COMPLIANCE — HOW TO PREPARE YOUR EAP

RESOURCE GUIDE

2019 EAPA presentation by Diana Wicker, Director of Compliance and Reporting

Specialists You Need to Know

1. Forensic IT analyst firm
2. Security specialist
3. HIPPA compliance auditing firms
4. SOC II auditors from AICPA

Sample Documents

1. Sample list of policies and procedures
   https://hipaacow.org/resources/hipaa-cow-documents/privacy-security/

Additional Training Available

1. Web based webinars on security available at:
   https://www.hhs.gov/hipaa/for-professionals/training/index.html
   https://www.nist.gov/video/flexible-methodology-manage-information-security-and-privacy-risk

Important Links

1. HIPAA regs can be found at:
   1. 160 - General administrative requirements
   2. 162 - Administrative requirements
   3. 164 - Security and privacy
      - A. (Admin safeguards)
      - B. (Physical standards)
      - C. (Technical standards)
      - D. (Policy & procedure & documentation requirements)
   4. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
   5. https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
   6. Sign up for the OCR Security Listserv to receive the OCR cyber awareness newsletters in your email inbox.
2. HITECH regulations can be found at: 170 - Health Information Technology Standards, Implementation specifications, and certification criteria and certification programs for health information technology
   1. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html
   2. Learn more about the Privacy and Security Framework and view other documents in the Privacy and Security Toolkit, as well as other health information technology resources.
3. Confidentiality of alcohol and drug abuse patient records can be found at: Part 2 - Confidentiality of Substance Use Disorder Patient Records (1975)
   1. https://www.samhsa.gov/laws-regulations-guidelines/medical-records-privacy-confidentiality
4. Breach notification
   1. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
5. State legislature
   1. http://www.ncsl.org/research/telecommunications-and-information-technology.aspx
6. FTC: Federal Trade Commission Act 5 - https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
   1. Yes! This is important!
      - A. https://healthitsecurity.com/news/12-states-sue-business-associate-for-2015-health-data-breach?eid=CXTEL000000394242&elqCampaignId=9600&elqTrackId=00b61d7320b141d8ac378006837aab76&elq=f62fb0384da44bd0a4c06d06f29be064&elqaid=10095&elqat=1&elqCampaignId=9600
        1. Unfair and deceptive practice named in HIPAA breach lawsuit

7. Mobile health apps
    1. https://www.hhs.gov/hipaa/for-professionals/special-topics/developer-portal/index.html
8. Cloud computing
    1. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
9. Nice reference for all federal security protection acts: https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

Other good regulation integration links:

- https://www.hhs.gov/hipaa/for-professionals/special-topics/related-links/index.html
- https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-ftc-act/index.html
- https://www.iso.org/isoiec-27001-information-security.html
- https://www.nist.gov/itl

You May Ask Yourself

- Do you have a company website? Do customers and clients interact with it? Is it secure? Do you have BAA where necessary?
- Do you utilize email with your customers and clients? Is it secure? Do you have BAA where necessary?
- Do you utilize SMS texting (cell phones) with your customers and clients? Is it secure? Do you have BAA where necessary?
- Do you utilize messaging/chat services — no video, text only — (smart phones, tablets, computers) with your customers and clients? Is it secure? Do you have BAA where necessary?
- Do you utilize video conferencing services (smart phones, tablets, computers) with your customers and clients? Is it secure? Do you have BAA where necessary?
- Do you utilize/provide to your customers and clients with any smart phone/tablet apps? Wellness, behavioral health, mental health — Do these apps include live interaction with a counselor or coach? Do you have a BAA with the company providing the database BEHIND the app that gathers client information? Did you know that these items will soon be regulated as medical devices?
- Do you utilize/provide an AI SMS/chat service to your customers and clients for their cell/smart phones? Is it secure? Do you have BAA where necessary? Did you grant permission for conversations to be used in research? Did you update your Notice of Privacy Practices to include this?
- Do you maintain your own computer server/network? Do all the testing!
- Do you work from individual computer work stations via a private cloud VPN network? Do you have the testing for your private cloud provider? Is it secure? Do you have BAA where necessary?
- Do you work from individual computer work stations utilizing cloud applications? I login to an online service via my web browser. I login to an App (application/program) that I downloaded that syncs to the online service when the Internet is active. Is it secure? Do you have BAA where necessary?
- Do you work from individual computer work stations that record and store PHI directly to the hard drive of that physical machine? Is it secure? (Are you very sure?)

Other Considerations:

- Do you serve 10K+ US citizens per year? Consumer Privacy Protection Act of 2017
- Do you serve European citizens? EU-US Privacy Shield
- Do you serve federal employees? The **Privacy Act** of 1974, 5 U.S.C. § 552a
- Do you serve clients IN ANY state that has data security laws? http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx
    - Example: South Carolina Insurance Data Security Act - https://www.doi.sc.gov/918/Cybersecurity