PAT-607 HIPAA PRIVACY AND SECURITY RULE: MITIGATION AND SANCTIONS

I. Policy

A. It is USC's[1] policy to:

1. Monitor compliance with HIPAA policies and to mitigate, to the extent practicable, any harm resulting from inappropriate access to, acquisition of, use of, or disclosure of protected health information.

2. Permit individuals to report privacy complaints and issues.

3. Impose sanctions, as applicable and pursuant to USC policies, for violations of USC's privacy policies.

II. Procedures

A. Reporting To USC Office of Compliance

Information regarding any violation of USC's HIPAA privacy policies, including any unauthorized access to, acquisition of, use of, or disclosure of protected health information or violation of a patient's rights with respect to his/her Protected Health Information[2] discovered by any employee of USC must be reported as soon as possible to the USC Office of Compliance.

B. Monitoring Plan.

The USC Office of Compliance is responsible for monitoring compliance with USC's HIPAA policies and shall develop a monitoring plan to test appropriate use and disclosure of Protected Health Information according to USC policies.

C. Mitigation Plan.

---

[1] For purposes of the HIPAA Privacy Rule, USC includes those entities that comprise Keck Medicine of USC, including but not limited to, USC Norris Cancer Hospital, Keck Hospital of USC, USC's employed physicians, nurses and other clinical personnel, those units of USC that provide clinical services within the Keck School of Medicine, School of Pharmacy, the Herman Ostrow School of Dentistry, Physical and Occupational Therapy, Suzanne Dworak-Peck School of Social Work, as well as USC Care Medical Group, affiliated medical foundations of Keck and their physicians, nurses and clinical personnel, Engemann Student Health Center, Eric Cohen Student Health Center, USC Verdugo Hills Hospital, its nurses and other clinical personnel, Verdugo Radiology Medical Group, Verdugo Hills Anesthesia, and Chandnish K. Ahluwalia, M.D., Inc. and those units that support clinical and clinical research functions, including the Offices of the General Counsel, Audit and Compliance.

[2] Protected Health Information is defined as identifiable information that relates to the individual's past, present or future physical or mental health condition or to payment for health care.

The USC Office of Compliance, in response to any report of or information about an unauthorized access, acquisition, use or disclosure by a member of USC's Workforce or any of its Business Associates, or any other security incident or breach, shall investigate the incident, and develop and implement a plan as soon as reasonably practicable to mitigate any known or reasonably anticipated harmful effects from such disclosure (the "mitigation plan").

The mitigation plan shall be documented and tailored to the circumstances of each case, but shall include as appropriate, the following elements:

1. Identifying source(s) of the unauthorized access, acquisition, use, or disclosure and taking appropriate corrective action, which may include instituting immediate action to ensure that vulnerable systems are secured.

2. Evaluating the type and amount of damage that occurred; the type and amount of PHI that was acquired, accessed, used or disclosed; the reasons for the acquisition, access, use or disclosure; and what steps can be taken to ensure the type of incident does not occur again.

3. With respect to unauthorized access to, acquisition of, use of, or disclosure of PHI by a member of USC's Workforce, following the Sanction's process outlined below as applicable.

4. With respect to unauthorized disclosures of PHI, contacting the recipient of the information that was subject of the unauthorized disclosure and requesting that such recipient either destroy or return the information or take some other appropriate action to mitigate further use or disclosure.

5. Depending on the circumstances, notifying the patients whose Protected Health Information was the subject of the unauthorized access, acquisition, use, or disclosure, suggesting the affected patients monitor their health information records for signs of misfeasance, and potentially providing credit monitoring where a social security number was involved.

6. Depending on the circumstances, notifying the appropriate state and/or federal agency.

D. Sanctions.

The USC Office of Compliance is charged with implementing and enforcing USC HIPAA policies. USC faculty, staff, students and other employees who breach the privacy or security of Protected Health Information or otherwise violate USC's HIPAA policies will be disciplined as set forth in the Sanctions Guidance in Exhibit A and in accordance with USC's Cooperation with Compliance Investigations policy at http://policy.usc.edu/cooperation-with-compliance-investigations/.

The USC Office of Compliance will document sanctions that are applied pursuant to this Policy and maintain such documentation for a period of six (6) years, or longer if required by state law. Such documentation shall include: (a) the name of the USC Workforce member; (b) a description of the sanctioned activity, (c) the date of the sanctioned activity; and (d) a description of the authorized sanction. A copy of the document may be provided to USC Human Resources to place in the USC Workforce member's personnel file. Violations of USC's HIPAA policies also may be taken into account in such individual's performance evaluation.

Additional References

45 CFR § 164.308(a)
45 CFR § 164.530(e)

45 CFR § 164.530(f)

Responsible Office: Office of Compliance
http://ooc.usc.edu/
compliance@usc.edu
(213) 740-8258

Appendix A

USC Office of Compliance Guidance for HIPAA Sanctions

The USC HIPAA Policies[3]classified faculty, staff, employees, students, volunteers and trainees as "covered workforce". Pursuant to USC HIPAA Policies, all covered workforce members must complete HIPAA training and are accountable for complying with federal and state health information privacy regulations.

The following provides guidance as to how privacy and security violations will be managed at USC:

1. **Review each circumstance of inappropriate access to, acquisition of, use of, and/or disclosure of PHI uniquely and consistently apply corrective disciplinary action.** The following considerations may be made when determining the appropriate disciplinary action:

    a. What was the intent of the inappropriate access, acquisition, use, and/or disclosure?
        1. Unintentional.
        2. Unintentional resulting in a reportable breach.
        3. Intentional.
    b. What is the potential organizational risk associated with the inappropriate access, acquisition, use, and/or disclosure?
        1. Potential for patient harm.
        2. Potential for organizational harm.
        3. Potential for external/public exposure versus confined internal exposure.
    c. What is the history of the workforce member's work performance?
        1. Has the member been disciplined for previous patient privacy concerns?
        2. Has the member been subject to a series of progressive disciplinary actions, related or unrelated to patient privacy concerns?
    d. What is the history of the organization's disciplinary actions for like occurrences?
    e. Are there mitigating circumstances that include conditions that would support reducing the disciplinary/corrective action in the interest of fairness and objectivity?

2. **Follow the corrective disciplinary action tree recommendations.** Inappropriate access, acquisition, use, and/or disclosures of PHI may be divided into the following three levels with recommended corresponding disciplinary

[3] See USC GEN-101: *Education of Covered Workforce* and USC PAT-607: *Mitigation and Sanctions Policy*

action for each. If the workforce member has a history of previous corrective disciplinary actions, then the subsequent disciplinary action should be applied in a progressive manner.

Level of Infraction	Description	Infraction examples	Range of Discipline Recommended
1 – Unintentional Resulting in no reportable breach	Occurs when member unintentionally accesses, reviews or reveals PHI to him/herself or others without a legitimate need to know or beyond the minimum necessary level of access assigned to his/her role, but the PHI stays within the covered workforce.	Typing in the wrong MRN or patient name and viewing wrong patient's information. Not properly safeguarding or securing PHI (e.g., leaving PHI face up for other clinic personnel to see) within the clinic/department. Leaving a computer station open without logging out for an extended period of time.	Verbal Reminder and/or additional HIPAA Education.
2 – Unintentional, Resulting in reportable breach	Occurs when member unintentionally accesses, reviews or reveals PHI to him/herself or others without a legitimate need to know or beyond the minimum necessary level of access assigned to his/her role and such action results in a reportable breach, where the PHI is shared outside of USC and/or covered workforce.	Mailing/faxing errors – sending another patient's documentation to another person/entity resulting in a breach. Inappropriately accessing or disclosing patient's medical information (minimum necessary rule not followed, email sensitive information, access to sensitive information outside of role). Password compromised by sharing it and patient medical information was accessed.	Varies depending on circumstances: Written reprimand, final warning or unpaid leave. Severe and multiple infractions that lead to breaches may result in termination pursuant to applicable USC policies.

		EMR left open and patient medical information was accessed.	
3 - Intentional	Occurs when member deliberately accesses, shares, or releases PHI for (i) personal gain, (ii) with malicious intent, (iii) out of curiosity, (iv) or for any other reason not required for his/her job function and not authorized or permitted under USC HIPAA policies or privacy laws.	Accessing medical records or disclosing PHI of family, friends, prominent patients, or colleagues. Unauthorized and intentional disclosure of patient information to a 3rd party. Intentionally sharing or disclosing patient information or the patient's presence in the hospital without that person's need to know or for a specific treatment, payment, or healthcare operation requirement. General curiosity about a patient and accessing their medical record to determine or view their demographics or why they need medical care.	**FOR STAFF:** This behavior constitutes serious misconduct and will result in immediate termination. **FOR FACULTY:** This behavior constitutes serious misconduct that relates directly and substantially to the fitness of a faculty member in his or her professional capacity, as provided in the Faculty Handbook, and disciplinary measures will be taken in accordance with the Faculty Handbook, up to and including dismissal for cause.