Children's Hospital LOS ANGELES Medical Group	POLICY AND PROCEDURES		
	POLICY NUMBER:	CHLAMG-CI-1010	
	ORIGINAL DATE: 11/1/2018	REVISED:	EFFECTIVE:
DEPARTMENT: Compliance	APPROVED BY: Carl Grushkin, MD and Chief Compliance Officer		
POLICY TITLE: **Breach Risk Assessment and Notification**			

PURPOSE: To establish a policy and procedure to describe the steps that must be taken in the event of a Suspected or Actual Breach of Unsecured Protected Health Information ("Breach") and, when appropriate, to report the Breach as required by the Health Information Technology for Economic and Clinical Health ("HITECH") Act and its implementing regulation and as required under California state law.

DEFINITIONS:

1. **Breach or Actual Breach:** An unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of PHI. Examples of a breach may include, but are not limited to:

    - Lost or stolen laptops, desktops, servers, tapes, smartphones and any other mobile data storage medium containing PHI;
    - Lost or stolen paper PHI;
    - Emails or papers containing PHI sent to an unauthorized party;
    - Electronic transmissions of PHI sent outside CHLAMG/CHLA's network in unencrypted format that are accessed without authorization;
    - An intentional violation of physical controls to areas where PHI is kept;
    - Deficient information security controls that allow unauthorized access to PHI;
    - Saving ePHI in a location that grants access to people without a need to know;
    - Notification from a business associate, law enforcement authority, government agency or other source of a confirmed Breach of the computing environment where PHI is stored or processed.

2. **Breach exceptions**:

    a. A good faith unintentional acquisition, access or use of PHI by a CHLAMG/CHLA workforce member or business associate acting within the scope of their duties that is not further used or disclosed, e.g., a staff member accidentally accesses the wrong medical record, realizes the mistake, and closes the record.
    b. An inadvertent disclosure of PHI by one person authorized to access PHI to another person authorized to access PHI at the same entity, business associate or organized health care arrangement if the PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule, e.g., the wrong patient's information is sent to the wrong provider at CHLAMG.
    c. A disclosure of PHI where CHLAMG has a good faith belief the unauthorized recipient did not retain the PHI, e.g., results of lab tests sent to the wrong patient are returned unopened.

3. **Business Associate**: Is a person or entity that performs certain functions or activities that involve the use of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a Business Associate. CHLAMG is required to have a Business Associate Agreement in place with any Business Associate.

4. **Personal information**: Under California state law, personal information means:

    a. An individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data element(s) is not encrypted: Social Security number; driver's license or California identification card number; account number, credit or debit card number, in combination with any security code, access code, or password that would permit access to the individual's financial account; medical information (medical history, mental or physical condition or medical treatment or diagnosis by a health care professional); health insurance information (health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application or claims history, including appeals records); and, information collected through the use of an automated license plate recognition system.
    b. A user name or email address, in combination with a password or security question/answer that would permit access to an online account.

5. **Suspected Breach**: An incident where there is a reasonable likelihood that PHI or PI was inappropriately acquired, accessed, used or disclosed.

6. **Incident Response Team**: The CHLAMG team assembled to work through HIPAA security incidents, including Breaches and Suspected Breaches, and is normally comprised of representatives from Compliance, Information Services, Risk Management, Legal Counsel, and Communications.

7. **Unsecured PHI**: PHI that is not encrypted or destroyed in a manner that makes the PHI or PI unreadable to unauthorized individuals.

SCOPE: This policy covers federal and state breach notification requirements for CHLAMG Suspected and Actual Breaches of PHI or PI.

POLICY:

Children's Hospital Los Angeles Medical Group (CHLAMG) and its Business Associates 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 Compliance Department shall investigate potential breaches of Protected Health Information ("PHI") and Personal Information ("PI"), determine whether notification is required, and manage the notification and post-investigation process. In the event CHLAMG personnel are involved in a Breach or Suspected Breach involving CHLA and its information systems, the CHLAMG Compliance Director and CHLA's Chief Compliance Officer or Privacy Manager will coordinate incident response under CHLA's breach investigation and notification policies.

PROCEDURE:

A. **Discovery and Internal Reporting of Suspected Breach or Breach.** If a CHLAMG workforce member becomes aware of an Actual or Suspected Breach, the workforce member is required within 48 hours to notify their supervisor and the Compliance Department.

    1. If CHLAMG is acting as a business associate, CHLAMG will notify the covered entity of the Suspected or Actual Breach in accordance with the terms of its Business Associate Agreement;

2. If a Business Associate becomes aware of a breach, the Business Associate is required to notify CHLAMG in accordance with the terms of its Business Associate Agreement;

3. If CHLAMG is not acting as a business associate but becomes aware of a Suspected Breach or Breach involving a payor or other business partner with respect to PHI, CHLAMG will timely report the Breach to the payor or business partner in accordance with its contractual terms.

B. Incident Manager

1. The Incident Manager, in conjunction with the CHLAMG division where the Suspected or Actual Breach occurred, will determine required actions. If CHLA is involved in the Suspected or Actual Breach, the Incident Manager will coordinate his/her activities with the designated CHLA Incident Manager.

2. If the Incident Manager deems it necessary, he/she will convene the Incident Response Team to participate in the investigation and mitigation of the Suspected or Actual Breach. This will occur as soon as practicable after the report of the Suspected or Actual Breach.

    a. If a Breach occurred, the division and the Incident Response Team will take appropriate action as described in this policy.
    b. If a Breach did not occur, the Incident Response Team will document how it reached this conclusion.

C. **Determining if a Reportable Breach Occurred.** Upon notice of a suspected breach, the division, in conjunction with the Incident Response Team, will determine if:

1. The Suspected Breach involved unsecured PHI or PII;

2. The Suspected Breach involved an impermissible use or disclosure of PHI under the HIPAA Privacy Rule or of PII under state law; and,

3. Whether any other breach notification laws or expectations for handling the incident apply.

4. If the Suspected Breach did not involve unsecured PHI or an impermissible use or disclosure of PHI under the HIPAA Privacy Rule, or of PII, a Breach under the HITECH Act and state law did not occur and no breach notification is required.

5. If a Suspected Breach did involve unsecured PHI or an impermissible use or disclosure of PHI or PII, the Incident Response Team must determine whether the Suspected Breach meets one of the exceptions under the Definitions above. If it does, no Breach has occurred and no notification is required.

D. **Risk Assessment.** If the Suspected Breach does not fall into an exception, the Incident Response Team will conduct a risk assessment to determine if the Breach compromises the security or privacy of the information. In determining whether there is a low probability of compromise, the risk assessment must consider the following four factors:

1. The nature and extent of the PHI/PII involved, including the identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI/PI or to whom the disclosure was made;

3. Whether the PHI/PII was actually acquired or viewed; and,

4. The extent to which the risk to the PHI/PII has been mitigated.

E. Documentation of Risk Assessment. The CHLAMG Compliance Director or his/her designee shall document the outcome from the risk assessment for inclusion into an appropriate reporting system. This documentation is required even if the risk assessment determines that no notification is required**.**

F. **The Date a Breach is Discovered.** A Breach is "discovered" on the first day the Breach is known to CHLAMG. CHLAMG is deemed to have knowledge of the Breach when any workforce member other than the person committing the Breach, becomes aware of the Breach. For example, if a division head is informed of a Breach on October 15, and does not report the Breach to Compliance until October 20, the Breach is considered discovered on October 15.

G. Actions if a Reportable Breach Has Occurred.

1. **Timing of Notification**. Except for cases in which a law enforcement official requests a delay in notification (see below), the CHLAMG Compliance Director or designee shall provide notification to the affected individual(s) without unreasonable delay and in no case may the initial notification be later than fifteen (15) days after the discovery of the Breach by CHLAMG or by a business associate. If the requirements of the notification letter cannot be met within the 15-day period, the CHLAMG Compliance Director will send an initial notification letter to individual(s) containing as much information as is known at the time, followed by a supplemental letter with the additional information. Unless otherwise directed by law enforcement, the follow-up letter shall not be delayed more than sixty (60) days from the discovery of the breach.

2. **Written Request by Law Enforcement for Delay in Notification**. If a law enforcement official provides CHLAMG with a written statement that a notification described in this policy would (a) impede a criminal investigation or cause damage to national security, and (b) specifies the amount of time for which law enforcement is requesting a suspension of the notice requirement, the CHLAMG Compliance Director/designee shall suspend temporarily the notice for the time specified by the law enforcement official.

    a. If the law enforcement official makes a statement orally, the CHLAMG Compliance Director/designee must document the statement, including the identity of the official making the statement, and suspend temporarily the notice requirement for no longer than thirty (30) days from the date of the oral statement unless a written statement is submitted during that time.

3. **Notification to Individuals**. If, after conducting a risk assessment, the Incident Response Team and the division cannot determine that there is a low probability of compromise to the Unsecured PHI, a letter will be drafted notifying the affected individual(s) of the Breach. The letter will be reviewed, signed and sent by the CHLAMG Compliance Director in the role of the organization's Privacy Officer. This letter will include:

    a. A brief description of what happened, including the division name and address, the date of the breach, and the date of discovery of the breach, if known;
    b. Whether notification is delayed as a result of a law enforcement investigation;
    c. A description of the types of PHI or PII involved in the breach, e.g., full name, Social Security number, date of birth, account number, diagnosis, etc.

d. Any steps the individual should take to protect himself or herself from potential harm from the breach;
e. A brief description of what CHLAMG and the division are doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches;
f. All information necessary to take advantage of an offer, if any, to provide identity theft and mitigation services.
g. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an email address, Web site, or postal address.
h. If a Social Security number, driver's license or California identification card number was breached, the letter will contain the toll-free telephone numbers and addresses of major credit reporting agencies.

4. **Methods of Notifying Individuals**. The CHLAMG Compliance Director/designee, as appropriate, shall:

a. Provide notification in writing by first-class mail to the individual(s) at the last known address. Email may be used if the individual has agreed to electronic notice and has not withdrawn the agreement.
b. If the individual affected by the Breach is a minor or lacks legal capacity due to a physical or mental condition, notice is provided in writing by first-class mail to the parent or personal representative of the individual.
c. If it is known that the individual whose information was Breach is deceased, notice is sent by first-class mail to the next of kin or personal representative of the deceased individual.
d. If it is believed there is a risk of imminent misuse of Unsecured PHI, additional notice will be provided by telephone or other appropriate means.

5. **Substitute Notice**.

1. *Federal Law*. If there is insufficient or out-of-date contact information for fewer than 10 patients, substitute notice may be provided by an alternative form of written notice, by telephone or by other means, e.g., email communication. Alternatively, CHLAMG may post a notice on its website. If there is insufficient or out-of-date contact information for 10 or more patients, the substitute notice must be in the form of a conspicuous posting for 90 days on CHLAMG's website, or conspicuous notice must be placed in major print or broadcast media in the geographic area where the patients affected by the breach likely reside. A toll-free number will be included where the patient can learn whether his or her unsecured PHI was included in the breach.
2. *State Law*. Substitute notice is permitted if the costs of providing notice will exceed $250,000, or if more than 500,000 individuals are affected, or if CHLAMG does not have sufficient contact information. Substitute notice under California state law includes all of the following:
    (1) Email notice if CHLAMG has an email address for the affected individuals;
    (2) Conspicuous posting for at least thirty (30) days of the notice on the CHLAMG website; and,
    (3) Notification to major statewide news media.

6. **Notification to the Media**. If a Breach of Unsecured PHI involves more than 500 residents of a state or jurisdiction, the division and the Incident Response Team will work with Communications to provide notice to prominent media outlets serving the area. The notification must include the same content that is required in the notice to individuals affected by the Breach. Except for cases in which law enforcement officials request a delay in notification, such notice shall be provided to the media without unreasonable delay and in

no case later than sixty (60) calendar days after discovery of the Breach. Notification to the media should be provided at approximately the same time, but not before, notification to the individual.

7. **Notification to the California Attorney General and the Secretary of Health & Human Services of a Breach involving more than 500 Individuals**.

    a. **California Attorney General**. The CHLAMG Compliance Director will electronically submit a sample copy of the notification to individuals without including any PI. Such notices will be provided at approximately the same time as notice is provided to individuals affected by the Breach.

    b. **HHS Secretary**. The CHLAMG Compliance Director/designee will report Breaches involving more than 500 individuals to the HHS Secretary by entering required information into the HHS data portal.

8. **Notification to the Secretary of Health & Human Services of a Breach involving 500 or fewer Individuals**. The CHLAMG Compliance Director/designee will report Breaches involving 500 or fewer individuals to the HHS Secretary by entering the required information into the HHS data portal quarterly. All breaches involving fewer than 500 individuals must be entered no later than 60 days after the beginning of the new calendar year.

9. **Records Retention**. All official documentation pertaining to Breaches and Suspected Breaches must be maintained for a period of seven (7) years from the date of discovery of a Breach or Suspected Breach.

10. **Notification from a Business Associate**. Business Associates are required to report Suspected or Actual Breaches to CHLAMG in accordance with the terms of the Business Associate Agreement and no later than five (5) days from the date of discovery of the breach by the Business Associate. If a CHLAMG workforce member is notified of a breach by a Business Associate, the workforce member should notify CHLAMG Compliance immediately or call the CHLAMG Compliance Line at 877.658.8022.

    a. Content of Business Associate Notification. The report of a Suspected or Actual Breach from a business associate to CHLAMG shall include, to the extent possible, the following elements:

        i. The identification of each individual whose Unsecured PHI has been or is reasonably believed by the business associate to have been accessed, acquired, used or disclosed during the Breach;
        ii. A brief description of what happened, including the date of the Breach, if known, and the date of discovery of the Breach;
        iii. A description of the types of Unsecure PHI that were involved; and,
        iv. A brief description of what the business associate is doing to investigate the Breach, mitigate harm to individuals and to protect against further Breaches.

    b. CHLAMG will coordinate with its Business Associate on any required notifications as a result of a Breach or Suspected Breach.

H. **Administrative Requirements.** CHLAMG must comply with the following administrative requirements:

1. Train existing and new workforce members on any Breach notification policies and procedures. All training must be documented.

2. Provide a process for individuals to make complaints concerning CHLAMG's Breach notification policies and procedures, or any CHLAMG division's compliance with these policies and procedures. All complaints and their disposition must be documented.

3. Have and apply appropriate sanctions against workforce members who fail to comply with the Breach notification policies and procedures. Workforce members who have knowledge of a Suspected Breach and who do not report it will be subject to sanctions.

4. CHLAMG may not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for the exercise of their rights under the HIPAA Privacy Rule and California laws relating to the filing of complaints relating to Breach notification policies and procedures.

REFERENCES:

45 CFR §§ 164
Cal. Civ. Code §§ 56-6.16
Cal. Civ. Code § 1798.82

ATTACHMENTS
Attachment 1: California Notice of Data Breach
Attachment 2: HIPAA Breach Decision Tool and Risk Assessment Documentation

POLICY OWNER:
CHLAMG Compliance Director

Approved by CHLAMG Executive Compliance Committee on December 26, 2018.

Children's Hospital LOS ANGELES Medical Group	DATE:
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing	
What You Can Do	
Other Important Information:	

For More Information	Call [insert telephone number] or go to [Internet Web Site]

ATTACHMENT 1: California Notice of Data Breach

ATTACHMENT 2: HIPAA BREACH DECISION TOOL AND RISK ASSESSMENT DOCUMENTATION

Incident ID#:			
Person Completing Form:			
Date Incident Occurred:		**Date Incident Detected:**	
Brief Summary of Incident and # of Patients Affected:			

1. **Was protected health information (PHI) involved?** (PHI is health information including demographic information that identifies or there is a reasonable basis to believe it can be used to identify the individual. PHI does not include employment records or PHI of a person deceased for more than 50 years.

   ☐ YES, PHI was involved. Continue to Question 2.
   ☐ NO, PHI was not involved. Breach reporting is not required under HIPAA.

   Describe the information that was involved:

2. **Was the PHI unsecured?** ("Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary such as encryption or destruction.

   ☐ YES, the PHI was unsecured. Continue to Question 3.
   ☐ NO, the PHI was secured. Breach reporting is not required under HIPAA.

   Describe the PHI (verbal? Paper? Electronic? How was the PHI secured or protected?

3. **Was there an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule?** (A violation of the "minimum necessary" standard is a violation of the Privacy Rule. However, use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and that occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule.)

   ☐ YES, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. Continue to Question 4.
   ☐ NO, there was no violation of the Privacy Rule. Breach reporting is not required under HIPAA.

   Describe who acquired, accessed, used and/or disclosed the PHI, whether the person was authorized or unauthorized, and how the PHI was acquired, accessed, used or disclosed:

4. **Does an exception apply?** Check any box below that applies:

   ☐ **Exception A**. A breach does not include an unintentional acquisition, access or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate if it:

      a. Was made in good faith; and,
      b. Was within the course and scope of authority; and
      c. Does not result in further use or disclosure in a manner not permitted by the Privacy Rule.

   ☐ **Exception B**. A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

   ☐ **Exception C**. A breach does not include disclosure of PHI where the provider or business associate has a good faith belief that the unauthorized person who received it would not reasonably have been able to retain the information.

      ☐ Yes, an exception applies. Breach reporting is not required under HIPAA.
      ☐ No, an exception does not apply. Continue to Question 5.

5. **Risk Assessment.** An acquisition, access, use or disclosure of PHI in a manner not permitted by the

Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors below. Documentation of consideration of all the factors is required.

Factor A: Consider the nature and extent of the PHI involved, including the types of identifiers, sensitive financial information (credit card or SSNs), or clinical information (STDs, mental health, etc.)

Describe the PHI involved, identifiers, and likelihood of reidentification, if applicable:

Could the PHI be used in a manner adverse to the patient or to further the unauthorized person's interests:

Factor B: Consider the unauthorized person who used or received the PHI. (This factor must be considered if the PHI was used impermissibly within the organization as well as when disclosed outside. Consider whether the person has legal obligations to protect the information, e.g., is the person required to comply with HIPAA or a government employee or other person required to comply with privacy laws. If so, there may be a lower probability the PHI was compromised.

Describe who used or received the PHI, whether they have a legal obligation to protect the PHI and whether they can re-identify the PHI, if applicable:

Factor C: Consider whether the PHI was actually acquired or viewed.

Describe whether the PHI was actually acquired or viewed (attach report from computer forensic expert if one was obtained:

Factor D. Consider the extent to which the risk to the PHI has been mitigated (returned, has been or will be destroyed). Describe the risk mitigation steps taken and any other relevant factors.

Based on these factors, is there a low probability that the PHI has been compromised?

☐ Yes, there is a low probability. Breach reporting is not required under HIPAA.
☐ No, there is a higher probability. Breach reporting is required under HIPAA

Sign and date the Risk Assessment.