HIPAA PRIVACY RULE PAT-608: BREACH NOTIFICATION POLICY

I. POLICY:

USC[1] shall comply with breach notification requirements under federal and state laws, including the HIPAA privacy and security regulations and the Health Information Technology for Economic and Clinical Health Act ("HITECH") Regulations. The Office of Compliance shall investigate potential breaches of Protected Health Information[2] ("PHI"), determine whether notification is required and manage the notification and post-investigation process, as applicable.

II. PROCEDURE:

A. Discovery and Internal Reporting of Potential Breach

1. All USC employees, including faculty and staff, students, trainees and volunteers ("USC Workforce") must immediately notify their supervisor and the Office of Compliance of any suspected breach of patient privacy through the unauthorized acquisition, access, use or disclosure of PHI ("unauthorized activity").

2. A breach is, generally, an impermissible use or disclosure that compromises the security or privacy of PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. *See* HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

3. Unauthorized activities are described in USC's HIPAA Policies and include, but are not limited to, the following activities:

---

[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.

a. Accessing the medical record of a co-worker, colleague, friend, family member, or celebrity without authorization;

b. Sending faxes, emails or regular mail containing PHI to an unauthorized recipient;

c. Disclosing to friends, family, or reporters information about patients without authorization;

d. Posting PHI on public websites;

e. Discarding electronic devices without first securely wiping any PHI;

f. Leaving documents containing PHI in public locations; and

g. Collecting PHI for research use without the required approvals and consent.

4. A USC supervisor or manager who is informed of any unauthorized activity shall immediately report the activity to the Office of Compliance.

B. Investigation of Potential Breach

1. The Office of Compliance shall determine whether a breach has occurred and shall be responsible for the management of the breach investigation, including conducting interviews, risk assessments, and coordinating with other USC departments as appropriate (e.g., Information Security, Human Resources, Risk Management, and the Office of General Counsel).

2. In assessing a potential breach, the Office of Compliance shall:

a. Determine whether the potential breach fits within one of the following exceptions to the definition of a breach:

(1) The unauthorized activity involved the unintentional acquisition, access, or use of PHI by a USC employee or other individual acting under the authority of USC;

(2) The unauthorized activity involved the inadvertent disclosure of PHI from an authorized employee or authorized individual within USC to another authorized employee or authorized individual within USC; or

(3) The unauthorized activity involved unauthorized disclosures in which an unauthorized person to whom PHI was disclosed would not have been able to retain the information. *See* 45 CFR §§ 164.402.

b. Determine whether individual, governmental or other notice is required under federal or state law and oversee the provision of such notice

c. If a determination is made that the unauthorized activity does not constitute a breach, a risk analysis outlining such conclusion shall be documented as a record of the completed investigation.

C. Notification

1. The Office of Compliance shall facilitate all breach notification processes to the appropriate entities (e.g., the United States Department of Health and Human Services ("HHS"), the California Department of Public Health ("CDPH"), an individual patient, or the media). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years. *See* 45 CFR §164.530(j)(2).

2. If the Office of Compliance determines that unauthorized activity constitutes a breach, notification shall be made in accordance with the following:

a. Patient Notification

(1) Timing. A breach notification of PHI from hospital-licensed facilities requires notification within 15 days of the discovery[3] of the breach. Breach notification of PHI from non-hospital licensed facilities requires notification within 60 days of the discovery of the breach.

(2) Method. Notice to individuals shall be provided in writing by first-class mail or by email if the individual has indicated a preference to receive email communications. For individuals who are deceased or for whom USC has insufficient contact information, U.S. federal regulation 45 C.F.R. 164.404(d) shall be followed.

(3) Content. Notice to individuals shall contain:

[3] A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to USC, or, by exercising reasonable diligence would have been known to USC (including breaches by USC's business associates).

(a) Approximate date of occurrence;

(b) General information of how/why disclosure occurred;

(c) Type of information disclosed, including whether a social security number or other financial information was disclosed;

(d) Remediation/corrective action; and

(e) Contact information for any questions.

b. Government Notification

(1) Federal: If a breach involves the PHI of 500 or more individuals, notification must be made to HHS. Such notification shall be made at the same time individual notification is provided. If a breach involves the PHI of less than 500 individuals, the breach must be logged or otherwise documented and notification must be made to HHS not later than 60 days after the end of the calendar year. Notifications to HHS shall be made in the manner specified on the HHS web site.

If a breach involves the PHI of 500 or more California residents as a result of a single breach of the security system, notification must be made to the California Attorney General.

(2) CDPH: A breach arising from hospital-licensed facilities requires notification to CDPH within 15 days of the discovery of the breach. The content of such communication shall be the same as that provided in the individual's notifications.[4]

c. Media Notification

(1) If a breach involves the PHI of more than 500 residents of a state, notification must be made to a prominent media outlet without unreasonable delay and in no event later than 60 days of discovery of the breach. Breaches involving Business Associates

3. Breaches Involving Business Associates

a. In the event that USC is notified of unauthorized activity by a USC HIPAA Business Associate, USC will investigate and assess the potential breach in accordance with the procedures outlined above.

[4] For breaches involving health data and other sensitive information protected under state law, refer to Civil Code Section 1798.82 for breach notifications.

b. The Office of Compliance will coordinate with the Business Associate to ensure that USC receives all relevant and necessary information and documentation, and in accordance with the terms of the applicable Business Associate Agreement. Breaches are determined to be discovered as of the date that the Business Associate notified USC of the unauthorized activity.

c. In the event of unauthorized activity regarding PHI maintained, used, accessed or disclosed in USC's capacity as a HIPAA Business Associate, the Office of Compliance will notify the relevant USC Covered Entity in a manner consistent with the terms of the applicable Business Associate Agreement.

D. Accounting of Disclosures

1. The breach must be logged such that if an affected patient or patient representative requests an accounting of disclosures at any future date, USC is able to disclose the breach on the accounting.

2. The Office of Compliance shall determine whether unauthorized activity is subject to inclusion in disclosures which must be tracked in order to comply with HIPAA accountings of disclosures requirements.

E. Post-Investigation Follow-Up and Closing

1. The Office of Compliance will work with the Office of General Counsel, Information Security, Human Resources, Risk Management and/or other department as necessary to mitigate any harmful effects of any breach that are known to USC.

2. The Office of Compliance shall document and track a plan of action, if any, including whether employment corrective action is appropriate. Such action could lead to a letter in the employee's Human Resources file, administrative leave/suspension, or termination, depending on the severity of the violation and past disciplinary action. *See* USC HIPAA Policy PAT-607, Mitigation and Sanctions.

Executed by:

Michael Quick
Provost and Senior Vice President, Academic Affairs

Todd R. Dickey
Senior Vice President, Administration

Date issued: November 30, 2016