What Your Privacy Officer Is Trying To Tell You (Security)... If Only You Would Listen.

Live Presentation by Lori Hopper and Doc Blackburn

SANS | GIAC CERTIFICATIONS

Lori Hopper
Institutional Compliance & Privacy Officer at University of Colorado Denver and Anschutz Medical campuses.

Doc Blackburn
Cybersecurity Evangelist and coauthor of SANS SEC474: Building A Healthcare Security & Compliance Program.

> *"The Privacy Team wants the same thing the Security Team does."*
> —Lori Hopper

Effects of the HIPAA Privacy and Security Rules

- **HIPAA made information more portable for doctors**
- **Outlines how to keep the data safe**
- **Patient privacy is a civil rights issue and handled by the Office for Civil Rights (OCR)**

What a Privacy Officer Does

- Tasks that the Security Team doesn't want to do
- Expert communicator and relationship builder
- Oversight of:
  - Policies and procedures
  - Governance
  - Controls
  - Oversight
  - Education
  - Communication
  - Monitoring and auditing
  - Enforcement and Discipline
  - Response and prevention

How can the Security Team and the Privacy Team work together?

- Know what each team is doing so that you can maximize your efforts and not duplicate your work.
- Use your Privacy Team as the go-between for the regulatory enforcement agency and your team. Let your Privacy Team do what they do best so you can do what you do best.
- Document! This flows all the way down to conversations and meetings; not just the formal documentation (policies, procedures, etc.).
- Build a culture of compliance or "Psychology of Compliance."
- Separation of duties exists, but often times there is overlap. Create a partnership with your Privacy Team.
- Communication is key between the teams. Get back to basics:
  - Understand your audience
  - Understand their business (roles)
  - Speak their language
  - Provide some solutions

How does HIPAA affect the Security Team and the Privacy Team?

- The HIPAA Privacy Rule and the HIPAA Security Rule want to accomplish the same thing, use the Security Rule in support of the Privacy Rule.
- All regulations related to privacy and security are interrelated.
- Build the best program for the size of organization you can, while building in opportunities for continuous improvement.
- Documentation best supports the Privacy Rule – is the "case file in front of the OCR."
- Rules are black and white, but your Security Program has to be documented.