1/22/08

PRACTICES FOR HIPAA SECURITY RULE COMPLIANCE

The HIPAA Security Rule

UC Santa Cruz is subject to the federal Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which identifies legal requirements for the protection of electronic protected health information (ePHI)[1] for health care providers and related entities. UC Santa Cruz is taking a campus-level approach to HIPAA Security Rule compliance by identifying a set of practices which, when fully implemented, fulfill the HIPAA Security Rule requirements.

Practices for HIPAA Security Rule Compliance

Units subject to HIPAA Security Rule requirements must implement the *UCSC Practices for HIPAA Security Rule Compliance* (http://its.ucsc.edu/policies/hipaa-practices.html). Units must also document their implementation, including any associated or supporting policies or practices, utilizing the *UCSC HIPAA Security Rule Compliance Workbook* (available at http://its.ucsc.edu/policies/hipaa.html or a comparable documentation method.

The *UCSC Practices for HIPAA Security Rule Compliance* were developed by a cross-functional sub-group of the UCSC HIPAA Compliance Team, including all units subject to the HIPAA Security Rule, Internal Audit, and ITS Security. They incorporate information, practices and guidelines from a number of federal, University and industry sources (see References), as well as UCSC technical and business considerations. The development of these practices also incorporated a risk assessment process, ensuring that areas of risk or concern were identified and addressed, and acknowledging that any set of practices would inherently embody some degree of risk.

> A Special Note about Required vs. Addressable Implementation Specifications
>
> The HIPAA Security Rule consists of a series of administrative, technical, and physical security procedures, or "Standards" for safeguarding ePHI. Most Standards are delineated into either "required" or "addressable" implementation specifications[2]. Required Standards and implementation specifications must be implemented as stated for compliance. For addressable implementation specifications, it must be determined whether each specification is reasonable and appropriate. If it is, it must be implemented as stated. If it is not, the entity must document the reasons for this determination and implement alternative compensating controls, or otherwise indicate how the intent of the standard can still be met.

Related Policies & References for More Information

- *The HIPAA Security Rule ([US] Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule):* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
- *US Department of Health and Human Services, Centers for Medicare and Medicaid Services (CMS)*: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html and http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
- *UC Guidelines for HIPAA Security Rule Compliance:* http://www.universityofcalifornia.edu/hipaa/docs/security_guidelines.pdf
- *UC HIPAA Website:* http://www.universityofcalifornia.edu/hipaa/
- *UCSC HIPAA Security Rule Website:* http://its.ucsc.edu/policies/hipaa.html
- *UC Davis Health System HIPAA Security Compliance Workbook*
  - *Single User Guide:* http://www.ucdmc.ucdavis.edu/compliance/pdf/subook.pdf
  - *Multi-User Guide:* http://www.ucdmc.ucdavis.edu/compliance/pdf/mubook.pdf
- *NIST SP 800-66 (An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule):* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
- *UHC (University Healthsystem Consortium) Standards of Good Practice for HIPAA Security Compliance* [no longer available online]

[1] Electronic Protected Health Information (ePHI) is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.

[2] An "implementation specification" is an additional detailed instruction for implementing a particular standard.