UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES (USU)

SUBJECT: UNIVERSITY PRIVACY PROGRAM

Instruction 7751

(OAC)

RECEIVED JAN 2 8 2018

ABSTRACT

This USU instruction details implementation of the DoD Privacy Program in accordance with Department of Defense Directive number 5400.11, "DoD Privacy Program, the Privacy Act of 1974, as amended; and, the Department of Defense Instruction 5105.45," Uniformed Services University of the Health Sciences.

A. Purpose. To ensure that all USU military, civilian, and contractor employees are fully aware of their rights and responsibilities under the provisions of the Privacy Act of 1974; to balance the government's need to maintain information with the obligation to protect individuals against unwarranted invasions of their privacy stemming from the USU's collection, maintenance, use, and disclosure of Personally Identifiable Information (PII); and, to require privacy management practices and procedures be employed to evaluate privacy risks in systems of records and other information collections. Additionally, this instruction establishes the authority and responsibilities of the USU Privacy Officer under the authority invested in the University President by the Assistant Secretary of Defense for Health Affairs and is prescribed in accordance with the Privacy Act of 1974, DoD Directive 5400.11, and DoD Regulation 5400.11-R.

B. Reference. *See Enclosure 1.*

C. Applicability. The provisions of this Instruction apply to all USU departments, centers, institutes, and other functional activities.

D. Mission. The USU Privacy Office exists to oversee all ongoing activities related to DoD Directive 5400.11, "DoD Privacy Program," and the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, PII, to include Protected Health Information (PHI), in compliance with Federal and state laws and the organization's information privacy practices.

E. Organization and Management. The USU Privacy Office is an independent and objective organizational component reporting to the Assistant Vice President, Accreditation & Organizational Assessment (OAC).

1. The University President shall act as the Senior Component Official for Privacy (SCOP).

2. The USU Privacy Officer shall be appointed by and have direct access to the through the Office of the Chief of Staff.

3. If determined necessary, an Assistant Privacy Officer may also be appointed at the discretion of the SCOP. The Assistant Privacy Officer shall serve as Acting USU Privacy Officer when the Privacy Officer is otherwise unable to perform the functions and duties of the office.

F. Responsibilities and Functions. The Privacy Office shall:

1. Provide development guidance and assist in the identification, implementation, and maintenance of USU information privacy policies and procedures in coordination with DoD and USU leadership, management, administration and legal counsel.

2. Complete initial and periodic information privacy risk assessments. Conduct related ongoing compliance monitoring activities in coordination with other compliance and operational assessment functions. Ensure the proper administrative, technical, and physical safeguards are in place to protect PII and related information systems.

3. Collaborate with legal counsel, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization, and information notices and materials reflecting current organization and legal practices and requirements.

4. Oversee, direct, deliver, or ensure the delivery of initial privacy orientation and training to all applicable employees, volunteers, medical and professional staff, contractors, and other appropriate parties with access to information resources. Oversee the provision of privacy refresher training to applicable employees working with PII or PHI. Initiate, facilitate, and promote activities to foster information privacy awareness and best practices within the University and related entities.

5. Participate in the review of ongoing System Security Verifications (SSVs), Data Use Agreements (DUAs), Memorandums of Understanding (MOUs), Interagency Agreements, cooperative research and development agreements, and other documents to ensure all privacy concerns, requirements, and responsibilities are adequately outlined.

6. Work cooperatively with applicable organization units in overseeing individuals' rights to inspect, amend, and restrict rights to records and PII/PHI when appropriate.

7. Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions (i.e. Cybersecurity, Institutional Review Board (IRB), and when necessary, legal counsel).

8. Provide Privacy Act subject matter expertise (SME) to the University's IRB, cybersecurity functions, and clinical, administrative, and information systems. Serve as privacy resource to all USU departments and appropriate entities.

9. Coordinate with all University personnel involved with any aspect of collection or release of PII/PHI to ensure full coordination and cooperation under DoD and University policies, procedures, and legal requirements. Ensure information collections include a Privacy Act Statement, if required.

10. Maintain current knowledge of applicable Federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.

11. Investigate, mitigate, document, and report any breach or potential breach of PII/PHI in accordance with DoD Regulation 5400.11-R and OMB 17-12 [references (c) and (d)]. The USU Privacy Office will work in coordination with the University's Office of the Chief Information Officer (OCIO), the United States Computer Emergency Readiness Team (US-CERT), the Office of the Secretary of Defense and Joint Staff (OSD/JS) Privacy Program, and the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD).

12. Establish and maintain a Privacy Incident Response Plan (PIRP). The PIRP establishes the Privacy Incident Response Team (PIRT) membership, to include: USU Privacy Officer, Information Systems Security Officer, Information Systems Security Manager, Office of General Counsel, department leadership of affected area, and others, as necessary (such as the Walter Reed National Military Medical Center Privacy Office, Office of External Affairs, the Henry M. Jackson Foundation, or other contractors, as appropriate). The PIRP, outlines responsibilities, reporting duties, and the handling / containment / notification / resolution procedures in case of a privacy incident. See the University's PIRP for full responsibilities.

13. Perform periodic reviews of current USU System of Records Notices (SORNs) to ensure accuracy and completeness of all applicable record systems. This process can include Privacy Impact Assessments (PIAs) in accordance with DoDI 5400.16 [reference (e)], social security number use justification [reference (f)], and compliance with the Paperwork Reduction Act (PRA) [reference (g)].

14. Ensure that any collection or use of SSNs, new or existing, is necessary and complies with applicable privacy and security requirements.

15. Include appropriate Federal Acquisition Regulation and Defense Federal Acquisition Regulation Supplement privacy clauses in all contracts that provide for contractor staff to access Privacy Act systems of records.

16. Provide information as directed by OSD/JS Privacy for various privacy reports, which include the privacy portion of the annual Federal Information Security Modernization Act Report (FISMA) submitted to the Office of Management and Budget, and the semi-annual report pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 which is provided to Congress and the DPCLTD.

G. Relationships.

1. In the performance of assigned responsibilities and functions, the USU Privacy Office shall:

a. Report to and be under the general supervision of the Assistant Vice President, Accreditation & Organizational Assessment. No activity or authority shall be permitted to prevent or prohibit the USU Privacy Office from initiating, carrying out, or completing any investigation, evaluation, inspection, or other privacy-related tasks, except as specified in the Privacy Act of 1974 or DoD Privacy Program [references (a) and (b)].

b. Coordinate actions, as appropriate, with other University components and, unless precluded by the nature of the matter, notify the heads of the components concerned before conducting investigations, evaluations, audits or inspections of matters normally under the jurisdiction of the heads of the components.

c. Give particular regard to activities of USU Cybersecurity Branch within the OCIO with a view toward avoiding duplication of effort and ensuring effective, advanced coordination and cooperation.

d. Report expeditiously to the USU Office of the General Counsel whenever the Chief Privacy Officer has reasonable grounds to believe there has been a violation of Federal or state law.

e. Report expeditiously any suspected or alleged violations of chapter 47 of reference (h) (also known as "The Uniformed Code of Military Justice") to the Brigade Commander responsible for military personnel assigned to USU.

2. Nothing in this Directive shall be construed as limiting the authority and/or operational control of the authority of each respective component of the University.

H. Authorities. Pursuant to, or in addition to, the authorities provided in references (a), (b), and (c), the USU Privacy Office is delegated authority to:

1. Access all records (electronic or otherwise), reports, investigations, reviews, documents, papers, recommendations, or other information on containing PII/PHI or material available to any USU component. USU Privacy Office officials shall possess the appropriate security clearance and access authorization when classified or other privileged information is requested.

2. Communicate directly with personnel of other University components on matters related to reference (b) and this Directive. To the extent practicable, and consistent with the responsibilities and functions of the University departments, the head of the department concerned shall be kept informed of such direct communications.

3. Request assistance, having executed prior coordination with the Office of the University President, from other investigative, evaluation, response, or inspection units of the DoD

components as needed. In such cases, and when appropriate, assistance shall be requested in coordination with head of the component concerned.

4. Request information or assistance from any Federal, state, or local governmental agency, or unit thereof.

5. Obtain sworn statements from individuals on matters that the USU Privacy Officer considers appropriate for investigation and or breach mitigation, pursuant to references (a), (b), (c), and (d) with due regard for the rights and witness protections established by law.

I. Effective Date.

This Instruction is effective immediately.

Richard W. Thomas, MD, DDS, FACS
President

Enclosures:

1. References
2. Privacy Incident Response Plan (PIRP)

REFERENCES

(a) Privacy Act of 1974, as amended, Pub. L. No. 93-579, 88 Stat. 1896.

(b) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014.

(c) DoD Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

(d) OMB 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information".

(e) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015.

(f) DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use within DoD," August 1, 2012.

(g) Paperwork Reduction Act of 1995, Pub. L. No. 96-511, 94 Stat. 2812.

(h) Uniform Code of Military Justice, 64 Stat. 109, 10 U.S.C. Chapter 47.

(i) DoD Instruction 5105.45, "Uniformed Services University of the Health Sciences," December 26, 2013.

(j) E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899.

(k) DoD Regulation 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003.

(l) Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

Uniformed Services University of the Health Sciences

Privacy Incident Response Plan

INTRODUCTION

BACKGROUND

In September 2006, Office of Management and Budget (OMB) issued a Memorandum for the Heads of Departments and Agencies entitled "Recommendations for Identity Theft Related Data Breach Notification." In February 2007, DOJ issued the U.S. Department of Justice Incident Response Procedures for Data Breaches Involving Personally Identifiable Information implementing the recommendations in OMB's Memorandum. In May 2007, OMB issued Memorandum 07-16 entitled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which requires agencies to develop and implement a notification policy for breaches of personally identifiable information (PII), including the establishment of an agency response team.

PURPOSE

This policy is established to clarify roles and responsibilities in the event of a privacy incident. A swift and complete response to any incidents is necessary in order to protect public and private information. This document and governance structure provides the oversight of and guidance for the required processes for the Uniformed Services University of the Health Sciences' privacy and data security breach response in compliance with federal privacy laws.

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 authority (defined below), or their designee, to determine when to convene the Privacy Incident Response Team (PIRT), however, it will generally be necessary for all "significant" or "high-visibility" incidents (described below). If the PIRT is convened, this plan document must be consulted, and the elements appropriate to the individual incident must be used.

MAINTENANCE

The USU Privacy Office is responsible for the maintenance and revision of this document.

AUTHORITY

The USU Privacy Office is charged with executing this plan in accordance with Federal policies such as the Privacy Act of 1974; DoD 5400.11-R, Department of Defense Privacy Program; DoD 6025.18-R, the Health Insurance Portability and Accountability Act (HIPAA); DoD Health Information Security Regulation; and DoD 5200.01, DoD Information Security Program.

ROLES AND RESPONSIBILITIES

This section is intended to describe the chain of command required to respond to privacy incidents. Responding to significant incidents may require several individuals and subject matter experts in order to properly resolve and contain.

LEAD AUTHORITY

The designated lead authority shall be the USU Privacy Officer or designee, responsible for the oversight of the investigation and the determination of notification for breaches of personally-identifiable information (PIP).

The USU Privacy Officer, or their designee, will determine whether to convene the Privacy Incident Response Team (PIRT), and will serve as, or appoint, the PIRT Coordinator.

PRIVACY INCIDENT RESPONSE TEAM (PIRT)

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

- PIRT Coordinator
- USU Privacy Officer (may also serve as PIRT Coordinator)
- Information Systems Security Officer (for electronic breaches; may also serve as PIRT Coordinator)
- Information Systems Security Manager
- Office of General Counsel
- Department leadership of affected department (Dean, Chair, etc.) or their designee
- Assistant Vice President, Accreditation and Organizational Assessment

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

- Various OCIO Departments depending on the SME requirement, e.g. Network Operations and Communications (NOC), Academic Support & Operations (ASO), Registrar's Office, and/or Customer Service (CSD)
- Office of External Affairs (for media engagement and breaches involving outside parties)
- The Henry Jackson Foundation, Infused Solutions, or other contracting agencies (for breaches involving contracted USU employees, students, or equipment)
- Office of the Inspector General
- Civilian Human Resources
- Law enforcement, including FBI, as appropriate
- Other executives, as appropriate

WORKFORCE RESPONSIBILITIES

Every member of the faculty, staff, and students at USU has the responsibility to immediately report suspected or known breaches of the privacy or security of restricted information. Reports may be made to a supervisor, the IT Help Desk, departmental management, Cyber Security (infosec@usuhs.edu), or directly to the USU Privacy Office. All incidents or suspected incidents should be reported to the USU Privacy Office as soon as they are discovered. Criminal acts, such as thefts, or suspected criminal acts, should also be reported to base police.

RESPONSIBILITIES FOR INCIDENT RESPONSE

a. Upon initial determination of a possible breach, departmental leadership shall notify the USU Privacy Office immediately, who will serve as or appoint the PIRT Coordinator.

b. The PIRT Coordinator is responsible for the execution of this plan that are applicable to the specific incident, and may deviate from this plan, after consultation with the PIRT, to the extent necessary to respond to the incident.
c. As one of their first actions, the PIRT Coordinator shall consult with the Office of General 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. The PIRT 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.
e. For electronic incidents, the designated IT resources shall conduct the initial forensic investigation, and liaise continuously with the PIRT.
f. The PIRT 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. USU and DoD 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.
g. The PIRT is responsible to ensure that, if necessary, evidence is preserved, and each incident is adequately documented. The rationale to notify or not to notify must be clearly documented. Further information on Incident Documentation is below.

REPORTING RESPONSIBILITIES

The following outlines the steps that need to be taken for any confirmed or suspected privacy incident. Following an incident, the following reporting chain will be set in motion:

1. Incident detection.
2. The USU community is responsible for reporting any incidents or suspected incidents to the USU Privacy Office as soon as the incident is detected.
3. In cases of electronic incidents, the USU Privacy Office must notify the United States Computer Emergency Response Team (US CERT) within one hour using the Incident Reporting System.
4. The USU Privacy Office will then notify the Office of the Secretary of Defense and Joint Staff (OSD/JS) Privacy Office within 24 hours using DD Form 2959. See DoD 5400.11-R for detailed instructions.
5. The OSD/JS Privacy Office, in coordination with the USU Privacy Office, will submit the DD 2959 to the Defense Privacy and Civil Liberties Division within 48 hours

Figure 1. Reporting chain and timeline.

Incident reports should use appropriate reporting forms, identified above, and must include as much information as known at the time of the report. The PIRT Coordinator or designee is responsible for updating the form as additional information becomes available.

In addition to this reporting chain, the USU Privacy Office must keep USU senior leadership informed of all incidents.

TRIAGE AND SCOPING

The triage and scoping phase involves the process of analyzing the information to determine whether or not a security incident has occurred. 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?

Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm USU or the Federal Government. Events occur routinely and will be examined for impact. Those showing either harm or intent to harm may be escalated to an incident.

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

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

Incidents can result from any of the following:

- intentional and unintentional acts
- actions of USU employees
- actions of vendors or constituents
- actions of third parties
- external or internal acts
- credit card fraud
- potential violations of USU or DoD policies
- natural disasters and power failures
- acts related to violence, warfare or terrorism
- serious wrongdoing, or
- other

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; computer theft; unsecured physical files containing confidential information; loss of control of physical files; or any other failure to adhere to Federal policy and regulations.

CHARACTERISTICS OF "SIGNIFICANT" OR "HIGH VISIBILITY" INCIDENTS

The PIRT will 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 notable individuals or "VIPs"
- Incidents involving key USU personnel such as university leadership, system leadership, Regents, prominent faculty or alumnae, 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., VIPs)
- 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 USU of which senior leadership should be aware

INCIDENT REPORTING

All suspected or confirmed privacy or data security incidents must be reported in accordance with DoD and OSD/JS Privacy Office policy. The PIRT coordinator that responds to an incident will initially classify the incident severity based on their perception. The initial severity level may be escalated or de-escalated by the Information collected during the investigation. 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.

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 (including PII categories, types and number of individuals affected, etc.)
- actions they have taken since incident discovery
- their contact information
- any additional relevant information known at the time.

See the US-CERT Incident Reporting Form and DD2959 for additional elements which need to be collected when reports are filed.

INCIDENT CLASSIFICATION

Potential impact on organizations and individuals Federal Information Processing Standards Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest.

The potential impact is **LOW** if – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. (Note: Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.)

> AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is **MODERATE** if – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

> AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is **HIGH** if – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

> AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1. Potential impacts of incidents.

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 organizations and personnel who may be involved in incident response. Containment may involve a combination of physical, technical, and administrative controls. This may include 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 USU General Counsel 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 a PIRT 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 data processing 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 and requirements of DoD 5400.11-R.

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 PIRT should consider bringing in a third party, such as an external organization to assist in the triage and scoping effort.

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

If it is suspected that other parts of the University are vulnerable to a similar attack, the PIRT Coordinator should send an alert. If it is suspected that other systems are vulnerable to a similar privacy breach, the PIRT Coordinator should notify the Information Systems Security Officer or Information Systems Security Manager.

EXECUTION

PREPARATION

The PIRT should collect and/or review the incident documentation and event reports. This information should first be verified as being factual (information may have been misreported, or incorrectly documented). The PIRT should assign the incident impact determination, or re-consider its appropriateness if already assigned. The PIRT should determine who, outside of the PIRT, needs to be notified of the incident, both internal and external to the affected department 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 mission 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 report, and signing every page of the report. Document each individual's time spent on the incident, and any other incident response costs/resources.

Refer to Exhibit B: Incident Response Check List.

CONTAINMENT

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

The PIRT must assess whether to disrupt services to internal or external stakeholders. Decisions of this nature must be made in consultation with the appropriate senior leadership and an evaluation of whether the systems impact critical functions to complete the University mission.

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 and when. Pay particular attention to any actions taken to respond, contain, or prevent reoccurrence.

ASSESS THE CAUSE AND TYPE OF BREACH

Depending on the documentation provided to the PIRT, 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, affected individuals (type and number), whether the data was electronic or not, encrypted (and the method / strength of encryption), adequacy of password/physical security, and the type of incident. It is particularly important to validate information provided to the PIRT, 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 system (computer hardware, file storage area, etc.) to the incident under investigation.
- Develop and record a 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.
- The PIRT must perform an analysis to determine whether individuals and/or other agencies need to be notified of the breach, and ensure that regulatory deadlines for such notification are met.

ASSESSMENT OF INCIDENTS INVOLVING PHI (HIPAA)

Refer to DoDI 6025.18-R – DoD Health Information Privacy Regular. The PIRT must perform and document a risk assessment to determine whether there is a significant risk of harm to the individual whose PHI 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 the US-CERT Incident Report (in cases of electronic incidents; within one hour of incident detection) and DD 2959 to the OSD/JS Privacy Office (for all incidents within 24 hours), ensuring that the following information is included:

- High-level description of the incident and its scope
- Actions taken to in response to the beach (to include actions taken to prevent recurrence and lessons learned)
- Impact on the organization and affected individuals
- PII involved in the breach and type of media or equipment involved
- Recommendations for further action/containment

When accurate information is available, be sure to update reports with:

- 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 information.
- Develop a Call Center (for significant incidents): 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, coordinate 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 (coordinate with External Affairs).
- If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted

- population by whatever means the Component believes is most likely to reach the affected individuals.
- 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. Email is acceptable when notifications are urgent or if it is the only means of contact available.
- Refer to Exhibit C: DoD 5400.11-R sample 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., OSD/JS), 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 OGC to identify possible legal issues that may need clarification; develop responses.
- Notification Launch & Coordination: 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

According to DoD 5400.11-R:

The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained. The 10-day period begins after the Component is able to determine the identities of the individuals whose records were lost. If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

REMEDIATION AND POST-INCIDENT REVIEW

RESPONSIBILITIES

The PIRT Coordinator initiates and coordinates remediation and post-incident activities as soon as basic risk mitigation activities have been taken to stabilize the environment. The PIRT Coordinator keeps the

senior leadership 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 PIRT Coordinator convenes one or more Remediation and Post-Privacy Incident Review Teams (PPIRTs).

- The PIRT Coordinator and PPIRTs document findings and activities continuously throughout the review.
- Scopes of various PPIRTs 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 PIRT Coordinator may be a participating member of PPIRTs or may delegate the work to other individuals. In any case, the PIRT Coordinator maintains continuous, close communications with PPIRTs, and over-all control of remediation and post incident review activities.
- PPIRTs 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 PIRT Coordinator and PPIRTs 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/medical center/DoD.
- The PIRT Coordinator and PPIRTs prepare an action plan for recommended changes to improve the local environment going forward.
- PPIRTs 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) or removed altogether.
- 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/medical center/DoD, 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/medical center/lab/DoD.
- Share lessons learned with appropriate contacts, including the OSD/JS Privacy Office (via DD2959).

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 PIRT 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 PIRT Coordinator assesses findings and recommendations of the PIRT(s), and then issues a report of the incident and its response to the University leadership, 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 PIRT 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;
        - hardware, software
        - operational procedures
        - 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 University leadership, works with the CIO and other stakeholders to convene appropriate team(s) to start remediation activities throughout the campus/lab/medical center/DoD environment.
- Prepare detailed action plans and/or project descriptions to improve the technical environment both locally and throughout the campus/lab/medical center/DoD.
- Identify any areas where policy, guideline, or organizational structure changes would have improved results; then work with responsible University authorities 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/sufficient. 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.

CONTACTING THE USU PRIVACY OFFICE

If you have additional questions or concerns about the Privacy Incident Response Plan, or other Privacy-related matters, the USU Privacy Office can be contacted through the department of Accreditation & Organizational Assessment.

- Phone: 301-295-1054
- Web: https://www.usuhs.edu/oac/
- Additional Privacy Info: https://www.usuhs.edu/oac/privacyact

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	Email servers Router & firewall logs Individual workstations Backups
Internal Employee or Contractor Activity	System logs Mail server logs User logs Proxy logs Router & firewall logs Individual workstations Electronic devices (cell phone, tablet, electronic organizer) Removable media Paper files or copies

PRESERVATION OF EVIDENCE

Consult with USU OCIO 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 PIRT Coordinator.

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 USU mission operations. The decision should be made in consultation with the PIRT.

Protect perishable data both physically and electronically, such as data found on pagers, caller ID, cell phones, smart phones, tablets 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. The OCIO may determine that the disk image should be investigated by Defense Information System Agency (DISA) to complete forensic media analysis.

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 CHECKLIST

Privacy Incident Response Checklist			
Date of Incident:			
Date Detected:			
Date of Last Update:			
Step	Task	Resources (Dept or POC)	Completion Date
1	**Identify Affected Individuals / File Initial Reports / Initiate Remediation**		
1.1	Conduct Forensic Analysis to Identify Victims' Names, Addresses, Email Addresses and Types of Data Stolen.		
1.2	1.2.1 File Report with initial data to the US CERT within 1 hour of discovery for all electronic breaches. Update as necessary.		
	1.2.2 File initial DD2959 with the OSD/JS Privacy Office within 24 hours of discovery for all breach types. Update as necessary.		
	1.2.3 File report with law enforcement or FBI, as appropriate. Update as necessary.		
1.3	Determine appropriate PIRT membership based on breach type and scope.		
1.4	Contain data spill and impose preventative measures for additional data compromise.		
1.5	Perform additional remediation and log all actions taken in response to the breach.		
2	**Establish Communication & Notification Plan**		
2.1	Establish a list of all affected individuals and prepare appropriate notification procedures.		
2.2	2.2.1 Communicate scope and impact of the incident to senior USU leadership.		
	2.2.2 Determine appropriate notification procedure and establish a call center and/or credit monitoring services, if necessary.		
2.3	2.3.1 Execute notification procedure within 10 days of identifying affected individuals (send email, mail, and/or phone notification)		
	2.3.2 Track individuals who are successfully notified and individuals with invalid or incomplete contact information.		
	2.3.3 Consider setting up a University website to alert individuals who are not able to be contacted directly.		
2.4	Utilizing the External Affairs office, determine appropriate press releases or other media relations, if necessary.		

3	**Conduct Review of Response and Document Lessons Learned**		
3.1	Establish the PPIRT to determine the completeness and effectiveness of the incident response.		
3.2	Determine preventative approach in case of next incident.		
3.3	Determine lessons learned and document all findings.		
3.4	Submit after action report DD2959 to OSD/JS Privacy Office and brief USU Leadership, as necessary.		

EXHIBIT C: SAMPLE NOTIFICATION LETTER

Excerpt from DoD 5400.11-R:

SAMPLE NOTIFICATION LETTER

Dear Mr. John Miller:

On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/idtheft/con_steps.htm. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,

Signature Block (Directorate level or higher)