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
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. Those 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 OSCRAudit@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.

<table>
<thead>
<tr>
<th>Audit Type</th>
<th>Section</th>
<th>Key Activity</th>
<th>Established Performance Criteria</th>
<th>Audit Inquiry</th>
<th>Required Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>§164.502 (a)(5)(i)</td>
<td>Prohibited uses and disclosures - Use and disclosure of genetic information for underwriting purposes</td>
<td>§ 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 failing within paragraph (1)(vi) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraphs (a)(5)(iii) of this section, underwriting purposes means, with respect to a health plan: (A) Except as provided in paragraph (a)(5) (iii)(B) of this section: (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>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 Obtain and review all underwriting policies and procedures (for example, published and unpublished underwriting guidelines currently used by underwriting staff, including manuals and training materials).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</td>
<td></td>
</tr>
</tbody>
</table>
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=f93fdec29fbd880fe0e2bfb252bad46&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

- Office of Inspector General (various HIPAA reports, investigation results, and guidance) https://oig.hhs.gov/

Professional Resources

- HCCA http://www.hcca-info.org/
- American Health Information Management Association http://www.ahima.org/
Other Information

- HcPro HIPAA Update
  http://blogs hcpro com/hipaa/
- HIPAA COW (Collaborative of Wisconsin)
  http://hipaadcow 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@firstclasssolutions.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?