

PAT-607 MITIGATION AND SANCTIONS

I. Policy

A. It is USC's¹ policy to:

1. Monitor compliance with HIPAA policies and to mitigate, to the extent practicable, any harm resulting from inappropriate use 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 use or disclosure or violation of a patient's rights with respect to his/her Protected Health Information² 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 privacy policies and shall develop a monitoring plan to test appropriate use and disclosure of PHI according to USC policies.

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 as well as USC Care Medical Group, affiliated medical foundations of Keck and their physicians, nurses and clinical personnel, 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.

Issued by:	Michael Quick Provost and Senior Vice President, Academic Affairs	Todd R. Dickey Senior Vice President, Administration
Date issued:	July 1, 2016 University of Southern California Page 1 of 6	

C. Mitigation Plan.

The USC Office of Compliance, in response to any report of or information about an unauthorized use or disclosure by a member of USC's workforce or any of its Business Associates, shall 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 tailored to the circumstances of each case, but shall include as appropriate, the following elements:

1. Identifying source(s) of the unauthorized use or disclosure and taking appropriate corrective action.
2. With respect to unauthorized uses of PHI by a member of USC's Workforce, following the Sanction's process outlined below as applicable.
3. 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.
4. Depending on the circumstances, notifying the patient whose Protected Health Information was the subject of the unauthorized use or disclosure.
5. 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 of Protected Health Information or otherwise violate USC's HIPAA privacy 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/>. 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)

Issued by:	Michael Quick Provost and Senior Vice President, Academic Affairs	Todd R. Dickey Senior Vice President, Administration
Date issued:	July 1, 2016 University of Southern California Page 2 of 6	

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

Issued by:	Michael Quick Provost and Senior Vice President, Academic Affairs	Todd R. Dickey Senior Vice President, Administration
Date issued:	July 1, 2016 University of Southern California Page 3 of 6	

Appendix A

USC Office of Compliance Guidance for HIPAA Sanctions

The USC HIPAA Privacy Policies³ classified faculty, staff, employees, students, volunteers and trainees as “covered workforce”. Pursuant to USC Privacy 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 violations will be managed at USC:

1. **Review each circumstance of inappropriate use and/or disclosure 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 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 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?

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

Issued by:	Michael Quick Provost and Senior Vice President, Academic Affairs	Todd R. Dickey Senior Vice President, Administration
Date issued:	July 1, 2016 University of Southern California Page 4 of 6	

2. **Follow the corrective disciplinary action tree recommendations.**

Inappropriate use and/or disclosures of PHI may be divided into the following three levels with recommended corresponding disciplinary 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
<p>1 – Unintentional Resulting in no reportable breach</p>	<p>Occurs when member unintentionally or carelessly access, 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.</p>	<p>Discussion of PHI in public area (cafeterias, elevators of hospital campus). Typing in wrong MR# or Patient Name and viewing wrong patient’s information. Leaving PHI accessible within HSC public area (e.g., unattended computer, medical records/surgery schedules in meeting rooms, etc.)</p>	<p>Verbal Reminder and/or additional HIPAA Education.</p>
<p>2 – Unintentional, Resulting in reportable breach</p>	<p>Occurs when member unintentionally or carelessly access, 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.</p>	<p>Mailing/faxing errors – sending another patient’s documentation to another person/entity resulting in a breach. Inappropriately accessing/disclosing patient’s medical information (minimum necessary rule not followed, email sensitive information, access to</p>	<p>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</p>

<p>Issued by: Michael Quick Provost and Senior Vice President, Academic Affairs</p>	<p>Todd R. Dickey Senior Vice President, Administration</p>
<p>Date issued: July 1, 2016 University of Southern California Page 5 of 6</p>	

University of Southern California POLICY
Administrative and Business Practices / HIPAA

		<p>sensitive information outside of role).</p> <p>Password compromised by sharing it and patient medical information was accessed.</p> <p>EMR left open and patient medical information was accessed.</p>	<p>applicable USC policies.</p>
<p>3 - Intentional</p>	<p>Occurs when member accesses, reviews, or discusses PHI for personal gain or with malicious intent. Willful and gross negligent use and/or disclosure of PHI, destruction of PHI, or knowingly violating state or federal laws protecting privacy and security of PHI.</p>	<p>Inappropriately accessing medical records of family, friends, or prominent people.</p> <p>Unauthorized and intentional disclosure of patient information to a 3rd party.</p>	<p>Varies depending on circumstances: Written reprimand, final warning or unpaid leave.</p> <p>Severe and multiple infractions that lead to breaches may result in termination pursuant to applicable USC policies.</p>

<p>Issued by: Michael Quick Provost and Senior Vice President, Academic Affairs</p>	<p>Todd R. Dickey Senior Vice President, Administration</p>
<p>Date issued: July 1, 2016 University of Southern California Page 6 of 6</p>	