Breach Policy

MolecularMatch implements a Breach Policy to provide guidance for breach notification when unauthorized access, acquisition, use and/or disclosure of ePHI occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities and business associates may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009 (pending publication HHS regulations).

In the case of a breach, all affected individuals will be notified.

Applicable Standards from the HITRUST Common Security Framework

- 11.a Reporting Information Security Events
- 11.c Responsibilities and Procedures

Applicable Standards from the HIPAA Security Rule

- Security Incident Procedures - 164.308(a)(6)(i)
- HITECH Notification in the Case of Breach - 13402(a) and 13402(b)
- HITECH Timeliness of Notification - 13402(d)(1)
- HITECH Content of Notification - 13402(f)(1)

Breach Response Process

1. **Discovery of Breach:** A breach of ePHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (including breaches by the organization's Customers, Partners, or subcontractors). We shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or Partner of the organization. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response) immediately, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Customer affected by the breach. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)
2. **Breach Investigation:** The Security and Privacy Officers shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years. Use this Breach Log.
3. **Risk Assessment:** For an acquisition, access, use, or disclosure of ePHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. A use or disclosure of ePHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of ePHI constitutes a breach and requires further notification, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. The organization shall document the risk assessment as part of the investigation in the Incident Report Form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications to appropriate Customers or that the use or disclosure did not constitute a breach (see Breach Checklist). Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

    - Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
    - The type and amount of ePHI involved;
    - The cause of the breach, and the entity responsible for the breach, either Customer, Organization, or Partner.
    - The potential for significant risk of financial, reputational, or other harm.
4. **Timeliness of Notification:** Upon discovery of a breach, notice shall be made to the affected Customer or individual no later than 4 hours after the discovery of the breach. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
5. **Delay of Notification Authorized for Law Enforcement Purposes:** If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:
    - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
    - If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.
6. **Content of the Notice:** The notice shall be written in plain language and must contain the following information:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - A description of the types of unsecured 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), if known;
    - Any steps the Customer or indvidual should take to protect their data from potential harm resulting from the breach.
    - A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
    - Contact procedures for individuals to ask questions or learn additional information, which may include a toll-free telephone number, an e-mail address, a web site, or postal address.
7. **Methods of Notification:** Customers and/or individuals will be notified via email and phone within the timeframe for reporting breaches, as outlined above.
8. **Maintenance of Breach Information/Log:** As described above and in addition to the reports created for each incident, we shall maintain a process to record or log all breaches of unsecured ePHI regardless of the number of records and Customers affected. The following information shall be collected/logged for each breach. Use this for

the Breach Log:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of records and Customers affected, if known.
- A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.), if known.
- A description of the action taken with regard to notification of patients regarding the breach.
- Resolution steps taken to mitigate the breach and prevent future occurrences.
- Attach an Incident Report Form.

9. **Workforce Training:** All workforce members shall be trained on the policies and procedures with respect to ePHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.
10. **Complaints:** Individuals must be provided access to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures.
11. **Sanctions:** Sanctions shall be made against members of the workforce, Customers, and Partners who fail to comply with privacy policies and procedures.
12. **Retaliation/Waiver:** There shall be no intimidatation, coercion, discriminatation, or other retaliatory actions against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Sample Letter to Customers in Case of Breach

[Date]

[Name here] [Address 1 Here] [Address 2 Here] [City, State Zip Code]

Dear [Name of Customer]:

I am writing to you from MolecularMatch, Inc. with important information about a recent breach that affects your account with us. We became aware of this breach on [Insert Date] which occurred on or about [Insert Date]. The breach occurred as follows:

Describe event and include the following information: A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known. B. A description of the types of unsecured 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), if known. C. Any steps the Customer should take to protect themselves from potential harm

resulting from the breach. D. A brief description of what Catalyze is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches. E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

Other Optional Considerations:

- Recommendations to assist customer in remedying the breach.

We will assist you in remedying the situation.

Sincerely,

Kevin Coker

CEO - MolecularMatch

kcoker@molecularmatch.com

303-351-2640