Privacy Basics for South Carolina Enterprise Information System (SCEIS) Users

Enterprise Privacy Office

admin

THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

ABOUT THIS PRESENTATION

- The purpose of this presentation is to provide employees who conduct transactions in SCEIS on behalf of their Agency, with an overview of privacy principles and safeguards.

- This presentation will
  - Describe what ‘privacy’ means, why it is important, and how it is different from security;
  - Describe how privacy requirements are determined; and
  - Describe privacy principles and best practices that should guide the handling of personally identifiable information and other sensitive information.

The information provided in this presentation should be supplemented at the Agency level to address privacy responsibilities connected to the employee’s specific job duties.

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

UNDERSTANDING PRIVACY

What Is Privacy?

Privacy, in the context of this presentation, means **information privacy**…

- Empowering individuals by giving them notice about how the State will use their information;
- When possible, providing individuals with choices regarding the collection, use, and sharing of their information; and
- Applying appropriate administrative, technical and physical safeguards to protect personal information.

Information Privacy in State Government

- State government agencies and institutions provide essential services, such as education, public safety, and healthcare, to citizens.

- To receive these essential services, individuals are usually required to provide very personal information to the State.

- State employees have specific legal and ethical obligations to protect the privacy of our citizens.

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Privacy & Security: What's the Difference?

PRIVACY	SECURITY
Determines - The types of information that need to be protected; - The laws, regulations, and policies that mandate the protection; and - Who should, or should not, have access to the information.	Determines - The technological mechanisms necessary to implement protections.
Focuses on the policies and business processes that help to ensure legal and ethical obligations are upheld.	Focuses on the technology that enforces appropriate protections.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

Think About It Like This …

SECURITY creates the vault.

Bank vault-style door (closed) to hallway from within vestibule. Facing southeast. - Travis Air Force Base, Building No. 925, W Street, Fairfield, Solano County, CA http://hdl.loc.gov/loc.pnp/hhh.ca2282/photos.324711p

PRIVACY identifies what goes inside the vault, whether some vault contents need to also be placed inside lockboxes, and who gets the vault combination and/or lockbox keys.

“Records in Humidifying Vault” photo by Jackie Martin, International News Photos, 1946. National Archives 64-NA-466. Accessed at http://blogs.archives.gov/prologue/?p=14739

What Information Needs to be Protected?

In general, special protections are placed around Personally Identifiable Information, or 'PII'.

- PII is information that, whether alone or when combined with other information, is linked or linkable to a specific individual. (''Linked'' and ''linkable'' refer to the ability to make a logical association between different sets of information.)
- PII includes information that is kept in electronic, as well as paper-based, format.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

What Information Needs to be Protected? (contd)

- Non-PII can become PII when seemingly harmless pieces of information, when combined, could be used to identify an individual. This is sometimes referred to as the ‘mosaic effect’. For example,
  - Date of birth and mother’s maiden name are commonly used to verify identity
  - Persons residing in zip codes with small populations may be easily identifiable based on just age and ethnicity
- Privacy risk assessments require a case-by case assessment

Examples of PII

Stand-alone data elements		
Social Security Number	Personal Email Address	Personal Bank Account Number
Name	Credit Card Number	Driver’s License Number
Tax Identification Number of a sole proprietor	Passport Number	State Identification Card Number
Information about an individual that is linked, or linkable, to one of the above		
Place of birth	Race	Religion
Medical information	Education information	Financial information
Geographical indicators, e.g. zip code	Employment Information	Date of Birth

Specific Privacy Mandates

A multitude of laws and regulations dictate how, and under what circumstances, certain information must be protected.

Examples of Specific Privacy Mandates	
Health-related data	• Health Insurance Portability and Accountability Act (HIPAA)
Financial data	• Gramm-Leach-Bliley Act (GLBA)
Educational data	• Federal Educational Rights and Privacy Act (FERPA)
Marketing Data	• Telephone Consumer Protection Act
Workplace Data	• Americans with Disability Act (ADA)

Privacy & Other Types of Sensitive Information

Additionally, business considerations may require that special protections be placed around other sensitive information.

- Trade Secrets
- Security Plans
- Training materials
- Network Architecture

- Information received from, and/or about, a business, such as procurement proposals, or business financials.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

PRIVACY BEST PRACTICES

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

With so many laws, regulations, and rules to follow, how can I best protect data when making business decisions?

CJIS

HITECH

HIPAA

GLBA

PCI DSS

IRS Pub 1075

FTI

PHI

PII

FERPA

FPPA

FOIA

SC Code Section 1-11-490

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Privacy Principles

As a State Agency or institution it is important to take privacy principles into account before collecting data from individuals.

1) **Notice and Transparency** – Inform the individual about what personal information is being collected and how it will be used and shared. Use clear and plain language in these communications. These communications are sometimes referred to as ‘providing notice’.
2) **Individual Participation, Access and Redress** – Whenever possible, allow individuals to choose how their personal data will be used and/or shared. Provide individuals with procedures on how to access, and correct or update information being held about them.

Privacy Principles (contd)

3) **Data Minimization and Retention** – Collect only the information needed to perform a job function. Keep data only as long as necessary to fulfill the business purpose, and dispose of data in accordance with Agency data retention schedules.

4) **Use and Disclosure Limitation** – Use and disclose data only in the manner described in the notice provided to the individual, unless

   - the individual consents to the additional use, or
   - the individual requests that the data be used in that way, or
   - law or regulation require additional uses of that data.

Privacy Principles (contd)

5) **Data Quality and Integrity** – Establish procedures to ensure data remains accurate, complete, and up-to-date.

6) **Security** – Implement technical safeguards to protect data against unauthorized access, use, distribution, modification, and/or disclosure.

7) **Accountability and Auditing** – Institute policies and procedures that assign information protection roles and responsibilities. Establish systems for evaluating compliance, effectiveness, and improvements.

General Privacy Best Practices

As an employee with access to sensitive data, consider these general privacy best practices as you perform your daily job functions.

GENERAL PRIVACY BEST PRACTICES
Paper Records

- If you do not need a hard copy of a document, consider keeping the document in electronic format only.

- If you need only one official hard copy of a document, do not make extra convenience copies.

- Avoid distributing hard copies of documents whenever possible.

- Dispose of documents in accordance with Agency retention schedules. Use a locked shred bin or approved shredder when disposing of hard copies.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

GENERAL PRIVACY BEST PRACTICES
Paper Records (contd)

- Store sensitive documents in a secure location at the end of each workday. A secure location is an environment that is protected and accessible only to authorized individuals. In an open work space, a secure location can be a locked desk or locked cabinet.
- Never leave sensitive paper documents unattended in a public place, such as a lunchroom, restroom or unsecured conference room.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

GENERAL PRIVACY BEST PRACTICES
Copiers

- Follow your Agency's policies regarding copier use. Generally, you should have no expectation of privacy when using a work copier.
- If you are copying sensitive information, stay in the copier area during the work process so that you will be able to immediately collect the original and copies after the job is complete.
- Do not email copies of sensitive information directly from the copier/scanner to recipients. Send the information to your email address through a secure method, and review the copies/scanned documents before forwarding.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

GENERAL PRIVACY BEST PRACTICES
Fax Machines

- Do not leave sensitive documents on a fax machine. Immediately remove the original documents from the machine after sending a fax.
- Ask to be alerted in advance if a sender plans to fax sensitive information to you.
- Prior to sending a fax, contact the intended recipient. Let the recipient know that you are sending a fax, and request that it be retrieved promptly.
- If possible, use an electronic fax to protect the privacy of sensitive information. Using a fax cover sheet with a confidentiality disclaimer on it will also provide your contact information in the event the recipient needs to contact you.

GENERAL PRIVACY BEST PRACTICES
Emails

- Follow your Agency's policies and procedures when sending sensitive information through email. To the greatest extent possible, limit sensitive information that you send through email.
- Do not open unknown links in emails without confirming with the sender the validity of the links.
- Consider the use of a confidentiality disclaimer on both outgoing and reply emails.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

GENERAL PRIVACY BEST PRACTICES
Passwords

- Do not share your password.
- Follow Agency guidance regarding setting and changing passwords.
- Do not keep a “sticky” with your password information where others may find it.
- Do not create easily identifiable passwords like pet names, favorite teams, names of family members, and birth dates.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

GENERAL PRIVACY BEST PRACTICES

Traveling or Working from a Remote Location

- Lock your computer whenever you leave your work space.
- Do not leave laptops, or documents containing sensitive information, in checked luggage.
- Do not leave sensitive information in your vehicle.
- Do not leave sensitive information in a hotel room.
- Do not access work email or other sensitive documents through open Wi-Fi systems.

GENERAL PRIVACY BEST PRACTICES
Privacy and Physical Security

- Do not discuss sensitive information in unsecured areas, such as restrooms, hallways, or elevators.
- Do not discuss sensitive information a speakerphone if unauthorized persons may be able to hear the discussion. Consider asking for a roll call of participants.
- If possible, do not leave voicemails containing sensitive information. Be sure to obtain prior written permission from the recipient before leaving any voicemail.
- Follow Agency procedures for verifying callers before discussing sensitive information with a caller you do not know.

GENERAL PRIVACY BEST PRACTICES
Incident Reporting

- If you suspect, or become aware of, unauthorized access to, or use of, sensitive information, follow your Agency's incident reporting protocol. If in doubt about how to report incidents, contact your supervisor immediately.
- Reporting suspected and actual incidents
  - helps the State improve privacy and security safeguards;
  - is essential to effective incident response; and
  - is a responsibility of every user granted access to State data.

admin
THE SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

SCEIS PRIVACY POINTERS

As an employee performing SCEIS transactions on behalf of your Agency, there are best practices that deserve heightened awareness.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

SCEIS PRIVACY POINTERS

Limit Access

- Review access privileges, at least annually, to ensure staff have access to only the SCEIS modules necessary to fulfill their job functions.

- Institute procedures to remove or adjust SCEIS access privileges when staff transfer to different roles, switch agencies, or terminate employment.

- Only share information with staff who have an authorized business need-to-know. Ensure role assignments are in compliance with the SCEIS segregation of duties policy found at http://sceis.sc.gov/page.aspx?id=306.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

SCEIS PRIVACY POINTERS
Scrutinize Attachments

Attachments may contain PII. Ask the question(s).

- What is the data classification category of the document being uploaded? Have you confirmed that SCEIS is configured to provide the appropriate security for data with that classification?

- Is the document required to process the transaction? If the document is required, can the PII be redacted and still serve its purpose in the transaction?

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

SCEIS PRIVACY POINTERS
Scrutinize Attachments (contd)

Attachments may contain PII. Ask the question(s).

- Can the social security number and/or credit card number be redacted?
- When requesting the reclassification of a previous transaction, rather than reattaching the supporting documentation from the original transaction, why not simply reference the original transaction number?

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

SCEIS PRIVACY POINTERS
Scrutinize Attachments (contd)

Attachments may contain PII. Ask the question(s).

- To provide verification of a closed account, rather than uploading a canceled check, why not upload a report or letter from the bank indicating the account has been closed?
- Some forms have been updated to remove the SSN field. Are you sure you're using the most current version of the form?

SCEIS PRIVACY POINTERS
Implement Retention Schedules

- Do not use SCEIS as a repository for historical records. Upload documents for the purposes of completing a SCEIS transaction only.

- Adhere to retention schedules and Agency policy regarding the archiving and destruction of paper and electronic data. Contact the SC Department of Archives and History http://scdah.sc.gov/Pages/default.aspx if your Agency needs assistance.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

SCEIS PRIVACY POINTERS
Beware of Using "Free Text" Fields

- Avoid putting PII in free text fields.

- Use the pre-set data fields to update and correct information.
  - Using free text boxes, instead of updating pre-set data fields, threatens data quality.
  - Reports, calculations, and statistics may not capture information in free text boxes.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

TAKEAWAYS

KEY TAKEAWAYS FROM THIS PRESENTATION

- Information privacy is about allowing individuals to make informed decisions about how their information is used and shared.
- Privacy determines what information should be protected. Security is one of many mechanisms for protecting data.
- It is every State employee's responsibility to protect the privacy of our citizens' information by applying appropriate administrative, technical and/or physical safeguards.
- Agency policies, procedures and decision making should incorporate privacy protection principles and best practices.

admin

THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

Enterprise Privacy Office

http://admin.sc.gov/technology/enterprise-privacy

privacyoffice@admin.sc.gov