

<b>UC Riverside, School of Medicine Policies and Procedures</b> <b>Policy Title: Privacy and Security Breach Response and Incident Notification Plan</b> <b>Policy Number: 950-02-225</b>
---

<b>Responsible Officer:</b>	Chief Compliance & Privacy Officer
<b>Responsible Office:</b>	University of California, Riverside School of Medicine
<b>Origination Date:</b>	(2/28/2019)
<b>Date of Revision:</b>	(2/28/2019)
<b>Scope:</b>	UCR School of Medicine and UCR Health Faculty Practice locations

**I. Policy Summary**

California state law requires notification of the affected individual of breaches of personally identifiable information including medical information. California law also requires mandatory reporting to the California Department of Public Health (CDPH) in the event of a breach of health information in certain facilities licensed by the State. Breaches of Protected Health Information (PHI) from covered entities (both hospital and non-hospital-based providers) must also be reported to the affected individuals, along with the Department of Health and Human Services, along with public reporting in certain circumstances.

California law requires any state agency (including the University of California) with computerized data containing Personal Information to disclose any breach of security of a system containing such data to any California resident whose unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person. (The acquisition of personal information by a University employee or agent for *bona fide* University business purposes does not constitute a Security Breach, provided that the Personal Information is not further disclosed to an unauthorized person).

In the event of a Security Breach, all University campuses must follow the system wide procedures for providing notification of the breach to those state residents whose personal information is reasonably believed to have been acquired by an unauthorized person. The procedures for reporting a security Breach at UC Riverside is set forth in UC Riverside Administrative Policies and Procedures Section 806-17: *UCR Implementation Guidelines for Notifications in Instances of Security Breaches Involving Personal Information Data*.

Federal Law requires the notification of breaches of unsecured PHI to the affected individual and to the Department of Health and Human Services. Some examples of possible breaches include, but are not limited to:

- A) Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource.
- B) Transmission or disclosure of Personally identifiable information to an unknown party;
- C) Transmission or disclosure of PHI or ePHI to an unknown outside party

## II. Definitions

*Personally Identifiable Information (PII):* As used in this policy is the combination of an individual's first name or first initial and last name, combined with their (2) driver's license number or California identification card number, or 3) Social Security Number, or 4) Account Number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

*Electronic Protected Health Information or e-PHI:* is any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual, and identifies the individual. This includes e-PHI that is created, received, maintained or transmitted. For example, e-PHI may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

*Individually identifiable:* means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as patient's name, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity

*Medical Information (California Civil Code 56.05):* means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.

*Protected Health Information (PHI):* is any individually-identifiable health information collected or created as a consequence of the provision of health care by a covered entity in any form (including verbal communications and information transmitted, received or used electronically).

*Security Breach:* refers to the situation in which unencrypted Personal Information is reasonably believed to have been acquired by an unauthorized person.

*Security Incident:* is the attempted or successful unauthorized access to, use, disclosure, modification, or destruction of information or interference with system operations in an information system (45 C.F.R. section 164.304). A security incident may involve any or all of the following:

- A violation of computer security policies and standards

- Unauthorized computer access
- Loss of information confidentiality
- Loss of information availability
- Compromise of information integrity
- Denial of service condition against data, network or computer
- Misuse of service, systems or information, or
- Physical or logical damage to systems.

*Possibly Compromised System:* refers to systems whose automatic detection methods (network, intrusion detection, anti-virus or anti-spyware, vulnerability scanners, etc) have flagged as potentially having security problems. False positives or conditions which are not serious are frequently reported. therefore a report is not a sure indicator of a security breach or indicator.

*Unsecured PHI:* "Protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standard developing organization that is accredited by the American National Standards Institute." (*DHHS Definition*)

### III. Policy Text

**A. All suspected breaches of patient information must be reported by all workforce members via the incident reporting system or directly to the Chief Compliance & Privacy or Information Security Officer immediately upon discovery or upon suspicion that an incident or breach has occurred. Examples of privacy incidents include but are not limited to: the distribution of an email or fax to the wrong recipient, unauthorized access to patient information, or the unauthorized disclosure of patient information, discovery that electronic media such as a laptop, CD, PDA, computer hard drive, or other similar equipment is stolen or missing and contains unencrypted personally identifiable information. Security incident examples include the presence of a malicious application, such as a virus; establishment of an unauthorized account for a computer or application; unauthorized network activity; or presence of an unexpected/unusual programs.**

1. In the event of a significant or high visibility breach, the Chief Compliance & Privacy Officer will notify the Dean of UCR School of Medicine, who will immediately inform the Chancellor and the Cyber Risk Responsible Executive (CRE). The CRE will make a determination to appoint an Incident Response Team (IRT) Coordinator. The Incident Response Team will include the IRT Coordinator, Health Sciences Chief Compliance & Privacy Officer, Information Security Officer, Legal Counsel, Risk Management, Department Leadership of the affected Department, and any other personnel appointed by the IRT Coordinator. In the event of a

smaller breach, the Chief Compliance & Privacy Officer and/or Information Security Officer will coordinate a UCR Health IRT as applicable to the size of the breach.

2. The Chief Compliance & Privacy Officer will immediately notify the UC HIPAA Privacy Official of all significant incidents, and prior to notification of any major media outlets or state or federal agencies, to allow sufficient time for UCOP internal consultation, without jeopardizing any regulatory obligations.
  - 1) The Incident report will be reviewed by the Chief Compliance & Privacy Officer, Legal Counsel, and Risk Management. A determination will be made as to which, if any of the notification requirements have been triggered under both state and federal law. The applicable notices will be made to the effected individuals and to the applicable state and federal authorities, and through media outlets, as required under federal law.

#### **IV. Responsibilities**

The UCR School of Medicine Compliance Office is responsible for maintaining and updating this policy and any related procedures. The Information Security Officer will be responsible for investigating any potentially compromised system to determine if there is an electronic breach.

#### **V. Procedures**

- A. If a UCR Health Workforce member suspects a breach may have occurred, the workforce member should first contact the Chief Compliance & Privacy Officer or Information Security Officer or notify their supervisor for assistance.**
- B. If a UCR Health Workforce member discovers that there has been a breach of unsecured personally identifiable information (as defined above), they must immediately report the breach directly to the Chief Compliance & Privacy Officer and Information Security Officer.**
  1. The Chief Compliance & Privacy Officer will, using the *HIPAA Breach Risk Assessment and Mitigation Policy*, determine if there is a HIPAA breach. The Chief Compliance & Privacy Officer and Information Security Officer will consult with Legal Counsel and Risk Management to determine the required reporting and breach notifications that need to be made. The Notice to the patient will be written in plain language and will include:
    - a) A description of what happened.
    - b) When the breach occurred and when it was detected.
    - c) How it was detected.
    - d) What data was compromised or potentially compromised.
    - e) Why they are being notified.
    - f) What steps are being taken to address the breach.

- g) Whether any data is known to be fraudulently used or whether notification is precautionary.
  - h) If the data breached included a Social Security Number, driver's license, or California identification card, the toll-free numbers and address of major credit reporting agencies.
2. If a significant breach as defined under UC Policy, the Chancellor's designee will be notified and an Incident Response Team (IRT)
  3. If the breach involves more than 500 individuals, the Dean of the School of Medicine will be notified immediately, who will inform the CRE. The Chair of the Department and the Administrative Director of the Department will also be notified. The UC Riverside Assistant Vice Chancellor Information Technology (Chief Information Officer), and the campus Chief Information Security Officer will be notified in the event of an electronic breach.
  4. The UC System Compliance Officer will be notified of all breaches and will be notified immediately of any significant breaches, and any involving notification to media outlets and those requiring immediate notification to state or federal agencies.
  5. The Chief Compliance & Privacy Officer and Information Security Officer will work with the impacted departments to notify the affected individuals.
  6. The Compliance Office will make the required notifications to the CDPH for breaches involving medical information in licensed components of UCR Health.
  7. The Compliance Office will make the required notification to the Department of Health and Human Services, the State Attorney General's office or include the notification on the annual breach notification as applicable.
  8. Media Relations will be consulted to make the appropriate notifications to media outlets if needed.
  9. The analysis of the reporting notification requirements will be documented by the Chief Compliance & Privacy Officer and Information Security Officer in writing and maintained in the Compliance Office Incident reporting database.
  10. The decision to offer credit monitoring services to individuals who are notified that their personal information was involved in a security breach will be made by the Chief Compliance & Privacy Officer and Legal Counsel. The criteria to be used in the decision includes whether the breach involved personally identifiable information that could be used to commit credit fraud or identity theft.
  11. Any staff member(s) who may have been involved with causing a potential breach shall be recused from the investigation and a suitable substitute will be used to assist with the investigation to ensure objectivity.

**VI. Forms/Instructions**

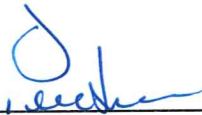
N/A

**VII. Related Information**

- References: 45CFR Parts 164.404 UC Riverside Administrative Policy 800-17 UCR Guidelines for Notification in Instances of Security Breaches Involving Personal Information
- Data Health and Safety Code 1280.15
- California Civil Code 1798.29 and 1798.82 (California Information Practices Act of 1977)
- UCR School of Medicine 950-02-015 HIPAA Breach Risk Assessment and Mitigation Policy
- University of California Guidelines: Privacy and Data Security Incident Response Plan (December 17, 2010)
- University of California BFB-IS-3: Electronic Information Security Policy (<https://policy.ucop.edu/doc/7000543/BFB-IS-3>)
- University of California UC Information Security Incident Response Standard (<https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf>)

**VIII. Revision History**

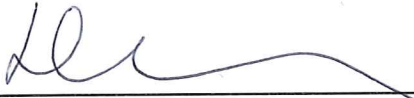
Approval(s):



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

8-12-19

DATE



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

8-12-19

DATE