University of California

Privacy and Data Security Incident Response Plan

TABLE OF CONTENTS

Section 1: Governance 4
Overview 4
When to use this document 4
Lead campus authority 4
Characteristics of "significant" or "high-visibility" incidents 4
Workforce Responsibilities 5
Incident Response Team (IRT) 5
Responsibilities for Incident Response 5
Reporting Responsibilities to UCOP 6
Section 2: Triage and Scoping 7
Overview 7
What is a security incident? 7
Incident reporting 7
Report description template 8
Initial incident reports 8
Initial incident documentation 8
UC Privacy / Security Incident Report Form 9
Incident classification 9
Containment strategy 10
Preservation of evidence 11
Incident Documentation 11
Identify and engage relevant expertise 11
Communication/disclosure strategy 12
References 12
Section 3: Execution 13
Preparation 13
Containment 13

Analysis: Data & Systems 13
Assess the cause and type of breach 13
Forensic analysis 14
Assessment of Incidents 14
Assessment of Incidents involving HIPAA PHI 14
Reporting Findings 15
Notification Process 15
Timing of Notifications 16
References 16
Section 4: Remediation and Post-Incident Review 18
Responsibilities 18
Technical Actions 18
Policy and Organization 19
Recommendations and Next Steps 20
Exhibits 22
Exhibit A: Forensic Evidence Methodology 22
Detection 22
Preservation of Evidence 22
Collecting Evidence 23
Handling of Evidence 23
Forensic Documentation 23
Exhibit B: Incident Response Check List 24
Exhibit C: Components of a Notification Letter 29
Version History 31

SECTION 1: GOVERNANCE

OVERVIEW

This document and governance structure provides the oversight of and guidance for the required processes for the University of California's (UC's) privacy and data security breach response in compliance with federal and state privacy laws.

WHEN TO USE THIS DOCUMENT

This plan is intended to be scalable. Its use is not necessary for every privacy and data security incident, as many incidents are small and routine, requiring only a single responder. It is left to the judgment of the lead campus authority (defined below), or their designee, to determine when to convene an Incident Response Team (IRT), however, it will generally be necessary for all "significant" or "high-visibility" incidents (described below). If an IRT is convened, this plan document must be consulted, and the elements appropriate to the individual incident must be used.

LEAD CAMPUS AUTHORITY

At each UC campus, the Chancellor is required[1] to designate either an individual or a functional position to be responsible for the oversight of the investigation of and the determination of notification for breaches of personally-identifiable information. The functional position of this "lead campus authority" is required to be at a level high enough to allow that individual to speak with authority for the campus.

The lead campus authority, or their designee, will determine whether to convene an Incident Response Team (IRT), and will appoint the IRT Coordinator.

CHARACTERISTICS OF "SIGNIFICANT" OR "HIGH-VISIBILITY" INCIDENTS

An IRT will almost always be convened for all "significant" or "high-visibility" incidents. This is an inherently subjective criterion, so individual judgment is required. However, for the purposes of guidance, some examples of such incidents include, but are not limited to:

- Incidents involving celebrities or "VIPs" (such as those defined by the medical centers)
- Incidents involving key UC personnel such as campus leadership, system leadership, Regents, prominent faculty or alumnae/i, etc.
- Incidents for which a press release may or will be issued, or media coverage is anticipated
- Incidents involving 10 or more affected individuals (incidents involving fewer individuals may still be "significant" or "high-visibility," e.g., celebrities)
- Incidents likely to result in litigation or regulatory investigation
- Incidents involving criminal activity
- Any other incident that is likely to involve reputational, regulatory, and/or financial risk to UC of which senior management should be aware

[1] See UC Business and Finance Bulletin IS-3: *Electronic Information Security*, section III.D.5.a

WORKFORCE RESPONSIBILITIES

Every workforce member at UC has the responsibility to immediately report suspected or known breaches of the privacy or security of restricted information[2] to the designated department or individual for their work area. This may be a local support person, an IT Help Desk, departmental management, or similar function, as defined by the campus, laboratory, or medical center. Criminal acts, such as thefts, or suspected criminal acts, should also be reported to campus police.

INCIDENT RESPONSE TEAM (IRT)

The following are the minimum required individuals or functional areas for the IRT for every breach for which the IRT is convened (smaller breaches will likely be handled by the Privacy Officer, or Information Security Officer, or their staff):

- IRT Coordinator
- Privacy Officer (may also serve as IRT Coordinator)
- Information Security Officer (for electronic breaches; may also serve as IRT Coordinator)
- Legal Counsel
- Risk Management (or Risk Services)
- Department Leadership of affected department (Dean, Chair, etc.) or their designee

The following functions, and any others not listed, may be added to the IRT, as appropriate to the incident:

- Information technology/records management
- Public Information Officer/ Public Affairs
- Government Relations/Legislative Liaison
- Regulatory Affairs
- Campus Ethics and Compliance Officer
- Human Resources/Academic Personnel
- UCPD and other law enforcement, including FBI, as appropriate
- Other executives, as appropriate
- Records Management
- Internal Audit

RESPONSIBILITIES FOR INCIDENT RESPONSE

a. Upon initial determination of a possible breach, departmental management shall notify the Chancellor's designee immediately, who will serve as or appoint the IRT Coordinator.

b. The IRT Coordinator is responsible for the execution of all the Sections of this plan that are applicable to the specific incident, and may deviate from this plan, after consultation with the IRT, to the extent necessary to respond to the incident.

[2] See UC Business and Finance Bulletin IS-2: *Inventory, Classification, and Release of University Electronic Information*, section III.A.1.c

c. As one of their first actions, the IRT Coordinator shall consult with legal counsel to identify possible conflicts of interest in the investigation. In particular, individuals or teams may not lead investigations within their own areas of responsibility. Counsel should also be consulted regarding possible law enforcement involvement, and/or the need for forensic investigation.

d. As one of their first actions, the IRT Coordinator shall consult with Risk Management/Services to determine whether UC Business and Finance Bulletin BUS-80, *Insurance Programs for Information Technology Systems*, might provide insurance coverage for the incident.

e. The IRT shall ensure that resources are assigned to conduct the investigation, as applicable to the incident. In the event of possible conflicts of interest, those resources must be sufficiently independent to avoid the appearance of a conflict of interest. For electronic breaches, in the event of a possible conflict of interest, the assigned IT resources must be external to the affected department.

f. For electronic incidents, the designated IT resources shall conduct the initial forensic investigation, and liaise continuously with the IRT.

g. The IRT is responsible for the decision to notify affected individuals and/or regulatory agencies based on data elements that are individually identifiable, and current laws or regulations requiring notification. UC and campus policy regarding breach notification must also be considered, as well as the risk of harm to the individuals impacted by the breach. In some cases, even though notification may not be required by law, it may be prudent to notify affected individuals.

h. The IRT is responsible to ensure that, if necessary, evidence is preserved, and each incident is adequately documented. "Adequate" documentation will stand on its own, without requiring further explanation. The rationale to notify or not to notify must be clearly documented. (Further information on Incident Documentation is in Section 2, below.)

REPORTING RESPONSIBILITIES TO UCOP

The IRT Coordinator must contact the UC Systemwide Information Security & Privacy Officer as soon as it appears that a "significant" or potentially "high-visibility" incident has occurred, or as soon as an IRT is convened, whichever occurs first. The UC Systemwide Information Security & Privacy Officer is responsible for notifying appropriate UCOP personnel.

The Chancellor's designee[3] is responsible for reporting[4] electronic incidents to UCOP.

Incidents must be reported to UCOP using the online UC privacy/security incident report form. Reports using the incident report form must include as much information as known at the time of the report. The IRT Coordinator or Chancellor's designee is responsible for updating the form as additional information becomes available.

[3] See UC Business and Finance Bulletin IS-3: *Electronic Information Security*, section III.D.5.a

[4] See UC Business and Finance Bulletin IS-3: *Electronic Information Security*, section III.D.5.d

SECTION 2: TRIAGE AND SCOPING

OVERVIEW

The triage and scoping phase involves the process of analyzing the information about the situation to determine whether or not a security incident has occurred. [5] This Section includes guidance for incident identification, initial reporting, priority-setting based on data and system criticality and sensitivity, required collection and analysis of incident information, information preservation, documentation, and communication.

WHAT IS A SECURITY INCIDENT?

A security incident may involve any or all of the following:

- a violation of campus computer security policies and standards,
- unauthorized computer access,
- loss of information confidentiality,
- loss of information availability,
- compromise of information integrity,
- a denial of service condition against data, network or computer,
- misuse of service, systems or information, or
- physical or logical damage to systems.

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; presence of unexpected/unusual programs; or computer theft.

INCIDENT REPORTING

All suspected or confirmed privacy or data security incidents must be reported in accordance with campus, medical center, or systemwide policy[6]. Workforce members that identify a potential incident will initially classify the incident severity based on their perception. The initial severity level may be escalated or de-escalated by the Information Technology staff for an electronic incident. All incident reports are to be made as soon as possible after the incident is identified, and with minimum delay for medium to high severity incidents.

[5] CMS *Information Security Incident Handling and Breach Analysis Notification Procedure* (Version 2.1, Oct. 28, 2008)

[6] Reporting requirements to UCOP are described in Section 1, above.

REPORT DESCRIPTION TEMPLATE

INITIAL INCIDENT REPORTS

Workforce member incident reports must include the following incident descriptors when describing the incident to their designated reporting point:

- date and time of incident discovery,
- general description of the incident,
- systems and/or data at possible risk,
- actions they have taken since incident discovery,
- their contact information,
- any additional relevant information known at the time.

INITIAL INCIDENT DOCUMENTATION

Most incidents will not be directly reported to the IRT Coordinator, but most likely will be processed through local IT support structure or business unit management. If an IRT is convened for an incident, the information identified in Figure 2, or as much of the information as is available, must be collected, documented, and shared with the IRT.

Figure 2
Incident Reporting Elements

Information to Record	**Description**
References	Use the assigned Help Desk Case Number, or similar, if available
Suggested Severity Level	Low, Medium, High
Type of Incident	Note all types that apply, including but not limited to 1. Compromised System 2. Compromised User Credentials 3. Network Attacks (DOS, Scanning, Sniffing) 4. Malware (Viruses, Worms, Trojans) 5. Lost Equipment/Theft 6. Physical Break-in 7. Social Engineering (Phishing) 8. Law Enforcement Request 9. Policy Violation
Incident Timeline	Date/time that the incident was discovered Date/time that the incident was reported Date/time or data range that the incident occurred (if known)
Who or what reported the event	Contact Information for the Incident Reporter: full name, userID, organizational unit/department, email address, phone number, and location (mailing address, office room number). If an automated system reported the event, include the name of software package, name of the host where the software is installed, physical location of the host, host or CPU ID of the host, network address of the host, and MAC address of the host if possible.
Incident Contact Information	List contact information for all parties involved in the incident.

Detailed description of the event	Include as much information as possible such as: Description of the incident (how it was detected, what occurred) Description of the affected resources Description of the affected organizations Estimated technical impact of the incident (i.e. data deleted, system crashed, application unavailable) Summary of response actions performed Other organizations contacted Cause of the incident if known (misconfigured app, unpatched host, etc.) List of evidence gathered Total hours spent on incident handling and/or additional non-labor costs involved in handling (estimate) Incident Handler Comments
Identification of the host(s)	Source of the Incident: List of sources Host name/IP Address Target of the Attack: Host Name/IP Address (note: Target of the attack should not be listed for incidents involving protected health information or sensitive student information)
Incident Handling Action Log	Include: actions taken, when, by whom
Physical Security Controls	If there is limited physical access to the computer, document the physical security controls that limit access (ask the person reporting the event to describe what they have to do to access the computer).

UC PRIVACY / SECURITY INCIDENT REPORT FORM

The online UC Privacy / Security Incident Report Form must be used when reporting incidents to UCOP. It is likely that complete information will not be available during the initial incident phase however reporting must not be delayed due to lack of information. It is the responsibility of the reporter to update the form as additional information becomes available.

INCIDENT CLASSIFICATION

All incidents that are processed by an IRT shall be classified by the IRT. Incident classification informs those involved of the severity and impact of the incident, and ensures that the incident receives the appropriate level of attention. Classification also ensures that the incident is reported timely to management.

If the incident was previously classified before being reported to the IRT (by an IT organization, for example), the IRT must re-evaluate that classification—preferably with a clean-slate approach—and come to its own determination, based on the collective input of the IRT.

The incident classification table, Figure 1, provides several incident factors to assist in proper incident classification. Depending on the nature of the incident, some of the incident criteria represented in the table may not be present in a particular incident. Moreover, if an incident contains characteristics in several different severity columns, the severity of an incident must reflect the highest category. For example: if an incident affects a service that possibly involves personally-identifiable information (medium severity) with a likely definite public impact (high severity), the incident should be classified as high severity.

Incident classification is a dynamic process. Incident severity may change one or more times as incident details emerge over time during the investigation process.

Figure 1
Incident Classification Table

Incident Factors	Incident Severity Characteristics		
	Low	**Medium**	**High**
Criticality – Application	Internal Systems and Applications	Internal or External Systems and Applications	Internal or External Systems and Applications
Criticality – Infrastructure	No	Limited Scope	Campus-wide impact
Impact – User/System	Affects few people or few systems	Department-wide impact	Campus-wide impact
Impact – Public	None	Potential Impact	Definite Impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures
Encryption	Robust encryption algorithm (e.g., FIPS 140-2 compliant), and key control	Weak algorithm and/or key controls	No encryption, or easily defeated encryption
Resolution Procedures	Available and well-defined	Resolution procedure not well-defined, bypass available	No resolution procedures or bypass available
Information Sensitivity	Affects an individual researcher or unit	Affects a School or a small campus	Statewide or National impact
Intellectual Property	Initial datasets	Research working papers and completed datasets	Publishable research
Protected Information (Personally-Identifiable Information or Protected Health Information)	None	Possible	Definite

CONTAINMENT STRATEGY

A containment strategy must be implemented that will limit the damage to University resources. The containment strategy must include contact information for various campus organizations and personnel who may be involved in incident response. Containment may involve a combination of technical controls, such as network and system disconnects, as well as media and communications to the public and to staff, depending upon the scope of the breach.

PRESERVATION OF EVIDENCE

Preservation of evidence is discussed in detail in the following Section, however consideration should be given to preserving evidence during the Triage and Scoping Phase, particularly if it becomes apparent that the incident involves criminal activity. Containment, however, takes precedence over preservation while the incident is active. Proper preservation of evidence requires establishment of chain of custody procedures prior to an incident. Any electronic evidence should be properly tracked in a documented and repeatable process. Preservation of evidence is also required for the purposes of insurance coverage, and failure to do so may limit or impact insurance recovery—consult with Risk Management/Services for incident-specific guidance).

INCIDENT DOCUMENTATION

The importance of adequate and sufficiently-detailed documentation cannot be over-emphasized, especially if regulatory investigation(s) or lawsuit(s) arise as a result of the incident. Very serious consideration must be given to dedicating a single, full-time resource to adequately document the decisions that are made, and the actions taken, particularly for larger incidents. It is especially important to begin this type of documentation as soon as the need for an IRT is identified, so that documentation is not done retrospectively (to the greatest extent practically possible).

Here are some kinds of questions that the documentation should consider:

- How was the decision made on how the incident was scoped, and thus what forensic data is in-scope or out-of-scope? How do we know we have all the relevant data in the hands of the analyst team? Why did we look at these systems, and no others?

  Objective: prove that no other systems (and hence forensic data) need to be considered by the analysts, and be sure we have a complete inventory of what's in-scope.

- How the determination was made about which people were potentially affected by the incident? In particular, how could this decision process be repeated to generate the same list, by another analyst? Are the data and the scripts processing the data organized and documented enough to allow for this?

  Objective: a repeatable procedure that stands on its own, so that the original forensic data would not need to be turned over to opposing counsel.

- How were notifications made to the affected people? In particular, where did you get the notification addresses (email, US mail, etc.)? How were bounces/returns handled? How were conflicting or multiple addresses handled? What did you do if you didn't have an address for people?

  Objective: show the details of notification clearly met due diligence.

IDENTIFY AND ENGAGE RELEVANT EXPERTISE

Identifying and engaging groups and individuals with relevant expertise is critical to accurately triage an incident and determine its scope. In large or complex cases, the IRT should consider bringing in a third party, such as another UC campus, or external organization to assist in the triage and scoping effort. In order to verify if BUS-81, *Insurance Programs*, provides coverage, the

insurance carrier may conduct a forensic investigation and participate in the incident response activities. Cooperation with the insurance carrier is required under the terms and conditions of the insurance policy.

COMMUNICATION/DISCLOSURE STRATEGY

Proper handling of internal and external communications is critical in the initial phases of incident response. It is quite possible that an initially small incident could blossom into a large multi-site incident. It is also quite possible that a suspected incident could be determined to be unfounded. Improper handling of communications could lead to embarrassment to the University in the event of a false positive, or could tip off any malicious attackers to cover their tracks, thus exposing the University to more risk.

Communication of incidents should be handled on a need-to-know basis, especially early on. Preferably these communications should be handled via an encrypted or "out-of-band" mechanism (such as cell phones—be wary of VoIP telephony systems) to avoid exposing this information to attackers.

Legal counsel should be consulted to determine whether the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel may establish particular procedures for communication and documentation.

All communications about the incident external to the IRT should be approved by the IRT. All communications about the incident external to the University must be approved by the IRT.

If it is suspected that other UC Campuses are vulnerable to a similar attack, the IRT Coordinator should alert the other UC Campuses. The UCSIRC list server provides a mechanism for such alerts.

If it is suspected that other UC Campuses are vulnerable to a similar privacy breach, the IRT Coordinator should notify the Systemwide Information Security & Privacy Officer, who will alert other campuses.

REFERENCES

NIST 800-61, *Computer Security Incident Handling Guide*

SECTION 3: EXECUTION

PREPARATION

The IRT should collect and/or review the incident documentation and event reports. This information should first be verified as being factual (information may have been mis-reported, or incorrectly documented). The IRT should assign the incident severity, or re-consider its appropriateness if already assigned. The IRT should determine who, outside of the IRT, needs to be notified of the incident, both internal and external to the affected campus and the University, and make those notifications. Information should be restricted on a need-to-know basis.

If the incident requires computer forensic analysis, arrangements must be made to gain access to the data and devices involved in the incident. Refer to Exhibit A: Forensic Evidence Methodology.

At this stage, thoroughness is more important than speed. The primary objective is to maintain and restore business continuity.

Every incident should be treated as if it will lead to a court case. Establish robust documentation procedures, by, for example, including the date and time of every entry in the incident log, and signing every page of the log. Document each individual's time spent on the incident, and any other incident response costs.

Refer to Exhibit B: Incident Response Check List.

CONTAINMENT

The IRT Coordinator must ensure that sufficient staff with appropriate technical skills are assigned to do an effective job of containment.

The IRT must assess whether to disrupt services to internal or external customers. Decisions of this nature must be made in consultation with the appropriate senior leadership and an evaluation of whether the systems impact critical patient care. life-support, or similar critical services.

If not already accomplished:

- Document how the incident was detected and contained
- Document all activities and include a date / time log as appropriate, e.g., who did what when

ANALYSIS: DATA & SYSTEMS

ASSESS THE CAUSE AND TYPE OF BREACH

Depending on the documentation provided to the IRT, it should either validate or determine what types of data are involved, e.g., personally identified information (PII), protected health information (PHI), which identifiers were involved, whether the data was encrypted (and the method / strength of encryption), adequacy of password security, the type of incident, and whether logging was active and adequate. It is particularly important to validate information provided to the IRT, as some breaches have initially overlooked PII or PHI. The cause of the breach is determined by technical analysis and investigation, as described below.

FORENSIC ANALYSIS

Forensic analysis entails a technical examination of evidence, preservation of that evidence, preservation of the chain-of-custody of the evidence, documentation of observations, and analysis drawn from logical conclusions based on the evidence, absent opinion or conjecture. When conducting a forensic analysis, the analyst must adhere to the following principles:

- Analysis must be an unbiased examination of the evidence submitted.
- The original evidence must be preserved intact; every effort must be made to work only on copies of the original.
- Forensic analysis does not pronounce or imply guilt. The purpose is to determine whether indicators exist that can tie the suspect hardware to the incident under investigation.
- Develop and record an hypothesis:
  - How does the evidence support/contradict it?
  - What did you do, what evidence did you find, and how did you test the hypothesis?
  - What important interactions took place?
  - Were there any other ideas at the time?
  - Record anything that helps the organization collectively remember things accurately.
- Report only verifiable information.
- Unless critical to the analysis, do not use names of persons, companies or organizations in the report. Instead refer to “subject”, “suspect”, or “victim”.
- Be precise. Statements such as “numerous”, “many”, “multiple hundreds”, etc. should be avoided. Specifically state the finding, as well as the precise locations of information.
- Identify the evidence being analyzed as thoroughly as possible.

ASSESSMENT OF INCIDENTS

Refer to the most recent version of the document entitled *Information Breach Decision Tree for California State Law* (available from UC HIPAA Officers or Health Lawyers). Using that document, the IRT must perform an analysis to determine whether individuals and/or state agencies need to be notified of the breach, and ensure that regulatory deadlines for such notification are met.

ASSESSMENT OF INCIDENTS INVOLVING HIPAA PHI

Refer to the most recent version of the document entitled *Information Breach Decision Checklist for HIPAA* (available from UC HIPAA Officers or Health Lawyers). The IRT must perform and document a risk assessment (in accordance with that document) to determine whether there is a significant risk of harm to the individual whose PHI (protected health information) was inappropriately released or disclosed into the wrong hands. Ensure compliance with any required notifications.

REPORTING FINDINGS

The complete evidence collection and subsequent analysis process should be documented thoroughly and in detail.

Complete and submit the Incident Report[7] required by Business and Finance Bulletin IS-3, ensuring that the following information is included:

- High-level description of the incident and its scope
- Impact on the organization
- Actions taken to prevent future occurrences
- Recommendations for further action

Create a Technical Report that includes:

- Detailed information about the event, including actions taken and personnel involved
- Detailed information about the investigation
- When, where, and from whom the evidence was received (or taken)
- The physical analysis (visual evaluation), including brand names, model numbers, and serial numbers
- The forensic duplication, including how the image was made (for digital evidence), the software and hardware used to make the image, and the hash comparison results
- Every step taken in the analysis of media. Explain what tools were used and what was or was not discovered as a result of these processes. Document other information such as: number and size of sectors, operating systems, significant software, anti-virus, crash-guard software, etc.
- All conclusions reached
- How and when the evidence was returned or the manner in which it was disposed
- Note: data used in this report should reference collected evidence, and be verifiable

NOTIFICATION PROCESS

General categories to consider in the notification processes:

- Identify the victims of data theft and cross-reference with other databases to compile the most recent contact addresses.

- Develop a Call Center: Decide on using an internal vs. external; toll-free telephone number; determine the staffing (numbers) and coverage hours and days of week; train staff to respond to incident calls (provide standard scripts); comfortable setting (head-sets, quiet area, computer); bi-lingual skills, etc.

- Communications Plan: identify who needs to be notified (internal / external), who is responsible, co-ordinate the response and message; develop internal FAQs; press release draft; escalation guide for call center; formal notification to other agencies, vendors, donors, politicians; media contact persons; press briefing.

[7] http://www.ucop.edu/irc/itsec/uc/documents/UCIncidentReportForm.v1.doc

- Notification methods: internal e-mail, US mail, media alert/press release; mail house/breach response company; type of letterhead and whose signature; envelope style; finalize the letter and determine whether to include FAQs with the letter.
- Refer to Exhibit C: Components of a Notification Letter.
- Administrative issues: Determine who signs the letter, which letterhead, style of envelopes, establish a separate account / index # for mailing expenses and for tracking all expenses, order stationary and envelopes for the mailing.
- Regulatory agencies: determine which agencies (e.g., CDPH, OCR, etc.), if any, require notification; provide each agency with their required information, in the format and manner (electronic, written, etc.) they require
- Mail house: Determine whether the mail house is required to cleanse the list with National Change of Address Office; if so, determine if you want to be notified of address updates; execute a HIPAA Business Associates Agreement (BAA) with the external mail house if the incident is associated with a breach of PHI (protected health information).
- Policy / Legal Issues: Consult with UC Counsel to identify possible legal issues that may need clarification; develop responses.
- Notification Launch & Co-Ordination: Update relevant stakeholders prior to sending the letters.

Document:

- Responses to letters and concerns.
- Include any unauthorized disclosure of PHI on the HIPAA Accounting for Disclosures log.
- Include any sanctions in the HIPAA sanctions log.

TIMING OF NOTIFICATIONS

Refer to the most recent versions of the documents entitled *Information Breach Decision Tree for California State Law* and *Information Breach Decision Checklist for HIPAA* (available from UC HIPAA Officers or Health Lawyers) for guidance on regulatory requirements for the timing of notifications to affected individuals, regulatory agencies, and the media, if appropriate.

REFERENCES

45 C.F.R. §§ 164.308 (a)(6)(i) & 164.308 (a)(6)(ii)

California Civil Code §§ 1798 & 1798.29

ARRA / HITECH Act, Section 13400

California Health and Safety Code § 1280.15

Federal Register Vol. 74, No. 162, August 24, 2009

California OHII: "Privacy / Security Advisory Guidelines for Health Information Exchange", Section 5.5 http://www.ohi.ca.gov/calohi/LinkClick.aspx?fileticket=Eoy3ujiykHI%3d&tabid=56

Excerpts from Debix, Inc. *Data Breach Incident Response Workbook*, http://debix.com/workbook/index.php

SECTION 4: REMEDIATION AND POST-INCIDENT REVIEW

RESPONSIBILITIES

The IRT Coordinator initiates and coordinates remediation and post-incident activities as soon as basic risk mitigation activities have been taken to stabilize the environment. The IRT Coordinator keeps the Chancellor's designee informed of status and actions being taken throughout the remediation and post-incident review process.

Based on reviews of findings at the time, and an assessment of project size and complexity, the IRT Coordinator convenes one or more Remediation and Post-Incident Review Teams (PIRTs).

- The IRT Coordinator and PIRTs document findings and activities continuously throughout the review.
- Scopes of various PIRTs may be segmented by type of technical expertise required, and/or by required knowledge of policy or organizational issues, as appropriate for the particular situation.
- The IRT Coordinator may be a participating member of PIRTs or may delegate the work to other individuals. In any case, the IRT Coordinator maintains continuous, close communications with PIRTs, and over-all control of remediation and post incident review activities.
- PIRTs analyze conditions in the IT environment local to the incident, including technical, policy, and organizational aspects. Scope of review includes circumstances and activities before the incident as well as during the response.
- Throughout the process, the IRT Coordinator and PIRTs continue to analyze implications of local IT environment issues and assess scope of areas potentially affected, potentially including other IT environments throughout the campus/lab/med center.
- The IRT Coordinator and PIRTs prepare an action plan for recommended changes to improve the local environment going forward.
- PIRTs document lessons learned, including aspects that were good as well as those which were problematic.

TECHNICAL ACTIONS

Specific technical review activities should include:

- Review whether remediation of affected local system(s) is complete.
    - Vulnerable hardware or software has been hardened against any break-ins, future attacks, or other security issues (e.g. installed patches, updated versions, replaced vulnerable sections of code).
- Conduct a root-cause analysis.
- Assess whether security vulnerabilities can be adequately remediated by making changes within the current environment or a new/replacement environment should be created.

- Take needed actions to restore essential systems to functioning status, either in the original or a repaired environment, or determine that the activities must cease or be suspended until a different or rebuilt environment can be created. If replacing the environment:
  - Review technology choices
  - Design proposed new environment
  - Create new (replacement) environment
  - Bring in preserved data or re-create the data anew
- Identify any areas where different technical measures would have prevented the breach or improved results in this environment. Also identify what technical measures worked well.
- Consider whether continuous monitoring of the local environment needs to be implemented or enhanced, including what type(s), and whether an outside neutral party should conduct the monitoring.
- Consider whether issues before the breach or during the response had detrimental impact on any out-of-scope systems, either locally, on-campus/lab/med center, or on the Internet at large. If so, conduct outreach to alert other appropriate contacts of possible need for reviews to discover whether they experienced impact.
- Analyze whether to recommend additional types of reviews in the local environment or elsewhere throughout the campus/med center/lab.
- Share lessons learned with appropriate contacts.

POLICY AND ORGANIZATION

Analyze sufficiency of policies and procedures, efficacy of organizational structure, and accountability of those who were involved, or should have been involved, in risk mitigation and in the response. Include internal and external environments and individuals who are staff, management, and organizational leaders.

- Review performance by individuals prior to the incident, including whether:
  - Sufficient roles and responsibilities relevant to this particular type of incident had been identified and were adequately documented in written procedures;
  - Role holders had been clearly informed of their responsibilities, and provided with requisite knowledge and skills to fulfill those responsibilities;
  - Role holders were regularly reviewed for performance of risk mitigation responsibilities, i.e.: security assessment and implementation of commensurate protective measures.
- Review performance during the incident response, including whether individuals:
  - Proactively assumed appropriate level and type of involvement in the response;
  - Followed documented response procedures when available and appropriate;
  - Acted productively and responsively to directions given by the response team and/or other leadership individuals, as appropriate;
  - Created and maintained adequate documentation of the incident response;
  - Acted with honesty and integrity to obtain needed information, and perform appropriate investigatory actions.

The IRT Coordinator will review whether, in the response to this incident, reporting lines were clear and organizational structures worked effectively, e.g.: lines of communication were sufficient and effective , escalation was paced appropriately, media communications were handled well, sufficient expert resources were available (legal, technical, service referral, expedited vendor arrangements).

RECOMMENDATIONS AND NEXT STEPS

The IRT Coordinator assesses findings and recommendations of the PIRT(s), and then issues a report of the incident and its response to the Chancellor's designee, including findings and recommendations. The report should be formatted in a modular manner for discrete use in varied communications with audiences having different levels of security clearance. The IRT Coordinator then leads follow-up actions, including:

- Document the vulnerabilities (including information from the Triage and Scoping Phase):
  - locations and/or events where the failures or compromises occurred;
  - the likely causes of the problems with supporting details;
    i. hardware, software
    ii. operational procedures
    iii. staff misconduct or insufficient skills
- Identify any areas where different technical remediation measures would have improved results in this environment. Analyze whether those "upgrades" could and should be applied to other areas within the larger environment. If so, recommend how to apply improvements to other areas.
- Upon approval of the Chancellor's designee, works with the CIO and other stakeholders to convene appropriate team(s) to start remediation activities throughout the campus/lab/med center environment.
- Prepare detailed action plans and/or project descriptions to improve the technical environment both locally and throughout the campus/ lab/med center.
- Identify any areas where policy, guideline, or organizational structure changes would have improved results; then work with responsible campus authorities (e.g. IT Policy Officer, Security Committee, Policy Review Board, and/or executives) to propose, refine, and issue any new or updated policies, guidelines, procedures, or organizational structures as deemed appropriate.
- Determine whether broad education, training, and/or awareness efforts are necessitated. If appropriate, develop and deploy general or targeted education, training, and/or awareness.
- In close cooperation with organizational contacts responsible for providing "due process" rights, ensure that responsive personnel actions or misconduct actions are considered and are pursued when appropriate.
  - Organizational responses may range from education or documented advisements up through escalation to dismissal.
  - Some actions may be referred to outside agencies for investigation and possible imposition of criminal proceedings.
- Identify and document needed corrective actions
  - Begin corrective actions

  - Track progress of corrective actions
  - Verify that the actions corrected the problem or re-assess needed corrective actions.

- Identify aspects of the response environment that served the organization well and analyze how/whether to apply the tenets of those to other areas within the larger environment, through outreach, cloning of local procedures, or other means.

EXHIBITS

EXHIBIT A: FORENSIC EVIDENCE METHODOLOGY

Once an incident has been declared and a decision has been made to preserve electronic evidence for use in either administrative, civil or criminal remedies, specific steps should be taken to ensure integrity of data and preservation of evidence.

Maintain a chronological log (date and time) of actions taken, and sign each page.

DETECTION

Type of incident and possible locations for evidence: The list below is not all-inclusive, and should not limit the scope of evaluation as to where digital evidence may only be found.

Type of Incident	Possible Locations of Relevant Evidence
Network Intrusions	System logs User logs Proxy logs Router & Firewall logs
Email	Mail Servers Router & Firewall logs Individual workstations Backup tapes
Internal Employee or Contractor Activity	System logs Mail Server Logs User Logs Proxy Logs Router & Firewall logs Individual Workstations Electronic organizers Removable media

PRESERVATION OF EVIDENCE

Consult with UC Counsel prior to searching or seizing computers.

Chain-of-custody: utilize a chain-of-custody form for documenting and securing evidence items recovered during an incident, and the date/time and identity of team members involved.

The following concepts should be applied:

- Actions taken to secure and collect electronic evidence should not change the evidence.
- Persons conducting examination of electronic evidence should be trained and preferably certified for this purpose.

- Activity relating to the seizure, examination, storage, or transfer of electronic evidence should be fully documented, preserved, and available for review.
- *Note: Incident responders should use caution when seizing electronic evidence devices. The improper access of data stored on electronic devices may violate provisions of federal law, such as the Electronic Communications Privacy Act (ECPA). Consult with UC Counsel*.

COLLECTING EVIDENCE

Securing and evaluating the scene: first responder should evaluate the scene and formulate a search plan. The condition of electronic devices should not be altered unless a threat to the safety of persons is indicated, or business operations are such that continued operation or non-operation threatens vital UC business operations. The decision should be made in consultation with the IRT.

Protect perishable data both physically and electronically, such as data found on pagers, caller ID boxes, cell phones, smart phones and other similar devices.

"Volatile" data, such as network connections, processes, login sessions, open files, network interface configurations, and the contents of memory, should be carefully captured from active systems.

HANDLING OF EVIDENCE

Full forensic disk images should be made to sanitized write-protectable or write-once media. File system backups should not be used for investigatory and evidentiary purposes. The analysis should be performed on an image, rather than the original, which should be preserved in its original state to the greatest extent possible.

FORENSIC DOCUMENTATION

- Description of the incident and how it was detected. Determine when the incident started (if possible) and how soon the organization detected it.
- Record exact dates and times, if known.
- Observations about the condition and location of the computer system including power status of the computer (on, off, or in sleep mode), and related electronic components.
- Photograph, if possible, the entire scene to create a visual record as noted by the first responder.
- Preservation of evidence. Document how and when the evidence was returned or the manner in which it was disposed.

EXHIBIT B: INCIDENT RESPONSE CHECK LIST

Privacy & Data Security Incident Response Checklist & Project Schedule				
Date:				
Last Update:				
Version:				
Step/ ID #	Tasks	Completion Date	Resources (Name or Dept)	Complete (yes/no)
1	**Identify Victims of Data Theft / Build Notification List**			
1.1	**Conduct Forensic Analysis to Identify Victims' Names, Addresses, Email Addresses and Types of Data Stolen**			
1.2	**Cross-Reference List of Data – Compile most-recent contact addresses**			
	1.2.1 Cross Reference with _____			
	1.2.2 Cross Reference with HR__			
	1.2.3 Cross Reference with _____System			
	1.2.4 Cross Reference Student Information System			
	1.2.5 Cross Reference with Student Athletes Database			
	1.2.6 Cross Reference with External Address Location Services			
1.3	**Add QA Test Contact Data for External Call Center**			
1.4	Establish a budget # / index number for tracking costs to a central account, e.g., call center, postage, stationary, toll free calls, long-distance calls, equipment / furnishings for call center, overtime.			
1.5	File a police report, maintain the police report #, report date, and incorporate this data into the Call Center scripting in case victims ask for these details.			
1.6	Remediation (refer to a separate list/chronological log of actions taken)			
2	**Call Center:** *External vs. Internal -- Business decisions: consider breach size (# of victims & type of data), anticipated call volume, sensitivity of data, hours / days of call coverage and internal resources, costs. Identify bilingual staff to assist with calls.*			
2.1	**External Call Center**			
	2.1.1 Prepare contract with External Call Center Vendor + HIPAA BAA (if required)			
	2.1.2 Sign contract with External Call Center + & Require signed Confidentiality / Nondisclosure Agreement			
	2.1.3 Establish 800 number + from / to hours			
	2.1.4 External Call Center Ramp-up			
	2.1.4.1 Provide Call Center with scripts including plans for escalation of Calls			
	2.1.4.2 Establish clear QA processes			
	Create QA data to be included in data feeds so we can assess call quality without impacting true impacted individuals			
	2.1.4.3 Send data about victims of the data theft to the Call Center, so Call Center staff can identify them (and for programming their systems). Includes QA data			
	2.1.4.4 Define documentation and reporting requirements for and from Call Center			

	2.1.4.5 Define process for callback/escalation. Establish incoming institution's email address for the escalations. Integrate escalations with institution's systems used in 2.x (Internal Call Center).			
	2.1.4.6 Conduct training of Call Center staff			
	2.1.4.7 Identify designated internal staff who will participate in the Quality Assurance testing of the External Call Center. Establish QA procedures and criteria.			
	2.1.5 Institution conducts initial testing to ensure correct messages and escalation are being employed.			
	2.1.6 Launch external Call Center (date / time)			
	2.1.7 Monitor and conduct on-going QA of external Call Center			
	2.1.8 Ongoing Review External Call Center QA			
	2.1.9 Continue to analyze QA results			
	2.1.10 Analyze response statistics from Call Center			
2.2	**Internal Call Center**			
	2.2.1 Identify internal staff to work in the Call Center + set Call Center Hours Hours: During week #1 prepare mgr coverage for add' hours (7:00AM-8:00PM PST). Triage long-winded calls to a manager so as not to tie up incoming lines.			
	2.2.2 Establish campus location for the Call Center, location should be in close proximity to managers for help with call escalation questions.			
	2.2.3 Install: Computers, telephones (multi-line with line appearance display), phone headsets, furniture, whiteboard, fax machine, printer, chairs and other equipment and establish incoming toll-free numbers and long-distance code for return calls.			
	2.2.4 Identify tracking and reporting system to use for Call Center			
	2.2.5 Set up tracking system for Call Center, including ID's for all agents and response managers			
	2.2.5 Identify staff who will participate in the Quality Assurance testing of the Internal Call Center			
	2.2.6 Provide Call Center staff with Scripts			
	2.2.7 Train Call Center staff			
	2.2.8 Conduct QA Testing of Staff by conducting simulated calls			
	2.2.9 Monitor and conduct on-going QA of Internal Call Center			
	2.2.10 Create institution's e-mail address & determine who will respond to emails from victims. (E-mail script)			
	2.2.11 Timing for 1st calls: Expect calls to start arriving 24 hours after mailing, be prepared.			
	2.2.12 Establish an internal call center database or ishare list to manage incoming calls and where call backs are needed.			
	2.1.13 Notify Credit Bureaus in advance -- as a "courtesy heads-up notice to expect calls". Ask for a direct telephone # for a customer service agent and an incident #. Obtain this information by sending the credit bureau an e-mail or by entering a dummy # to get through to customer service agent. Although most victims will be comfortable with the automatic fraud alert process, some callers will insist on speaking with a real person. Have this customer service direct number available in the Call Center script. Practice initiating a fraud alert, so that you can explain the process to victims.			

3	**Communications**			
3.1	**Plan Communications**			
	3.1.1 Identify Communications that need to be created			
	3.1.2 Identify who from institution will be participating in the response			
	3.1.3 Coordinate response planning with partner institutions effected by incident.			
3.2	**Create Communications**			
	3.2.1 Internal and External FAQ's			
	3.2.2 Press release - Draft and launch via designated spokesperson			
	3.2.3 Drafts of notification letters to various segments of the "victim" audience			
	3.2.4 Call center scripts			
	3.2.4.1 External Call Center			
	3.2.4.2 Internal Call Center			
	3.2.5 Communications to employees, vendors and business partners			
	3.2.6 Timeline for web site			
	3.2.7 “Resource" and "Reference" page for web site			
	3.2.8 Introductory piece for web site			
	3.2.9 Escalation guide for call center			
	3.2.10 Internal communications to leadership & advisory groups			
	3.2.11 Notification to institution's switchboards/operators, security, frontline staff			
	3.2.12 Formal Notification to development and alumni officers			
	3.2.13 Notification to vendors/suppliers (e.g. insurance, etc).			
	3.2.14 Notification to politicians??			
	3.2.15 Communication for internal stakeholders likely to have contact with victims			
3.3	**Send Out Victim Notification E-mails** *(will happen in waves based on getting the best data available from various data stewards)*			
	3.3.1 Identify e-mail addresses			
	3.3.2 Identify mechanism for sending e-mails			
	3.3.3 Identify which recipient receive which e-mails			
	3.3.4 Prepare email recipient list(s)			
	3.3.5 Send out e-mails to data theft victims			
3.4	**Send out Traditional U.S. Mail Letters to Victims** *(will happen in waves based on getting the best data available from various data stewards)*			
	3.4.1 Identify vendor / mail house to send out letters			
	3.4.2 Decide on which institution letterhead to use, which return address, signature			
	3.4.3 Order institution stationary + window envelopes			
	3.4.4 Prepare mailing list of Data Victims who should receive letters and which letters they should receive. Decide whether to include a page of FAQs.			
	3.4.5 Send final wording for the letter(s) to the Mail House Vendor for mail-merge			
	3.4.6 Send the Mailing List to the Mail-House Vendor with victim addresses and indicate type of letter to be sent to each recipient. Excel file: one data element per column: Mr/Ms, firstname, lastname, street addr1, street addr2, city, state, zip			

	3.4.7 Vendor prepares letters for mailing. For large mailings, Vendor will vet the address list to the "National Change of Address" (NCOA) clearinghouse (US Postal Service) to expedite delivery. Determine if you need to be informed of address changes. Process is sometimes referred to as "cleansing the mail list".			
	3.4.8 Decide if the letters will be sent via bulk mail or 1st class postage			
	3.4.9 Send Out Letters			
	3.4.10 Instruct Mail House Vendor what to do with the mailing list afterwards			
	3.4.11 Assign a call center staff member to document "mail bounce-back letters" in the call center database, for tracking purposes.			
3.5	**Media Relations**			
	3.5.1 Campus Communications or Media Point person			
	3.5.1.1 Identify the Campus Point Person to talk to the media			
	3.5.1.2 Conduct media training for campus point person to talk to the media			
3.6	**Press Release**			
	3.6.1 Identify Recipients of the press release			
	3.6.2 Send out press release			
	3.6.2 Conduct press briefing			
3.7	**Campus Response Web Site**			
	3.7.1 Identify where to host Web Site			
	3.7.2 Identify name for the Web Site			
	3.7.3 Register the domain name for the web site			
	3.7.4 Build the web site			
	3.7.5 Test the web site			
	3.7.6 Launch the web site			
	3.7.7 Include the web-link in the notice to victims			
	3.7.8 Depending on the size of the breach (e.g., # of individuals > 10,000) consider whether to post information about the incident on the UC Ethics Point Hot Line site (interim page posting for 60-days), in case public queries the site or calls the UC Hot Line looking for incident details. Include your local web-site and toll-free number for managing call referrals.			
3.8	**Campus Communication**			
	3.8.1 Send out Leadership memo, e.g., deans, directors, chancellor, inst president's office			
4	**Policy and Legal Issues**			
4.1	Identify types of responses required by State / Federal laws and campus policy			
4.2	Consult with counsel to determine whether to provide a voluntary notice to State / Federal agencies *(Note: If media coverage is likely, a courtesy notice is recommended -- even if not required to do so by law)*			
	4.2.1 If the number of affected California residents is more than 500, submit an electronic sample copy of notification to the California State Attorney General.			
4.3	Identify key policy questions to answer for response			
4.4	Determine answers for identified policy and legal issues			
	4.4.1 Will the campus offer identity theft insurance to the victims of the data theft?			

	4.4.2 What is the law regarding compensation for individuals who were victims of the data theft? What is the potential liability of the campus?			
	4.4.3 Did the institution violate any campus policies that led to the data theft?			
5	**Launch Response**			
5.1	Prepare readiness Check-list to launch response			
5.2	Fill out readiness Checklist			
5.3	Receive "O.K. for Launch" from project leads and campus leadership			
5.4	Launch (date: MM/DD/YYYY)			
6	**Conduct Review of Response and Document Lessons Learned**			
6.1	Preventive approach in case of next incident			
6.2	Update checklist accordingly			

EXHIBIT C: COMPONENTS OF A NOTIFICATION LETTER

Edit the following components into a letter of notification or a web site statement. The letter or statement must be written in plain language. Do not disclose anything that might hamper the investigation or give additional information to those who would do harm.

- What happened?
- When did the breach occur and/or when was it detected?
- How was it detected?
- What data was potentially compromised?
- How much data was compromised?
- Whose data was compromised, e.g., students, staff, faculty, patients, etc.?
- Why you are being notified.
- What steps are being taken, e.g., machine off the net, law enforcement notified (local, FBI), credit card companies notified (for cases where contact information is needed about cardholders), etc.
- Is any data known to be fraudulently used or is notification precautionary?
- Was the notification delayed as a result of a law enforcement investigation?
- What steps should individuals take? Example: Place a fraud alert with credit bureaus, contact credit card companies, close accounts, etc.
- Text: Although there is no evidence that an unauthorized person has obtained your personal information and is using it, there are some steps you can take to protect yourself … Insert name of credit bureaus, telephone numbers, web-links, FAQs, or insert the CalOHII ID Theft Prevention Document.
- Apology or statement of commitment to security. Example: We regret that your information may have been subject to unauthorized access and have taken remedial measures to ensure that this situation is not repeated. UCXX is committed to maintaining the privacy of <category of> personally identified information and takes many precautions for the security of personal information. In response to incidents of theft like this one and the increasing number of internet-enabled computer attacks, the University is continually modifying its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.
- Anticipated next steps, if any. e.g., intention to notify if any additional information becomes available.

- Who to contact for additional information. Contact name, number, hours of availability, web-site, hotline, e-mail address, etc. Should you have further questions about this matter, please contact [name of contact], at [e-mail address of contact] or [phone number].
- Signature. Who makes the most sense – president, dean, other contact familiar to the individual, consider multiple signatures for different constituent groups.
- Letterhead. Decide which institutional / facility letterhead to use.

VERSION HISTORY

Version	Date	Summary of Changes
1.0	December 17, 2010	
1.1	February 3, 2011	• Coordination with BUS-80, *Insurance Programs for Information Technology Systems* • Added Alternate Contact • Added Version History
1.2	December 1, 2011	• Added requirement to send sample notification letter to Attorney General if over 500 individuals • Added requirement that notification letter must be written in plain language.
1.3	July 1, 2012	• Added requirement for EthicsPoint form.