


Standards and Procedures

- Written Policies
 - Start with the Rule
 - How will you comply
- Procedures
 - Reflect what you are doing
 - Include appropriate operational departments
- Will need to revise regularly – annually or biennially and when there is a change

2012 Alaska Medicaid



HHS.gov U.S. Department of Health & Human Services
 Health Information Privacy

I'm looking for... 

HHS A-Z Index

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

HHS > HIPAA Home > For Professionals > Compliance Enforcement > Audit > Audit Protocol

Text Resize A A A Print Share Facebook Twitter +

HIPAA for Professionals

Audit Protocol – Updated April 2016

The Phase 2 HIPAA Audit Program reviews the policies and procedures adopted and employed by covered entities and business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These analyses are conducted using a comprehensive audit protocol that has been updated to reflect the Omnibus Final Rule. The audit protocol is organized by Rule and regulatory provision and addresses separately the elements of privacy, security, and breach notification. The audits performed assess entity compliance with selected requirements and may vary based on the type of covered entity or business associate selected for review. You may submit feedback about the audit protocol to OCR at OSOCRAudit@hhs.gov.

The protocol is available for public review and searchable by keyword(s) in the table below; export options will be made available soon.

Privacy +

Security +

Breach Notification +

Compliance & Enforcement -

Audit Type	Section	Key Activity	Established Performance Criteria	Audit Inquiry	Required/Addressable
Privacy	§164.502(a)(5)(i)	Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes	§ 164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5)(i)(B) of this section: (1) Rule for or determination	Does the health plan use or disclose for underwriting purposes, "Genetic Information" as defined at § 160.103, including family history? Inquire of management. Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials). Evaluate whether the underwriting policies	

Education and Training

- New Employees
 - Must train within a “reasonable amount of time”
 - Must be documented
 - Related to job
- Existing staff
 - Periodic security updates
 - Anytime there is a material change

Monitoring and Auditing

- RISK ANALYSIS (security and privacy)
 - Comprehensive
 - Living
 - Include everyone that touches PHI
- Talk about findings
 - HIPAA does not exist in a box
 - Refine standards and procedures
- On going event monitoring
- Regular privacy audits

Too Many Trees



Do Something



Response and Prevention

- BREACHES (45 CFR § 164 Subpart D—
Notification in the Case of Breach of
Unsecured Protected Health Information
 - Exceptions
 - Risk Assessment
- Mitigation and Prevention
- Requirements to disclose

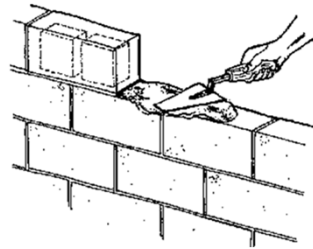
Enforcement and Discipline

- Sanctions
 - Workforce members
 - Document
- Punishment needs to match the crime

Reporting

- Report to the Board
- Include in your annual training

Fill in the Gaps



NIST Cybersecurity Framework

- HHS crosswalk
- Added support to your Standards and Procedures

Stay Current

- Review your professional resources
- Visit Governmental Websites
 - OIG
 - HHS

Conclusion

- Risks to Organization
- Use the basic structure to create a base and augment
- Tools and Resources
- Engage others for help
- Keys to HIPAA compliance
 - Risk Analysis
 - Document, document, document,

Rules Tools

- 45 CFR 160 HIPAA General Administrative Requirements
<http://162.140.57.127/cgi-bin/text-idx?SID=f93fdec29fbda880fe0e2bfb252bad46&mc=true&node=sp45.1.160.a&rgn=div6>
- 45 CFR 164 PART 164—SECURITY AND PRIVACY
<http://www.ecfr.gov/cgi-bin/text-idx?SID=fe60fe4d138c1ac86e2e81f99b4908a6&mc=true&node=pt45.1.164&rgn=div5>
- HHS HIPAA Audit Protocol <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html?language=es>
- Cornell University Law School, Legal Information Institute
<https://www.law.cornell.edu/>

Guidance and Information

- HIPAA/NIST crosswalk <https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf>
- HIPAA Privacy, Security & Breach Notification Compliance Audits phase 2, INFORMATIONAL WEBINAR, July 13, 2016
<https://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf?language=en>
- NIST Special Publication 800-53, rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Office of Inspector General (various HIPAA reports, investigation results, and guidance) <https://oig.hhs.gov/>
- HealthIT.gov Security Risk Assessment
<https://www.healthit.gov/providers-professionals/security-risk-assessment>

Professional Resources

- HCCA <http://www.hcca-info.org/>
- American Health Information Management Association <http://www.ahima.org/>
- Healthcare Information and Management Systems Society <http://www.himss.org/>
- AMA <https://www.ama-assn.org/practice-management/hipaa-compliance>
- AHA <http://www.aha.org/advocacy-issues/hipaa/index.shtml>

Other Information

- HcPro HIPAA Update
<http://blogs.hcpro.com/hipaa/>
- HIPAA COW (Collaborative of Wisconsin)
<http://hipaacow.org/>
- HIPAA News.org <http://hipaanews.org/>
- (NCHICA) North Carolina Healthcare Information & Communications Alliance, Inc.
<http://nchica.org/>

References

- Becker's Health IT and CIO review "10 largest HIPAA settlement fines"
<http://www.beckershospitalreview.com/healthcare-information-technology/10-largest-hipaa-settlement-fines.html>
- Becker's Health IT and CIO review "Missouri mom accused of violating HIPAA by taking son's photo is suing Mercy Hospital"
<http://www.beckershospitalreview.com/healthcare-information-technology/missouri-mom-accused-of-violating-hipaa-by-taking-son-s-photo-is-suing-mercy-hospital.html>
- Six people fired from Cedars-Sinai over patient privacy breaches, July 12, 2013 By Anna Gorman and Abby Sewell
<http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713>
- Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay \$239,800 <http://wayback.archive-it.org/3926/20170127185543/https://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html>



My Information

Ben Burton, JD, MBA, RHIA, CHPS, CHC
Ben.Burton@firstclassolutions.com
Consultant
First Class Solutions, Inc.
11426 Dorsett Road, Upper Level
Maryland Heights, MO 63043
Tel: 314-209-7800
Fax: 314-209-1911
Cell:207-420-5811



Questions?

