HAWAII HEALTH SYSTEMS CORPORATION "Quality Healthcare For All"	Department: *Quality Through Compliance*	Policy No.: **CMP 014A**
		Revision No.: 1
POLICY	Issued by: Audit and Compliance Committee	Effective Date: September 19, 2013
Subject: ***HIPAA Breach Notification***	Approved by: Carol VanCamp HHSC Board of Directors By: Carol A. VanCamp Its: Secretary/Treasurer	Supersedes Policy: Page: 1 of 7

Last Reviewed: August 13, 2013. Next Review: August 13, 2016

I. PURPOSE:

This policy establishes the process for notification of breaches of unsecured protected health information in each Hawaii Health Systems Corporation (HHSC) facility.

II. DEFINITIONS:

PHI: Protected Health Information.

Access means the ability or the means necessary to read, write, modify, or communicate PHI.

Acquisition means the obtaining of PHI by anyone.

Breach means acquisition, access, use or disclosure of PHI which violates the HIPAA Privacy Rule and compromises the security or privacy of the PHI.

Business Associate means vendors who have access to or utilize PHI. This would include but not be limited to vendors who perform claims processing or administration, data analysis, coding, billing, benefit management, or reprising, or who provide legal, actuarial, accounting, consulting accreditation or financial services to HHSC. (See CMP 031A.)

Compliance Officer refers to the HHSC Chief Compliance and Privacy Officer, the Regional Compliance Officer for each HHSC region, and/or the facility compliance officer.

Compromises the security or privacy of the PHI. An acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule is presumed to be a breach unless HHSC demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment, explained below.

Disclosure means the transmission of PHI outside the organization or outside the organization's business associate.

Discovered means the day the HHSC, or its business associate, knew or should have known by exercising reasonable diligence that the breach of unsecured PHI occurred.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009, Pub.L. 111-5, 123 Stat. 226, February 17, 2009, and their implementing regulations at 45 C.F.R. 160 and 164, as amended, collectively referred to in all HHSC policies as "HIPAA")

Notification process means the activities for notifying the individual, the federal government or such other actions required by federal and state law and this policy.

Unsecured PHI means any PHI which is not in a format which the United States Department of Health & Human Services (DHHS) has identified as rendering the PHI unusable, unreadable, or indecipherable to unauthorized individuals. DHHS has the ability to change the definition at any time. At the time of publication of this policy, DHHS has determined that any PHI which is not destroyed or encrypted (according to certain encryption methods) shall be considered "unsecured PHI." No encryption method shall be considered sufficient to render PHI not unsecured PHI unless the encryption method has been approved by the compliance officer. Additionally, PHI shall only be considered not unsecured when the de-encryption key is maintained on a separate device from the unsecured PHI. For example, a pass code should not be sent via email to the same email address to de-encrypt an encrypted document in a subsequent email.

Use means utilizing PHI which has not been disclosed outside of the organization or the organization's business associate (See CMP 031A).

III. POLICY:

A. HHSC shall comply with all federal laws requiring the organization to notify the individual and government authorities, and undertake other actions, if a member of HHSC's workforce or a business associate discovers a breach of unsecured protected health information (PHI) such that the HIPAA Privacy Rule was violated and the breach poses a significant risk of financial, reputational, or other harm to the individual.

B. HHSC's Regional Compliance and Privacy Officers ("compliance officer") in conjunction with the HHSC Chief Compliance and Privacy Officer (CCPO) ("compliance officer") shall be responsible for reviewing all HIPAA complaints or suspected HIPAA violations to determine whether notification to the individual or federal government, or other action, is required. HHSC need not notify the individual or federal government of a breach of unsecured PHI if federal law prohibits or does not require such notification.

C. Suspicions of breaches of unsecured PHI must be reported to the compliance officer. The compliance officer shall be responsible for investigating a suspected breach of unsecured PHI and shall make a determination whether notification to the individual or the federal government, or other action, is required. The compliance officer shall document the notification conclusion for every suspected HIPAA complaint reviewed by the compliance officer.

D. HHSC shall also comply with any additional State notification requirements, if any.

E. HHSC shall determine whether there is a low probability that the PHI has been compromised. HHSC must perform 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.
   5. A "Breach Notification Flow Chart" such as included in Attachment A shall be consulted.

F. Responsibility
   1. All workforce members shall report to the compliance officer any suspected or known breaches of unsecured PHI
   2. The compliance officer shall be responsible for investigating all suspected or known breaches of unsecured PHI

G. Investigation Procedure for Suspected or Known Breaches
   1. The compliance officer shall identify whether the PHI involved in the activity was "unsecured" at the time of the suspected breach. If PHI is not unsecured, then the organization is not required to notify the individual and federal government. The compliance officer should document a finding that the PHI is not unsecured and explain why he or she believes the incident did not involve unsecured PHI
   2. The compliance officer shall determine, to the best of the compliance officer's ability, whether the unsecured PHI was inappropriately acquired, accessed, used or disclosed and violated the HIPAA Privacy Rule.
      a) The compliance officer shall categorize the inappropriate activity with the PHI as acquisition, access, use or disclosure. An inappropriate activity may fall into more than one category.
      b) The compliance officer shall investigate and determine, to the best of the compliance officer's ability, whether the inappropriate activity was unintentional.
   3. The compliance officer shall investigate and identify, to the best of the compliance officer's ability, the day HHSC discovered that a breach of unsecured PHI occurred. If a breach was of PHI in the possession of or maintained by a business associate, then the compliance officer must attempt to identify the day the business associate discovered the breach occurred.

H. Notification Process Exceptions
   1. When the compliance officer has determined that a breach of PHI occurred, the compliance officer shall also determine whether any of the following conditions occurred (these shall be known as "Notification Exceptions"):
      a) The breach involved PHI that is not unsecured.
      b) The breach did not violate the HIPAA Privacy Rule.
      c) The breach involved unintentional acquisition, access, or use of unsecured PHI by a workforce member or person acting under the authority of HHSC or a business associate and was made in good faith within the course and scope of the person's authority and the PHI was not further used or disclosed in a way that violates the HIPAA Privacy Rule.
      d) Any inadvertent disclosure by a person who is authorized to access PHI at HHSC or a business associate to another person authorized to access PHI at HHSC or the same business associate, or within an organized health care arrangement in which HHSC participates, and the PHI was not further used or disclosed in a way that violates the HIPAA Privacy Rule.
      e) A disclosure of PHI where HHSC or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

I. Notification Process
   1. If none of the Notification Exceptions are met, then HHSC will consider that a breach of unsecured PHI has occurred which requires notification to the individual and to the federal government. HHSC will use the notification process set out in this policy.
   2. Notification shall occur as required by federal law, to the individual, to DHHS, and in some instances to local media.
      a) Letter: HHSC shall notify the individual whose PHI has been breached without unreasonable delay, but in no circumstances later than 60 days after discovery of the breach of unsecured PHI. If the compliance officer believes that the breached PHI is in danger of imminent misuse in a way that would harm the individual, then the

compliance officer must notify the individual immediately using whatever means of communication most easily assures communication with the individual. A letter shall be sent to the individual at the individual's last known address by first class mail and shall be signed by HHSC Chief Executive Officer or Regional Chief Executive Officer, as appropriate. The letter shall be written in plain language and include the following:

i. Brief description of what happened
ii. Date of the breach
iii. Date of the discovery of the breach
iv. Types of unsecured PHI that were involved in the breach, noting categories of identifying information such as, full name, social security number, date of birth, diagnosis, disability code, but not the actual identifying information
v. Steps individuals should take to protect themselves from potential harm
vi. What HHSC is doing to investigate the breach, mitigate harms to the individual, and protect against any further breaches
vii. Contact procedures for individuals to ask questions or learn additional information which shall include a toll-free number, email address, website or postal address.

b) Deceased Individual: If the individual is deceased, then the letter shall be sent to the last known address of the next of kin or personal representative.

c) Substitute Notice: If there is insufficient or out-of-date information to comply with Sections a) or b) above, then HHSC may undertake substitute notice in the following circumstances:

i. For fewer than 10 individuals: When there is insufficient or out of date contact information for fewer than 10 individuals, then HHSC may notify the individual (or next of kin or personal representative) by an alternative form of written notice, telephone, or other means.
ii. For 10 or more individuals: When there is insufficient or out-of-date contact information for 10 or more individuals, then HHSC shall post a notice on the home page of its website describing the type of breach and requesting persons who believe their information may have been involved to call a toll-free number. The posting for each breach shall remain on HHSC's website for a period of 90 days, OR:
iii. HHSC shall place a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

J. Notification to Department of Health and Human Services (DHHS): HHSC's Chief Compliance and Privacy Office shall notify DHHS of any breach of unsecured PHI which does not meet a Notification Exception. HHSC shall notify DHHS in the following ways:

1. If the breach involves 500 individuals or more, then HHSC shall notify DHHS at the same time as the notice to the individuals;
2. If the breach involves fewer than 500 individuals, then HHSC shall log the breach in a manner consistent with federal expectations and report the log annually to DHHS not later than 60 days after the end of each calendar year, or as DHHS may direct.
3. HHSC shall use the processes and procedures for notifying DHHS as may be prescribed by law.

K. Notification to Local Media: The facility shall notify a local prominent media outlet that a breach of unsecured PHI has occurred if the breach involved more than 500 individuals from the same State or jurisdiction and the breach requires notification to the individual.

Notification to local media shall occur without unreasonable delay and in no case later than 60 calendar days after discovery of a breach requiring notification.

L. Law Enforcement Request: Notification to the individual (or next of kin or personal representative) and the media shall be delayed to a date specified by a law enforcement officer in writing if the law enforcement officer states that notification would impede a criminal investigation or cause damage to national security. If the law enforcement officer requests delay orally, then the compliance officer shall document the request and the delay shall be no longer than 30 days from the date of the oral statement, unless a written statement is provided by the law enforcement officer.

M. Documentation
   1. An investigation of a suspected breach of unsecured PHI shall be treated as a matter of urgency by the compliance officer.
   2. The compliance officer shall document the investigation.
   3. All conclusions in a breach investigation must be supported with written reasons.
   4. The compliance officer shall log all known breach notifications.
   5. The compliance officer shall keep copies of all notification documents.

N. Each HHSC facility will implement procedures to operationalize this Policy.

IV. APPLICABILITY: This Policy shall apply to all HHSC Facilities.

V. AUTHORITY: Standards for Privacy of Individually Identifiable Health Information (HIPAA), 45 CFR Part 164§ §164.402; 164.404; 164,406; 164.408; 164.410; 164.412; 164.414. CMP 031A.

VI. ATTACHMENTS: Attachment A—"Breach Notification Flow Chart"

Attachment A
Breach Notification Flow Chart

Breach notification is presumed necessary in all situations involving improper use/disclosure of PHI unless the covered entity/business associate can demonstrate there is a low probability that the PHI has been compromised (or that an exception applies).

1. Did the breach involve protected health information (PHI)?

    a. If no, the breach does not require notification under HIPAA.

2. If yes, does an exception apply?

    i. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in the further use or disclosure in a manner not permitted by the Rule.

    ii. Any inadvertent disclosure by a person who is authorized to access PHI to a covered entity or business associate to another person authorized to access PHI at the same organization or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Rule.

    iii. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably been able to retain such information.

3. If an exception applies, the breach does not require notification under HIPAA.

4. If an exception does not apply, the covered entity or business associate must assess the probability that the PHI has been compromised. To determine if the PHI has been compromised, the Covered Entity/Business Associate must undertake a risk assessment that specifically considers four factors:

    a. The nature, extent, type and sensitivity of the PHI involved;

    b. The unauthorized person/entity that used or acquired the PHI, including whether they are subject to confidentiality obligations (such as HIPAA, but including others);

    c. Whether the PHI was actually acquired or viewed, or merely subject to the opportunity for such access; and

d. The extent to which the risk to the PHI was mitigated; including efforts to obtain assurances that the PHI will not be further used or disclosed, and the reliability of such efforts under the circumstances.

5. If a thorough, good-faith assessment of these, and perhaps other factors, fails to demonstrate that there is a low probability that the PHI was compromised, then breach notification is required.