

**PRIVACY BREACH
PRIVACY OFFICER'S RESPONSE CHECKLIST**

This checklist provides guidance to the Privacy Officer in the case of a breach, or suspected breach, of electronic protected health information (ePHI). Additional information is contained in the Breach Notification Policy.

Action Step	Responsible Contact	Notes (Include Date Action Carried Out)
Description of Incident		
<i>Incident Received and Documented</i>	<i>Privacy Officer</i>	
▪ <i>Reported By (and contact information)</i>		
▪ <i>Date and Time Report Received</i>		
▪ <i>Date and Time of Incident</i>		
▪ <i>Date and Time Incident Discovered</i>		
▪ <i>Source of breach? If application, ID of application.</i>		
<i>Customer and/or Partner Involvement</i>	<i>Privacy Officer</i>	<i>Locate Signed BA Agreement; If No BA with Vendor, Document Why Not</i>
▪ <i>Description of Incident</i>		<i>Include Name of Individual(s) Involved, ePHI, Description of what, why, how incident happened</i>
<i>If Applicable, Security Incident Initiated</i>	<i>Security Officer</i>	
Internal Notification (as Appropriate)		
<i>IT Leadership</i>	<i>Chief Technology Officer or Chief Security Officer</i>	
<i>Risk Management, Compliance Officer, Human Resources, Leadership, etc.</i>	<i>Privacy Officer</i>	
<i>Legal Counsel</i>	<i>Privacy Officer</i>	
<i>Building Services/Facilities</i>	<i>Compliance Officer</i>	<i>Contact any other relevant parties (Rackspace, data center owners, etc)</i>
External Notification (as Appropriate)		
<i>External Legal Counsel</i>	<i>Listed below</i>	
<i>Law Enforcement Officials</i>	<i>To be Notified by Privacy Officer or Risk Management</i>	<i>Based on Geographic Location; Nature of Crime</i>
▪ <i>Date/Time</i>		
▪ <i>Agency</i>		
▪ <i>Officer</i>		
<i>Customers</i>	<i>To be Notified by Privacy Officer or Security Officer</i>	
▪ <i>Date/Time</i>		
▪ <i>Agency</i>		
▪ <i>Agent</i>		
<i>Office for Civil Rights</i>		
<i>State and/or Federal Agency, if Required</i>	<i>Privacy Officer</i>	

	Action Step	Responsible Contact	Notes (Include Date Action Carried Out)
	(e.g., Health Plans with Medicare Plans – Contact CMS)		
Investigation Components			
	Complete Risk Assessment to Determine Potential for Significant Risk of Financial, Reputational, or Other Harm (see Attachment A for PHI Data Elements)	Privacy Officer	See Breach Notification Policy
	Assess/Engage Need for Forensics	Chief Technology Officer or Chief Security Officer	Considerations: Does a Contract with a Vendor Exist? If Not, Approval of Senior Leadership?
	Assess/Engage Need for Private Investigator (e.g., research Craigslist, E-Bay, etc. for stolen equipment)	Privacy Officer or Risk Management	Considerations: Does a Contract with a Vendor Exist? If Not, Approval of Senior Leadership?
Mitigation/Follow-Up Activities			
	Report to Senior Leadership/BOD	Privacy Officer	
	Completion of Investigation Report	Privacy Officer	
	Completion of Workforce Member Sanctions	Privacy Officer	
	Communication to Staff – Learning Opportunity (e.g., newsletter article, meeting presentation, etc.)	Privacy Officer	
	Record Disclosure Information in Accounting of Disclosures Records.	Privacy Officer	
	Completed Checklist Retained with Supporting Documentation for six years	Privacy Officer	

HIPAA Defined PHI Data Elements

Note: Any single or combination of ePHI data elements used, accessed, or disclosed without an authorization is a breach. A risk assessment must be carried out to determine if there is potential harm to the individual and whether or not notification should be carried out (e.g., Identity Information Trifecta: Name, DOB, SSN#).

1	Name	10	Account Numbers
2	Geographic Subdivision Smaller than a State	11	Certification/License Numbers
3	All Elements of Dates Related to Individual (birth, death, adm)	12	Vehicle Identifiers and Serial Numbers Including License Plates
4	Telephone Numbers	13	Device Identifiers and Serial Numbers
5	Fax Numbers	14	Web URLs
6	Electronic Mail Address	15	Internet Protocol Addresses
7	Social Security Number	16	Biometric Identifiers, Including Finger and Voice Prints
8	Medical Record Numbers	17	Full Face Photos and Comparable Images
9	Health Plan Beneficiary Numbers	18	Any Unique Identifying Number, Characteristic or Code

Key Contacts/Information Sources

<i>Name</i>	<i>Title</i>	<i>Phone</i>	<i>E-Mail Address</i>
<i>Kevin Coker</i>	<i>Privacy Officer</i>	<i>501-319-4156</i>	<i>kcoker@molecularmatch.com</i>
<i>Nick Tackes</i>	<i>Chief Technology and Security Officer</i>	<i>949-573-5288</i>	<i>ntackes@molecularmatch.com</i>
	<i>Compliance Leader</i>		
	<i>Legal Counsel</i>		