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
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-idx5sid=f93fde219f6da880f0e2ef652bad46&mc=true&node=s45.1160.x&rgn=dive
- 45 CFR 164 PART 164—SECURITY AND PRIVACY http://www.ecfr.gov/cgi-bin/text-idx?SID=fe60fe4d1381ac38e2e81f99b4908a6&mc=true&node=pt45.1.164&rgn=dive
- 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
- HIPAA COW (Collaborative of Wisconsin)
- (NCHICA) North Caroline Healthcare Information & Communications Alliance, Inc.

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](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](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](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

My Information

Ben Burton, JD, MBA, RHIA, CHPS, CIAC
Ben.Burton@firstclasssolutions.com
Consultant
First Class Solutions, Inc.
15400 Dorsett Road, Upper Level
Maryland Heights, MO 63043
Tel: 314-209-7000
Fax: 314-209-1511
Cell: 207-420-5811
Questions?