Acceptable Use for DHHS Information Systems Summary Presentation

This presentation is not required training. It provides a summary reminder of what is contained in the DHHS Acceptable Computer Use Policy and does not replace it. All users MUST review and acknowledge the policy. The policy is available at either:

https://www2.ncdhhs.gov/info/olm/manuals/dhs/pol-80/man/12acceptable_use1.htm

or

https://publichealth.nc.gov/employees/dphit/security.htm.

Acceptable Use for DHHS Information Systems

- All DPH employees and extended workforce (e.g., contractors) who have access to DPH computer systems and electronic data must:
  - Read the Acceptable Use for DHHS Information Systems Policy.
  - Acknowledge that they have done so by signing the User Certification of Notification and Agreement of Computer Use Policy, which is included at the end of the policy.
  - Follow the measures described in the policy when using state information systems.
- All users must agree to use the state's computer systems responsibly to conduct government business according to the terms in the acceptable use policy.

Definition of DHHS Information Systems

DHHS information systems include:

- All platforms (operating systems).
- All sizes (from PCs, laptops and PDAs up to mainframe computers).
- All equipment (telecommunications, printers, electronic facsimile).
- All applications (developed in-house and purchased).
- All data residing in the information systems or derived from them (e.g., screen displays, reports).

User Access Responsibilities

- All information systems to which users are given access are to be used only to conduct the activities authorized by the Department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the Department or on its behalf.

- The unauthorized use or disclosure of information provided by these information systems may constitute a violation of state and/or federal laws and DHHS policies, which may result in disciplinary or legal action consistent with state personnel policies.

Information Ownership

The Department and its Divisions/Offices retain the rights of ownership to all information system resources including hardware, software, functionality, data, and related documentation developed on behalf of the Department. All Department information system resources remain the exclusive property of the State of North Carolina and/or the Department, unless otherwise prescribed by contractual agreements.

Use of the NC Integrated Information Network and the Internet

While in performance of work-related functions, while on the job, or while using publicly owned or provided information processing resources, DHHS users are expected to use the NC Integrated Information Network (NCIIN) and the Internet responsibly and professionally. Users shall make no intentional use of these services in an illegal, malicious, or obscene manner as described in NC General Statute (GS) 14-190.1.

Use of the NC Integrated Information Network and the Internet (cont.)

- Users may make reasonable personal use of the NCIIN or Internet resources as long as:
  - The direct measurable cost to the public is none, is negligible, or access supports the mission of the agency;
  - There is no negative impact on user's performance of public duties;
  - The policy is applied equitably among all personnel of the agency;
  - Users may be required to reimburse the agency if costs are incurred that do not have prior approval by the Agency or Division/Office.

Use of the NC Integrated Information Network and the Internet (cont.)

- When sending or forwarding e-mail over the NCIIN or the Internet, users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law.
- Users are responsible for protecting DHHS sensitive information by following DHHS and DPH policies and procedures.
- Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via NCIIN and the Internet is accurate. Users shall provide the date information was current and an e-mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.

Use of the NC Integrated Information Network and the Internet (cont.)

- Users shall avoid unnecessary network traffic and interference with other users:
  - Unsolicited commercial advertising by DHHS Users. Such use is strictly forbidden.
  - Use of computer resources, including e-mail, to conduct any activities already prohibited by the Office of State Personnel or other DHHS policies (such as private/personal fund raising, political activities, etc.) shall be prohibited.
  - Mass emailing by public employees and NCIIN users that do not pertain to governmental business is prohibited.
  - Users shall not stalk others; post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, a civil liability, or violation of any applicable law.

Use of the NC Integrated Information Network and the Internet (cont.)

- Users shall not access or attempt to gain access to any computer account (or any portions of the NCIIN network) to which they are not authorized. Users shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.
- Users given access to which they are not privileged or entitled are required to report the circumstances immediately to their supervisor. Supervisors are responsible for determining a user's appropriate access rights. Contact DPH LAN Support to request changes to a user's access rights: **919 707-5160.**

Workstation Security

- Requirements apply to office, home or other remote access locations if utilized for DHHS business:
  - Sensitive information on paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, or behind locked doors, especially outside working hours.
  - Personal computers and computer terminals should not be left logged on when unattended or not in use. Personal computers or computer terminals shall be protected from unauthorized access by physical, technical, or administrative controls.
  - Classified or sensitive information should not be printed on a printer located in public areas. However, in the event that public printers must be used to print sensitive or classified information, such information shall be cleared from printers immediately.
  - Users must follow statewide IT Desktop and Laptop Security standards, which are posted at: https://publichealth.nc.gov/employees/dphit/security.htm.

Media Storage

- Classified information stored on external media (e.g., diskettes or CDs) must be protected from theft and unauthorized access. Such media must be appropriately labeled as classified information.
- The use of removable storage devices or external devices (e.g., USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user's supervisor in writing and specify the intended use of the device.
- Mobile computing devices and removable storage devices (e.g., laptops, PDAs, USB flash drives, etc.) must never be left in unsecured areas and their use must meet DHHS Security Standards. Any incidents of misuse, theft or loss of data must be reported to the supervisor and to the Division Privacy and Security Official (Larry Forrister).
- Sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor/manager. Users shall follow appropriate physical safeguards for offsite use.

System Activity Review

- User Privacy – Monitoring of Use
  - Any activity conducted using the State's computers, including E-mail and the use of the Internet, may be logged, monitored, archived or filtered, either randomly or systematically.
  - All network accounts and workstation hard drives are subject to periodic audit for the purpose of maintaining security and license requirements.
  - Both DHHS and the Division reserve the right to perform these actions without specific notice to the user.

Software License Agreements

- The theft of computer resources, including computer software, is illegal. All computer software, including software obtained from sources outside the Department, is subject to license agreements that may restrict the user's right to copy and use the software. Software distributed on a trial basis, even through the Internet, does not suggest that the software is free or that it may be distributed freely.

- The Department does not require, request, or condone unauthorized use of computer software by its employees, volunteers, and contractors. Federal Public Law 102-561 strictly prohibits any violation of copyright protection. Violation of copyright protection is considered a felony and is punishable by up to five years in prison and/or fines up to $250,000 for all parties involved.

Computer Viruses – Malicious Code

- It is the responsibility of each user to help prevent the introduction and spread of computer viruses and other malicious code. All personal computers in the Department must have virus detection software running at all times.

- All files received from any unknown source, including those on storage media and electronically downloaded or received as e-mail attachments, must be scanned for computer viruses before opening or using the files.
- Users should immediately contact their DPH LAN Support at **919 707-5160** immediately if they suspect a virus or other malicious code so the appropriate actions can be determined and taken.

Installation of Hardware & Software

- DHHS information system hardware and software installations and alterations are handled only by authorized DHHS/DPH employees or contractors. Users shall not install information system hardware or software.

- Users shall not download software from the Internet unless specifically approved by the user's supervisor and the designated IT personnel. Downloading audio or video stream for a work-related webinar or audio conference is permissible without prior authorization.

Remote Access

- Authorized users of DHHS's computer systems, networks and data repositories may be permitted to connect remotely to conduct state-related business. Users will be granted remote access only through secure, authenticated and managed access methods.

- Users shall not access agency networks via external connections from local or remote locations, including homes, hotel rooms, wireless devices, and off-site offices without knowledge of and compliance with the User Access Responsibilities summarized on slide 5 earlier in this presentation.

Employee Sanctions

- Disciplinary and Legal Actions
  - Intentional violation of the terms of the Acceptable Use for DHHS Information Systems policy and inappropriate access/use/disclosure of confidential health information can result in disciplinary and/or legal action.
  - DPH will follow State Personnel procedures and work with NC DHHS Human Resources regarding any potential disciplinary actions.

QUESTIONS?

If you are ever in doubt about anything related to HIPAA and DPH security (or privacy), **always** ask your supervisor or the DPH Security and Privacy Official!

HIPAA.DPH@dhhs.nc.gov