Purpose

This document describes Kaiser Permanente Northwest (KPNW) Region’s policy and procedures for reporting any use, acquisition, access, or disclosure of Protected Health Information (PHI) in violation of the HIPAA Privacy Rule, and subject to the HIPAA Breach Notification Rule.

Scope

This policy and procedure applies to all research conducted by employees of KPNW or conducted within KPNW facilities.

If research involves non-KP data recipients (e.g., research collaborators, sponsors, business associate(s) (BA), including BA workforce, agents or subcontractors), the provisions of this policy should be included within the scope of the appropriate research agreement (e.g., BAA, DUA or other KP contracts).

Definitions

See Appendix A. Kaiser Foundation Research Institute (KFRI) maintains an updated list of Privacy Rule definitions on their website.

Policy

1. Any impermissible use and/or disclosure of PHI must be reported to the regional Privacy Officer immediately, but in no event later than five (5) calendar days of becoming aware of the event.

2. An impermissible use and/or disclosure of PHI is assumed to be a breach until a risk assessment as required by HIPAA has determined there is a low probability that the security or privacy of the PHI has been compromised.

3. A breach is considered to be discovered by a KP or other data recipient on the first day the impermissible use and/or disclosure is known, or by exercising reasonable diligence should have been known, to the KP or other data recipient. (45 CFR 164.404(a)(2)).

4. KPNW Compliance will, following the discovery of a breach of PHI that requires notification, ensure that appropriate individuals and entities are notified as outlined in KP National Policy Notification Regarding Breaches of Protected Health Information NATL.NCO.PS.025.
Procedures

1. Any impermissible use/disclosure of PHI in the custody of a PI, Sub-investigator, research staff, or other research data recipient must be reported to the Research Compliance Manager and, if applicable, the IRB by phone or email **immediately**, but no later than five (5) calendar days of becoming aware of the event.

2. The Research Compliance Manager or designee will promptly notify and consult with the Regional Privacy Officer to conduct the risk assessment to determine if the incident constitutes a breach as defined by HIPAA, and if any notification is required.

3. The risk assessment will be conducted and documented in accordance with applicable regional compliance policies and procedures.

4. If the incident involves secured PHI or falls within an exception to the definition of breach (45 CFR 164.402(1)(i)-(iii)), no further action is required. The IRB, PI, reporting individual, and others as appropriate will be notified of this determination.

5. If the incident involves unsecured PHI, but a risk assessment determines that there is a low probability that the PHI has been compromised, breach notification is not required. Research Compliance and Regional Compliance will maintain documentation sufficient to support the determination to meet KP’s regulatory requirements. The IRB, PI, reporting individual, and others as appropriate will be notified of this determination.

6. If a determination is made that a breach requires notification, the Research Compliance Manager will work with the Regional Privacy Officer to ensure that notifications will be issued according to 45 CFR 164.404 and KP National Policy: Notification Regarding Breaches of Protected Health Information, NATL.NCO.PS.025.

7. Breach information will be documented in the KP NCO reporting system.

8. Additional State Law Notification: State law may impose additional breach notification requirements. KP will provide notification as required by state law.

9. Notification to the IRB will include the same information as required for the Notification of Individuals and include all supporting documentation. The IRB
HIPAA Breach Reporting for Research

will evaluate the incident as potential serious and/or continuing noncompliance per SOP KP-006.

Document Approval, Ownership, and History

A template of this document was reviewed by the KP National Privacy working group, and it was reviewed and approved by the KP FWA Institutional Official on 10/21/2014. It has been adapted to fit KPNW organizational structure. This document will be reviewed every two years for accuracy, relevance, and completeness.

Document owner: Research Compliance Manager, KPNW
Document Approval Authority: Research Compliance Committee (RCC)
Approval Date: September 18, 2017

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reviewed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version: 1.0</td>
<td>11/06/2014</td>
<td>Center Operations Group</td>
</tr>
<tr>
<td>Version: 1.0</td>
<td>11/06/2014</td>
<td>Research Compliance Committee</td>
</tr>
<tr>
<td>Version: 2.0</td>
<td>08/22/2017</td>
<td>Harry Mayfield (COG/RCC)</td>
</tr>
<tr>
<td>Version: 2.0</td>
<td>09/15/2017</td>
<td>Research Compliance Committee</td>
</tr>
</tbody>
</table>
References

- Notifications Regarding Breaches of Protected Health Information.  
  NATL.NCO.PS.025
- Mitigation of Impermissible Uses and Disclosure of PHI.  
  NATL.NCO.PRIV.15
- American Recovery and Reinvestment Act/Health Information Technology for Economic and Clinical Health Act (HITECH) Title XIII Section 1302-Notification in the Case of Breach.
- SOP KP-006, IRB Review and Reporting of Unanticipated Problems, Noncompliance, and Suspensions or Terminations

Appendices

Appendix A: Privacy Rule Definitions
http://kpnet.kp.org/kfri/regulations/index.htm#six

As used in this subpart, the following terms have the following meanings:

Breach

Means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

1) Breach excludes:
   a) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
b) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

c) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

b) The unauthorized person who used the protected health information or to whom the disclosure was made;

c) Whether the protected health information was actually acquired or viewed; and

d) The extent to which the risk to the protected health information has been mitigated.

Unsecured Protected Health Information

Means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5