NC Department of Health and Human Services

Information Technology Division
Privacy and Security Section

April 10, 2025

The DHHS Privacy and Security Section

- The Privacy and Security Section (PSS) provides privacy and security information for the Department of Health and Human Services (DHHS). The PSS safeguards information from unauthorized use, disclosure, modification, damage or loss.
- The PSS 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 PSS serves as the liaison between various Federal and State Agencies.
- The PSS is responsible for conducting annual reviews based on Federal and State requirements.

Understanding the Security CIA Triad

- **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.

Common Privacy Threats and Best Practices for Privacy

Common Privacy Threats:

- **Data Breach**: incident that occurs when an unauthorized person views, alters, or steals secured data.
- **Phishing Attacks**: Fraudulent attempt to obtain sensitive information (e.g., user credentials) by impersonating a legitimate entity or individual through email, messaging apps, or websites.
- **Social Engineering**: Exploits human psychology to obtain confidential information or unauthorized access.

Best Practices:

- Enable two-factor authentication (2FA) wherever possible.
- Regularly review and update privacy settings on social media and applications.
- Exercise caution when disclosing personal information on the internet.
- Encrypt data at rest and in transit

Common Security Threats and Best Practices for Security

Common Security Threats

- **Third-Party Exposure**: Organizations increasingly rely on third-party relationships. Third-parties must follow security best practices and standards and be compliant with Federal and State regulations.
- **Cloud Vulnerabilities**: Security weaknesses and risk factors associated with cloud computing environments.
- **Social Engineering**: A tactic to bypass technological defenses by exploiting human psychology.
- **Malware & Ransomware:** Malicious software designed to steal data or hold it hostage in exchange for ransom. loss of data, system downtime, financial loss, and reputational harm.

Best Practices for Security

- Keep all software including operating systems and applications, updated.
- Use reputable antivirus and anti-malware software.
- Regularly back up data to secure locations.

Understanding Security Controls

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

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.

Organizational Cybersecurity Hygiene

- Cybersecurity hygiene, is a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data. *-TechTarget*
- Finding the optimal balance between security and business operations can be difficult.
- Cybersecurity hygiene isn't something you can ever complete, but rather it’s a never-ending practice mundane but important tasks or behaviors that can be easily neglected.

Organizational Cybersecurity Hygiene Best Practices

- Control access both privileged and nonprivileged.
- Harden hardware and control software.
  - Deactivate any enabled resource that are not needed for the purpose of system.
  - Ensure only authorized software is installed on systems.
  - Remove any unneeded software.
- Keep policies and procedures updated and review on an annual basis.
- Educate and remind users of their legal and shared security responsibilities.

Continuity of Operations Planning

- Ensures that critical business operations can continue even in the event of a disruption, degradation, or disaster such as:
  - Cyber attacks or incidents
  - Natural disasters or localized emergencies
  - Technology service outage
- Is comprised of 4 phases:
  - Readiness and Preparedness
  - Activation and Relocation
  - Continuity Operations
  - Reconstitution

Continuity of Operations Planning Pain Points

These are the top 5 things we often see missing from plans.

- Delegations of Authority
- Vital Records Management
- Human Capital Planning
- Devolution of Control and Direction
- Reconstitution

Insider Threat

- Insider: person(s) who has or had authorized access to or knowledge of an organization's resources. E.g., personnel, facilities, information, equipment, networks, and systems.
- An Insider Threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.
- Due to the access and organizational knowledge Insider Threats pose a complex and dynamic risk.

Key actions to mitigate Insider Threats:

- Identify systems and data vulnerable to Insider Threats.
- Introduce Insider Threat focused training and education efforts.
- Understand and monitor user behavior.
- Identify insider threats.

Social Engineering

- Social engineering is the use of deception, manipulation, or influence to get individuals to divulge confidential or personal information that may be used for fraudulent purposes.
- Social engineering attacks can be complex and contain multiple parts.
- Phishing, Tailgating, Scareware, Dumpster Diving, and Quid Pro Quo are all types of social engineering attacks.
- Attacks often include posing as a trusted brand, or authority figure; are designed to appeal individuals to helpfulness or curiosity; and are designed to induce fear or a sense of urgency in the victim.

Key actions to mitigate Insider Threats:

- Destroy sensitive documents regularly.
- Avoid plugging an unknown USB into your computer.
- Clean up your social media.
- Don't open email attachments from suspicious sources.
- Be wary of tempting offers.

Cloud Considerations

Cloud security controls are a set of measures designed to protect cloud environments, and the data stored and processed within them from security risks, unauthorized access, and data breaches.

- Cloud (cloud computing) is a platform for delivering services (e.g., storage, software applications, processing). This environment allows for on-demand network access to a shared pool of configurable computing resources (e.g., networks and servers) provisioned and released with minimal management effort or interaction from the Cloud Service Provider (CSP).
- Cloud platforms may fall under the Cloud Shared Responsibility Model.
- Many of our existing Privacy and Security Requirements are technology agnostic and the environments, to the cloud without specifically identifying it.
- special considerations are needed when utilizing cloud services.
- Cloud provides have their own version of common services specific to their cloud environment.

Artificial Intelligence (AI) Considerations

- Artificial intelligence (AI) is a set of technologies that enable computers to perform a variety of advanced functions. E.g., the ability to perceive, understand and translate the spoken and written language, analyze data, make recommendations, and more.
- AI is becoming one of the fastest adopted technologies.
- AI regulations will rapidly evolve for the foreseeable future.
- Many of our existing Privacy and Security Requirements are technology agnostic (designed to be compatible with or independent of specific technologies) and therefore applies to AI without specifically identifying the technology.
- The Department of Information Technology (DIT) AI Corner https://it.nc.gov/programs/privacy-data-protection/artificial-intelligence.
- State has hired its first AI Governance and Policy executive

SSA Triennial Assessments

Social Security Administration (SSA) - Security Assessment Plan (SAP) was developed to document the plan to assess the Organization's baseline and tailored security controls. The objective of the SAP is to define and document for an Organization, a series of security test and assessment procedures in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Rev 5 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The Organization will be assessed by SSA personnel, supported by an independent third-party assessor organization

Performed only on divisions/offices with the SSA data: NCFAST, NCTracks, and the Employment and Independence with People with Disabilities (EIPD)

IRS Triennial Assessments

Internal Revenue Service (IRS) - **IRS Publication 1075** outlines the requirements for **Safeguarding Federal Tax Returns and Return Information**. This publication is primarily aimed at entities that handle federal tax information (FTI) and provides detailed guidelines on the protection, security, and management of such sensitive data. IRS calls for Security Assessment review based on IRS 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf

Compliance with IRS 1075 is required for Child Support

Performed only on divisions/offices with the IRS FTI data: NCFAST, NCTracks, Employment and Independence with People with Disabilities (EIPD) and counties

Biennial Security Reviews

The Biennial Security Review is in accordance with the United States Department of Agriculture 7 CFR 277.18 (m)

- Conducted on North Carolina (NC) DHHS divisions/offices with the Internal Revenue Service (IRS) Federal Tax Information (FTI), and Social Security Administration's (SSA) data. This is including all the ADP projects under the development and the operational systems involved in the administration of the Health and Human Services (HHS) programs.
- The review is scheduled to complete biennially at the end of September of every other year. The next one is in the year 2026 and must be completed by September.

Biennial Security Reviews

Security review pertains to the following areas:

- Physical security of EDP resources
- Equipment security
- Software and data security
- Telecommunications security
- Personnel security
- Contingency planning
- Emergency preparedness

PSS willl select two or three counties for review and all findings are remediated by the counties

Incident Management Basics: Security

Security Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices, event where an information technology resource is accessed or used without authorization. In summary, an attack against an information asset that poses a clear threat to the Confidentiality, Integrity, or Availability (CIA) of information.

Examples of security incidents:

- Unauthorized attempts (failed or successful) to gain access to a State owned, operated, and managed system or its data.
- Intentional or unintentional disruption of processing capability or denial of service (DoS) attacks.
- Changes to system hardware, firmware, or software configurations without appropriate agency approval.
- Malicious logic (virus, worm, Trojan horse) attacks.
- Attempted or actual instances of social engineering.
- Unauthorized network scans or probes.

Incident Management Basics: Privacy

Privacy Incidents

- An adverse event that occurred due to a violation of the organizational or regulatory privacy policies and procedures.
- Event that results in, or could result in, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or terms referring to situations where persons other than an authorized user or where there is an authorized purpose have access or potential access to Personally Identifiable Information (PII) or Protected Health Information (PHI), whether physical or electronic.

Examples of privacy incidents include:

- Employee access sensitive personal data without proper authorization.
- Failure to redact personal data.
- Device with unencrypted data is lost or stolen.
- Sending medication record to the wrong patient, none compliance with HIPPA.

Incident Management Basics: Breach

Data Breach

- Incidents that meet specific legal requirements and involve data loss.
- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an unauthorized purpose.
- Breach typically requires the obligation to notify affected individuals.
- Social Security Administration requires to report the breach or an incident within 60 minutes.
- IRS requires to report the breach or an incident within 24 hrs. minutes
- NC State Requires to report to State CIO within 24 hrs.

Examples of data breach:

Social engineering, results in the disclosure of information to unauthorized individual.

unauthorized access and theft of sensitive data.

Human error that results in accidentally exposing sensitive data.

Insider threat accidental or malicious.

Cybersecurity Considerations for Counties

- Report cyber security incidents immediately to the DHHS Privacy and Security Section (PSS) at https://security.ncdhhs.gov.

- In the event of a network incident provide us MiFi \ FirstNet IP addresses to NCDHHS ASAP. This will ensure county access to DHHS applications is provided while the county is offline (WIC, Child Support, OLV etc.).

- Once cyber events are remediated, provide the PSS an attestation stating what remediation steps were taken and the network is secure, as we may need to provide this to our Federal partners (Child Support, IRS, SSA). This will allow us to open access back to your network.

- Printers MUST be secured and behind the firewall. Use ACLs to allow only the state mainframe access through the firewall.

- Run external and internal vulnerability scans to identify vulnerabilities. The county IT Strike Team lead by Shannon Tuffs can provide scans for you. You can contact them via: https://www.nclgisa.org/page/strike-team.

- Ensure you patch management process is current and all critical and high vulnerabilities are patched.

- Replace end of life hardware and software.

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 May 8, 2025

Questions