HAWAII HEALTH SYSTEMS
C O R P O R A T I O N

"Touching Lives Every Day"

COMPLIANCE ALERT 13-11

Addressing Potential HIPAA Violations

The new HIPAA Omnibus Rule of 2013 makes every unauthorized use of protected health information (PHI) a presumed breach until risk analysis is conducted. Consequently, it is even more critical that Reporting Data Security Incidents be reported and that all employees and contractors take precautions to prevent unauthorized use and access of PHI.

All potential security incidents involving sensitive information should be reported immediately to your Regional Compliance Officer, Corporate Compliance Hotline, HHSC's Security Officer (for IT issues), or HHSC's Chief Compliance and Privacy Officer.

Examples of Incidents to Report: Any of the following could constitute a potential data security incident:

- Misuse of sensitive information – e.g. posting of patient information on a social website
- Social Engineering attempts
- Potential malware infections
- Loss or theft of a PC or other electronic storage device
- Missing hard-copy documents or media
- Sensitive information e-mailed without encryption

Communications: To reduce potential liability, it is important to take care in how you communicate about a potential data security incident. Specifically -

- Avoid using email to communicate about the incident. Use the telephone instead.
- If you must use email, copy your in-house legal counsel (or your outside attorney).
- Strictly follow your facility's reporting procedure and do not discuss the incident with:
  - any other employees, family, the media, or any other person until authorized to do so.
- Do not use the term "breach" because that may require a legal conclusion. Early in the process, there is rarely enough information to make this conclusion. Instead, call it what it is. If it is a lost laptop, refer to the incident as "a lost laptop"; if it is a potential malware intrusion, refer to the incident as a possible malware intrusion.
- Do not send incident-related documents to any other person, including your insurance company, unless authorized to do by your Compliance Officer and/or Senior Management. Such authorization is typically granted only with approval from in-house legal counsel (or other legal counsel).

Dealing With Media Inquiries:

Refer any inquiries from outsiders (e.g. the media) to the designated person in your organization.

Source: Beazley/ePlace Inc—3-13