Eliza Jennings

choices for aging well

M2A Building a Cybersecurity Auditing and Monitoring Plan

Presented by

Jennifer Griveas and Michael Gray

1

Who We Are

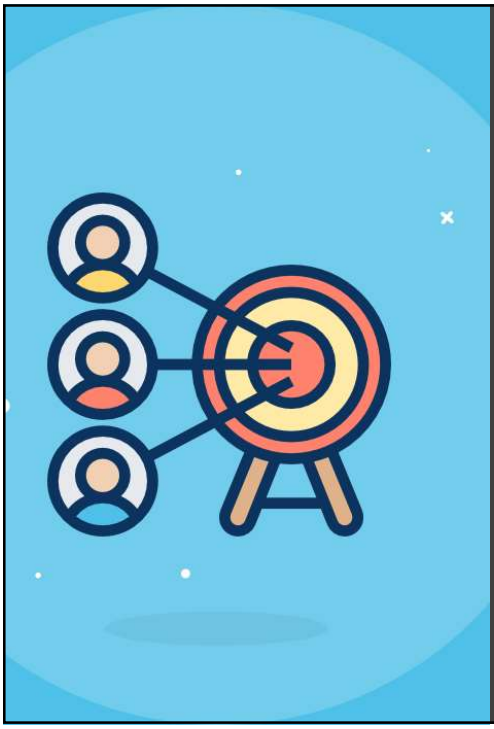
Jennifer Griveas, Esq., CHC, is the Chief Human Resources Officer and General Counsel for the Eliza Jennings Senior Care Network, where she has served as a member of the senior management team since 2011. She oversees all legal matters for the organization, including regulatory compliance and risk management, labor and employment issues, litigation management, and transactional matters. She is certified in health care compliance by the HCCA, and works extensively with company management on matters of compliance and IT security.

2

Who We Are

Michael Gray, HCISPP, HIT, is Vice President of Information Technology and Compliance Officer. He has worked for Eliza Jennings for ten years. He is primarily responsible for ensuring that the company mission is met through the use of technology on a daily basis, maintaining various compliance requirements, ensuring that the department meets and exceeds quality benchmarks, and ensuring that the organization is in a position to meet future challenges.

3



Focus Areas

- How to decide
- Granular vs Broad

4

HIPAA

- HIPAA compared to other regulations
- Overwhelming amount of guidance
- Levels of risk
- Related frameworks
- HIPAA is not the only compliance concern

5

Risk Assessment

- Requirements (as they apply to your organization)
- Systems
- Users
- Types of Data
- Lengthy process – there are tools to help!
- This process takes time

6

Common Threats

- Users
  - Mobile Devices
  - Passwords
  - User Access/Terminations
- Ransomware
- Pandemic “inspired”
  - EHR is more valuable
  - Vaccine and COVID specific threats
  - Work From Home – increased risk

7

Now What?

- Who is in charge?
- Auditing and monitoring
- How do you develop action plans?

8

Plan Examples

- Auditing logs and software
  - Is SIEM for you?
- Who is reviewing and where does it go?
- What is your workflow for sharing this data?

9

Plan Examples

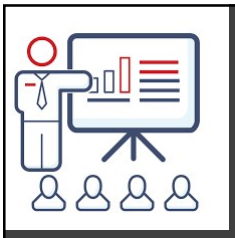
- Mobile Devices
  - Who has them?
  - BYOD
  - Encryption
- Mobile Device Management (MDM)
- Virtual Private Network (VPN)

10

Policies

- Major risk areas require written policies even where policy may not be required by statute.
- Audits are great for trends – this needs constant monitoring
- New account creation
  - Who?
  - Template based?
- Highest risk user groups
  - Permission groups
  - Scrutinized more
- Terminations
  - Advance notice
  - Heavily monitor
  - Cooperation between HR and IT

11



Train. Keep Training.

- Staff awareness: know the threats, not just the rules
- Training on hire is only the beginning
- Set work plan for role-based training
- Bite-sized pieces are easier to digest
- Did something go wrong? Time to train. Again. Embrace the repetitive.
- This stuff is fun! It pertains to real life!

12

Questions?