Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;

iv. Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

v. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image. *N.Y. General Business § 899-aa(1)(a), 899-aa(1)(b).*

c. Notice Method: If a Private Information Breach occurs, any person or business which conducts business in New York State must notify the individual(s) either by written notice, electronic notice, telephone notification, or substitute notice if the business can demonstrate to the State Attorney General that the cost of providing notice would exceed two hundred fifty-thousand dollars ($250,000), or that the affected class of individuals to be notified exceeds five hundred thousand (500,000) individuals, or the business does not have sufficient contact information. *N.Y. General Business § 899-aa(5).*

d. State Agency Notification: If New York State residents are to be notified, the person or business shall notify the State Attorney General, the Department of State, and the Division of State Police as to the timing, content and distribution of the notices and approximate number of affected individuals. *N.Y. General Business § 899-aa(8)(a).*

e. Consumer Reporting Agency Notification: In the event that more than five thousand (5,000) New York residents are to be notified, the person or business shall also notify consumer reporting agencies in addition to the State Attorney General, the Department of State, and the Division of Police, as to the timing, content and distribution of the notices and approximate number of affected individuals. *N.Y. General Business § 899-aa(8)(b) .*

f. Attorney General Notification of HIPAA Breach: In the event that Equinox, Inc. is required to provide notification of a breach to the Secretary of Health and Human Services pursuant to Section 6 of this Policy, and such breach does not include Private Information as defined in Section 7(b) of this Policy, Equinox, Inc. shall provide notification of such breach to the State Attorney General within five (5) business days of notifying the Secretary. *N.Y. General Business § 899-aa(9).*

Attachment 1

## Breach Notification Assessment Tool

Affected individuals and the Office for Civil Rights ("OCR") must be notified of a breach of unsecure Protected Health Information unless it is established that there is a low probability that the Protected Health Information has been compromised.

The use of this tool is required to determine if a breach has occurred and notification is necessary. The specific facts and circumstances of a violation may require additional consideration and evaluation; however, this tool provides a consistent approach in performing a risk assessment and assists in the determination of whether the violation is a breach and requires notification.

### Section 1: Does an exception apply?

**Exceptions to the breach definition**: (check all boxes that apply)

- □ An unintentional acquisition, access or use of Protected Health Information by a Workforce Member if the acquisition, access or use was made in good faith and within the course of carrying out authorized duties if such information is not further acquired, used or disclosed.
- □ An inadvertent disclosure of Protected Health Information from one person authorized to access Protected Health Information to another similarly situated person at the same or related covered entity, business associate, or Organized Health Care Arrangement such, as a clinically integrated care setting, if such information is not further acquired, used or disclosed.
- □ A disclosure of Protected Health Information where there is good faith belief that an unauthorized person to whom the impermissible disclosure was made would not reasonably have been able to retain such information.

If any of the above boxes are checked, an exception to the breach definition applies and a breach has not occurred. If an exception does not apply, continue with the risk assessment.

An exception applies: _____ _____

Name and Title Date

### Section 2: Breach Risk Assessment

| Variables | Options | Scores | Results |
|---|---|---|---|
| **I. Method of Disclosure** | • Verbal – No documentation involved | 1 | |
| | • Paper<br>• Electronic | 2 | |
| **II. Unauthorized Recipient(s)**<br>(Who was the recipient of the Protected Health Information?) | • Business Associate<br>• Another covered entity<br>• Internal Workforce Member<br>• Health care regulatory agency | 1 | |
| | • Unauthorized family member of patient or resident<br>• Non-covered entity or individual that is bound by privacy, security or ethical laws or standards | 2 | |

| | | | |
|---|---|---|---|
| | • Media<br>• Unknown<br>• Entity or individual of the general public including another patient or resident, or family member of the other patient or resident<br>• Authorized or unauthorized individual where improper intent is known or suspected | 3 | |
| **III. Circumstances of Release**<br>(How was the information accessed or disclosed?) | • Unintentional disclosure or access of Protected Health Information | 1 | |
| | • Intentional access | 2 | |
| | • Intentional disclosure<br>• Using false pretense to obtain or disclose<br>• Hack, theft or loss<br>• Access or disclosure that is adverse to the patient such as snooping | 3 | |
| **IV. Disposition or Mitigation**<br>(What happened to the information after the initial disclosure?) | • Information returned complete without leaving the premises<br>• No documentation involved in the disclosure (verbal)<br>• Information is attested to be properly destroyed or deleted by recipient who is bound by privacy/confidentiality or ethical laws and standards | 1 | |
| | • Information returned complete after leaving the premises<br>• Information is attested to be properly destroyed or deleted by recipient who is NOT bound by privacy, security or ethical laws or standards | 2 | |
| | • Unable to retrieve<br>• Suspicion of re-disclosure<br>• Knowledge that Protected Health Information already re-disclosed<br>• Unknown disposition | 3 | |
| **V. Nature & Extent of Protected Health Information Involved** – Refer to *Identifiers listed below | • Identifier from any of the below Group Identifiers as a standalone piece of information<br>• Combination of four or fewer Group One Identifiers, not including Name | 1 | |
| | • Combination of Name with any other Group One or Group Two Identifiers<br>• Combination of any Group Two Identifiers | 2 | |
| | • Combination of Name with any other Group Three Identifiers<br>• Combination that includes any Group Two and Group Three Identifiers<br>• Any combination of 5 or more Identifiers | 3 | |

| ***Identifiers** | | |
|---|---|---|
| **Group One Identifiers** | **Group Two Identifiers** | **Group Three Identifiers** |
| • Name<br>• Date of Birth<br>• Parent's legal surname prior to marriage<br>• Electronic identification numbers<br>• Email address: contains no name | • Address<br>• Driver's License, State identification card or Passport numbers<br>• Personal Identification (PIN) Code<br>• Photograph: contains identifiers<br>• Email address: contains name | • Social Security Number<br>• Checking or Savings Account numbers<br>• Credit or Debit Card numbers |

| | | |
|---|---|---|
| • Medical Record Number, Account Number or Case Number<br>• Photograph: contains no identifiers<br>• Medical information: non-sensitive | | • Internet account numbers or Internet identification names<br>• Digital signatures<br>• Any other numbers or information that can be used to access a person's financial resources<br>• Passwords<br>• Medical Information: sensitive |

## Section 3: Breach Determination

Total breach risk score: _____

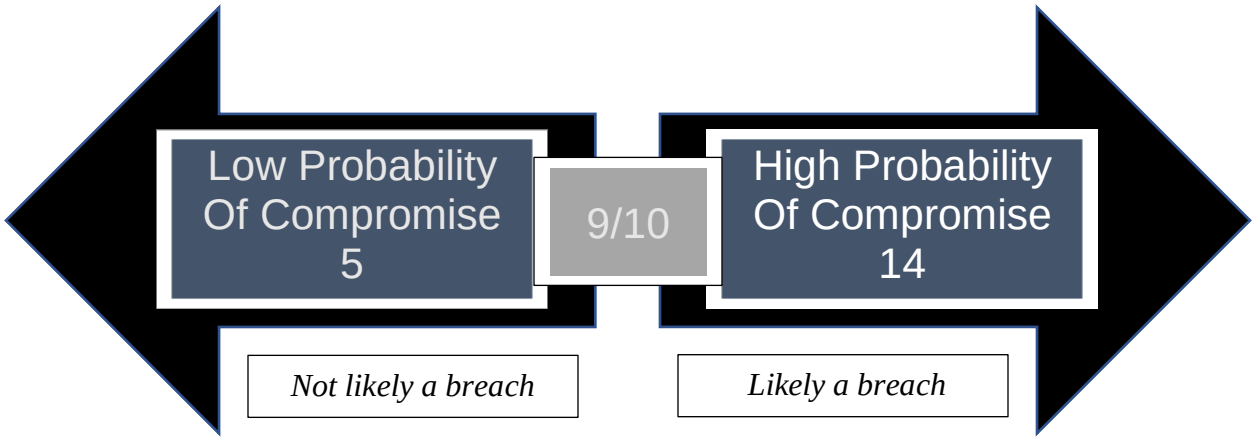
Is the HIPAA violation considered a breach? ☐ Yes ☐ No

If the breach determination is not consistent with the score, what are the special circumstances that caused the deviation?

_____
_____
_____
_____
_____
_____

Risk Assessment Completed by: _____ _____
*Name and Title* *Date*

# Total Risk Score




- A total breach risk score of 8 or less is not considered to be a breach. These disclosures should be appropriately logged, and no further action is required.
- A total breach risk score of 11 or greater is considered to be a breach and requires reporting.
- A total breach score of 9 or 10 requires careful consideration. Further review with legal counsel may be required.