

UC Riverside, School of Medicine Policies and Procedures
Policy Title: HIPAA Breach Risk Assessment and Mitigation
Policy Number: 950-02-015

Responsible Officer:	Compliance and Privacy Officer
Responsible Office:	Compliance Office
Origination Date:	5/2013
Date of Revision:	11/2019
Scope:	UCR School of Medicine and UCR Health Practice Locations

I. Policy Summary:

When an improper use or disclosure of Protected Health Information (PHI) is suspected, a breach risk assessment will be completed and the impacts of the improper use and disclosure will be assessed in order to identify and mitigate potential harm to the patient.

II. Definitions: Refer to Standard Definition Guide

III. Policy Text:

A. Breach Risk Assessment

1. The Breach Risk Assessment determines the probability that PHI has been compromised. The Breach Risk Assessment will be based on four factors, in combination, and not in isolation:
 - a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
 - b. The unauthorized person who used the PHI or to whom the disclosure was made.
 - c. Whether the PHI was actually acquired or viewed.
 - d. The extent to which the risk to the PHI has been mitigated.
2. A HIPAA Breach Decision Tool and Risk Assessment Documentation Form (Attachment A) will be completed by the Compliance and Privacy Officer or designee as part of the risk assessment in order to determine whether the potential breach is a reportable breach.
3. A determination will be made if the affected individual(s) or the Department of Health and Human Services will be notified of the incident if the subsequent breach assessment concluded that there was a low probability that the PHI was compromised.
4. In the event that the improper disclosure is determined to have caused any known harmful effects, UCR will act to mitigate the harm to the affected individuals. These mitigation efforts may include but are not limited to the following actions:
 - a. Retrieving the improperly disclosed PHI from the unauthorized recipient.

- b. Having the unauthorized recipient delete the PHI from their computer or mobile device.
 - c. Engaging IT to examine the unauthorized person's device to determine if PHI has been accessed, copied, or transmitted.
 - d. Wiping data from a lost or stolen laptop or mobile device.
 - e. Installing or upgrading automated tools such as intrusion detection/prevention systems, firewalls, encryption, anti-virus and anti-malware tools.
 - f. Using data loss prevention solutions to track the movement and use of PHI within the UCR Health system.
 - g. If a breach is active or ongoing, taking action to prevent further data loss by securing and blocking unauthorized access.
 - h. Obtain a signed affidavit from an unauthorized recipient, indicating that the PHI will/has been returned or properly destroyed and has not been/will not be further used or disclosed.
 - i. Review policies and procedures for possible revision.
 - j. Provide staff with in-service training and education.
5. If it is determined that the incident is "significant" or "high visibility" the Incident Response Team (IRT) will be convened. Examples of such incidents include but are not limited to:
- a. Incidents involving high profile individuals, such as celebrities or "VIPs."
 - b. Incidents involving key UC personnel such as UCR leadership, system leadership Regents, prominent faculty or alumnae, etc.
 - c. Incidents for which a press release may or will be issued, or media coverage is anticipated.
 - d. Incidents involving 10 or more affected individuals.
 - e. Incidents likely to result in litigation or regulatory investigation.
 - f. Incidents involving criminal activity.
 - g. Any other incident that is likely to involve reputational, regulatory and/or financial risk to UCR of which senior management should be aware.

B. Incident Response Team (IRT)

1. The IRT will consist of the following staff:
 - Health Sciences Compliance and Privacy Officer
 - Information Security Officer
 - Risk Management
 - Department leadership of affected area
 - Legal Counsel
 - Others as appointed by the Compliance and Privacy Officer and as appropriate to the breach.
2. IRT will be responsible for:
 - a. Developing the incident report and response plan.
 - b. Reporting to UCOP, as necessary.
 - c. Implementing a containment strategy.
 - d. Reporting of findings.
 - e. Remediation and post-incident review.

Refer to University of California *Privacy and Data Security Incident Response Plan* for further directions.

C. Breach Notification Requirements

1. Individual Notice

UCR Health must notify affected individuals following the discovery of a breach of unsecured PHI. This individual notice must be in written form by first-class mail or, alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If there is insufficient or out-of-date contact information for 10 or more individuals, UCR Health will provide substitute individual notice by posting the notice on the www.ucrhealth.org public-facing website for at least 90 days. Notification will include reference to a UCR Compliance toll free hot-line that individuals can call for further information. If the insufficient or out-of-date contact information is for fewer than 10 individuals, substitute notice will be provided by an alternative form of written notice, by telephone, or other means. This notification will be provided within 60 days of the breach discovery.

2. Media Notice

If UCR Health experiences a breach affecting more than 500 California residents, in addition to notifying the affected individuals, UCR Health will provide notice to prominent media outlets serving the area in the form of a press release. This media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and will include the same information required for the individual notice.

3. Notice to the HHS Office of Civil Rights (OCR)

The OCR will be notified of breaches of unsecured PHI. UCR Health will notify the Secretary by visiting the HHS web site and [filling out and electronically submitting a breach report form](#). If a breach affects 500 or more individuals, UCR Health will notify the OCR without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, UCR Health may notify the OCR of such breaches on an annual basis or at the time of discovery. Reports of breaches affecting fewer than 500 individuals will be submitted to the OCR no later than 60 days after the end of the calendar year in which the breaches are discovered.

4. Notice to California Department of Public Health (CDPH)

UCR Health will notify the CDPH and affected patient or patient's representative as may be applicable, of any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information not later than 15 days after the unlawful or unauthorized access, use, or disclosure has been detected.

5. Notification by a Business Associate

If a breach of unsecured PHI occurs at or by a UCR Health business associate, the business associate will follow reporting guidelines as outlined in the Business Associate Agreement.

IV. **Responsibilities:** Not Applicable

V. **Procedures:**

- A. All staff and faculty will immediately report a breach of patient information or a potential breach of information to the Compliance and Privacy Officer.
- B. The Compliance and Privacy Officer and Security Officer (as applicable) will perform a risk assessment of the incident to determine the impact on the privacy of the patient and identify appropriate action plan. These steps will include:
 - 1. Investigation into the circumstances of the breach, including consultation with legal counsel as appropriate to the situation.
 - 2. Identifying the scope of the breach, assuring that the breach is contained and taking measures to prevent subsequent disclosures.
 - 3. Determining other actions necessary to mitigate the effects of the breach.
 - 4. Ensuring that appropriate personnel actions are taken, including discipline of any employees, volunteers, or members of UCR Health staff and faculty who were responsible for the breach.
 - 5. Reviewing administrative standards (training, policies and procedures, etc.) and action as necessary to prevent future breaches (policy revision, personnel retraining).
- C. The Compliance and Privacy Officer will make applicable notifications to the patient(s) and to state and federal regulatory agencies.
- D. All documentation of the risk assessment and subsequent incident mitigation will be kept for 6 years from the date of the incident. This record will also include, but not be limited to, information describing disciplinary actions, corrective actions, policy and procedure revision, training records, and notifications.

VI. **Forms/Instructions:**

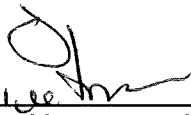
- Attachment A: HIPAA Breach Decision Tool and Risk Assessment Documentation Form
- Attachment B: Questionnaire and Confidentiality Agreement (Paper or Verbal PHI)
- Attachment C: Questionnaire and Confidentiality Agreement (Electronic PHI)

VII. Related Information:

University of California *Privacy and Data Security Incident Response Plan*
UCR SOM Sanctions Policy and Procedure 950-02-012

VIII. Revision History: 3/2016, 11/2019

Approval(s):



PAUL HACKMAN, J.D., L.L.M.
CHIEF COMPLIANCE AND PRIVACY OFFICER,
SCHOOL OF MEDICINE

2-10-2020

DATE



DEBORAH DEAS, M.D., M.P.H
VICE CHANCELLOR, HEALTH SCIENCES
DEAN, SCHOOL OF MEDICINE

2-10-2020

DATE

Attachment A

ATTORNEY CLIENT COMMUNICATION

HIPAA BREACH DECISION TOOL AND RISK ASSESSMENT DOCUMENTATION FORM

Name of person completing form: _____

Date incident occurred: _____ Date incident detected: _____

Brief summary of incident, including number of patients affected: _____

1. Was protected health information (PHI) involved? (PHI is health information (including demographic information) that identifies, or there is a reasonable basis to believe it can be used to identify, the individual. Health information includes any information relating to the physical or mental health or condition of an individual, the health care provided to an individual, or payment for health care provided to an individual. PHI does not include employment records held by a covered entity in its role as employer or PHI regarding a person who has been deceased for more than 50 years.)

- Yes, PHI was involved. Continue to Question 2.
No, PHI was not involved. No breach reporting required under HIPAA.

Describe the information involved:

2. Was the PHI unsecured? ("Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance, such as encryption or destruction. The guidance can be found on the DHHS website at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.)

- Yes, the PHI was unsecured. Continue to Question 3.
No, the PHI was secured. No breach reporting required under HIPAA.

Describe the PHI (for example, was it verbal, paper or electronic? Encrypted in compliance with NIST, password protected, other?):

3. Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule? (Providers should keep in mind that a violation of the "minimum necessary" standard

is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. Providers may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule.)

Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. *Continue to Question 4.*

No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

Describe who acquired, accessed, used and/or disclosed the PHI, whether the person(s) was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed: _____

4. **Does an exception apply?** Check any box below that applies:

Exception A. A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

(i) Was made in good faith; and

(ii) Was within the course and scope of authority; and

(iii) Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce" includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether or not they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

Exception B. A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

Exception C. A breach does not include disclosure of PHI where the provider or business associate has a good faith belief that the unauthorized person who received it would not reasonably have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.)

Yes, an exception applies. No breach reporting required under HIPAA.

No, an exception does not apply. *Continue to Question 5.*

5. **Risk assessment.** An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates

that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL of the factors listed below.)

Factor A. Consider the nature and extent of the PHI involved, including the types of identifiers (and the likelihood of re-identification if the PHI is de-identified). *(Consider whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, STD, cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interests. Covered entities should also determine whether there is a likelihood that the PHI could be re-identified (if the PHI is de-identified) based on the context and the ability to link the information with other available information.)*

Describe the PHI involved, including identifiers and likelihood of re-identification (if the PHI is de-identified):

Consider whether PHI could be used in a manner adverse to the patient(s) or to further the unauthorized person's interests: _____

Factor B. Consider the unauthorized person who used or received the PHI. *(This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information - for example, is the person a covered entity required to comply with HIPAA, or a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.)*

Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified):

Factor C. Consider whether the PHI was actually acquired or viewed. *(If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.)*

Describe whether the PHI was actually acquired or viewed (attach report from a computer forensic analyst, if one was obtained): _____

Factor D. Consider the extent to which the risk to the PHI has been mitigated — for example, as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed

(through a confidentiality agreement or similar means) has been completely returned, or has been/will be destroyed. *(Covered entities should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised. OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results in terms of the risk to PHI. For example, a covered entity may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)*

Describe risk mitigation steps taken: _____

Factor E. Describe any other relevant factors (write "none" if appropriate):

Based on the factors noted above, is there a low probability that the PHI has been compromised?

- Yes (there is a low probability), thus **No** breach reporting required under HIPAA.
- No (there is not a low probability; there is a higher probability) thus breach reporting is required under HIPAA.

Signature of person completing this form: _____

Title: _____ Date: _____

QUESTIONNAIRE AND CONFIDENTIALITY AGREEMENT *(Paper or Verbal PHI)*

UCR Health takes our responsibility to protect our patients' privacy very seriously. We are currently researching a disclosure of protected health information (PHI) that may potentially be considered a privacy breach. We greatly appreciate your help in answering three quick questions.

Date: _____

It is our understanding that you may have erroneously received some PHI. Please check the appropriate boxes:

1. I have shared or disclosed the PHI to the following persons:

-OR-

I have not shared or disclosed the PHI to anyone (either in writing or verbally).

2. I used the PHI as follows:

-OR-

I have not used the PHI in any way.

3. If paper PHI was involved, please check the appropriate box:

I returned all of the PHI to a representative of

Covered Entity.

-OR-

I destroyed or disposed of all of the PHI by:

- Shredding it myself
- Putting it in a locked bin to be shredded later
- Putting it in an unlocked bin to be shredded later
- Putting it in a locked bin to be recycled
- Putting it in an unlocked bin to be recycled
- Putting it in the "regular" trash
- Other. Please describe:

-OR-

- I am keeping all or some of the PHI, or a copy of the PHI.

I hereby affirm that the answers I have given to the questions above are correct. I also agree not to further use or disclose any PHI that I may have erroneously received.

Print name: _____ Date: _____

Signature: _____ Company: _____

Address: _____

Phone number: _____

NOTE: The covered entity must carefully review the answers provided by the unauthorized person on the questionnaire. If the unauthorized person has used or disclosed the PHI, put it in an unsecured location, etc., then additional follow-up by the covered entity should be undertaken.

QUESTIONNAIRE AND CONFIDENTIALITY AGREEMENT *(Electronic PHI)*

UCR Health takes our responsibility to protect our patients' privacy very seriously. We are currently researching a disclosure of protected health information (PHI) that may potentially be considered a privacy breach. We greatly appreciate your help in answering a few quick questions.

Date: _____

It is our understanding that you may have erroneously received some PHI. Please check the appropriate boxes:

1. I have read the PHI

-OR-

I have not read the PHI.

2. I have copied the PHI

-OR-

I have not copied the PHI.

3. I have shared, disclosed or forwarded the PHI to the following persons: _____

-OR-

I have not shared, disclosed or forwarded the PHI to anyone (either electronically, in writing or verbally).

4. I used the PHI as follows: _____

-OR-

I have not used the PHI in any way.

5. I returned the CD, DVD, hard drive, flash drive, tape, or other electronic media to a representative of _____ Covered entity.

-OR-

I deleted all of the PHI by: _____

Other. Please describe: _____

6. Describe your back-up system (for example, cloud, tape, virtual, near-line, disk, etc.): _____

7. The method I used to delete the PHI from my back-up was: _____

I hereby affirm that the answers I have given to the questions above are correct. I also agree not to further use or disclose any PHI that I may have erroneously received.

Print name: _____ Date: _____

Signature: _____ Company: _____

Address: _____

Phone number: _____

NOTE: The covered entity must carefully review the answers provided by the unauthorized person on the questionnaire. If the unauthorized person has used or disclosed the PHI, put it in an unsecured location, etc., then additional follow-up by the covered entity should be undertaken.