NC Department of Health and Human Services

Privacy and Security Office

September 11, 2025

The DHHS Privacy and Security Office

- The Privacy and Security Office (PSO) provides privacy and security information for the NC Department of Health and Human Services (NCDHHS). The PSO safeguards information from unauthorized use, disclosure, modification, damage or loss.
- The PSO provides consulting services around Privacy and Security, Business Continuity Planning (BCP), Continuity of Operations (COO), Disaster Recovery (DR), Forensic Investigations, Privacy and Security Policies, Incident Management, Risk and Threat Management.
- The PSO serves as the liaison between various Federal and State Agencies.
- The PSO is responsible for conducting annual reviews based on Federal and State requirements.

Security 101: Getting Back to Basics

“Start at the beginning and when you get to the end, stop.”

- The Mad Hatter

Security 101: The Security CIA Triad Review

- **Confidentiality:**
  Ensuring that sensitive information is accessible only to authorized individuals or systems, protecting privacy and preventing unauthorized disclosure.

- **Integrity:**
  Maintaining the accuracy and completeness of data, ensuring it hasn't been altered, corrupted, or destroyed, and that systems are reliable.

- **Availability:**
  Guaranteeing that authorized users can access information and resources when they need them, ensuring timely and reliable access.

Security 101: Security vs Privacy

Security

Is focused on protection of systems, assets, information, and data and physical locations including the methods employed to do so.

Privacy

Is focused on how a person’s information is disclosed, utilized, managed and controlled by an organization.

Security 101: Security Control Types Review

Security controls are measures and mechanisms put in place to protect information systems from security threats, vulnerabilities, and risks

Management Based Controls

- Focus on policies, procedures, and organizational structures to manage risk and ensure information security
- Includes incident response, access control, and service provider management, program management

Security 101: Security Control Types Review (cont.)

Operational Based Controls

- Focus on the actions and procedures used to protect systems and data during day-to-day operations
- Includes access control, change management and monitoring, ensuring a secure environment.

Technical Based Controls

- Focus on measures implemented through hardware and software to protect systems, networks and data from cyber threats.
- Includes logging, monitoring, encryption, firewalls, intrusion detection systems (IDS) and identification and authentication mechanisms.

Security 101: Security Control Types Review (cont.)

- **Deterrent Controls:** Discourage potential attackers by making their efforts more difficult or risky.
- **Preventive Controls:** Are designed to stop security issues from happening in the first place.
- **Detective Controls:** Identify security issues after they've begun, allowing for a quicker response.
- **Physical Safeguards:** Are designed to create safe and secure physical locations for resources.

Security 101: Starting Security Advice

- Start small
- Understand not only existing policies and procedures but think about what might be lacking
- Communication is key
- Start to document what you think needs to be done
- Create some milestones or accomplishments
- Let folks know what you are doing and why

Security 101: Starting Security Efforts

Things that can be done with minor effort but make a big impact

- Physical walk throughs.
- Review and enforce clean desk policies.
- Promote general cyber security awareness.
- Talk to people and groups about password best practices.
- Work with business teams to brainstorm ideas for promoting client security.
- Ensure systems are getting regular updates.
- Look at general technology best practices that are not specific to any vendor.

Security 101: Starting Security Communication Tips

- How the message is delivered matters.
- Follow what you tell others when it comes to privacy and security.
- Look at privacy and security as an educational opportunity for everyone.
- Delineate between best practices and regulations.
- When in doubt ask other security folks for help.

Security 101: General Reminders for Starting Security

- Finding the optimal balance between security and business operations can be difficult.
- This isn't something you can ever complete, but rather it’s a never-ending practice.
- Mundane but important tasks or behaviors can be easily neglected.
- Things don’t have to be complex to work.
- Everyone starts their journey somewhere.

Closing Thought

In the end many people are looking for a silver bullet when it comes to privacy and security. Just remember you are not only fighting werewolves.

Informational Slides

NC DHHS Privacy and Security Policies :
https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/

NC State Security Standards:
https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies

The DHHS Privacy and Security Awareness Hub (Information and Training):
https://www.ncdhhs.gov/about/administrative-offices/privacy-and-security/dhhs-privacy-and-security-awareness-hub

DIT Artificial Intelligence Resource Page:
https://it.nc.gov/resources/artificial-intelligence

Next Meeting Planned for October 9, 2025

Questions