#### National Archives and Records Administration

Federal Records Management Level 1: Maintenance and Use

Participant Guide

Module 7:

Identify Privacy Concerns Related to Records’ Use and Storage

Table of Contents

[Module 7: Identify Privacy Concerns Related to Records’ Use and Storage 3](#_Toc22884248)

[Module 7 Checklist 3](#_Toc22884249)

[Live Class Session 7: Identify Privacy Concerns 4](#_Toc22884250)

[Introduction – Notes 4](#_Toc22884251)

[Task Goal 4](#_Toc22884252)

[Task Objectives 4](#_Toc22884253)

[Privacy Act Basics – Notes 5](#_Toc22884254)

[A “record” under the Privacy Act 5](#_Toc22884255)

[Security Controls 6](#_Toc22884256)

[Administrative Controls 6](#_Toc22884257)

[Technical Controls 6](#_Toc22884258)

[Physical Controls 6](#_Toc22884259)

[Reporting Risks 7](#_Toc22884260)

[Practice: Breaches – Scenario 1 7](#_Toc22884261)

[Practice: Breaches – Scenario 2 8](#_Toc22884262)

[Practice: Breaches – Scenario 3 9](#_Toc22884263)

[Consequences of Privacy Breaches – Notes 10](#_Toc22884264)

[Activity: Privacy Concerns – Scenario 1: On the Web 10](#_Toc22884265)

[Activity: Privacy Concerns – Scenario 2: Supervisor Notes 11](#_Toc22884266)

[Activity: Privacy Concerns – Scenario 3: Records Clean-Up Day 12](#_Toc22884267)

[Module 7 Assignments 13](#_Toc22884268)

[Module 7 – Notes 14](#_Toc22884269)

# Module 7: Identify Privacy Concerns Related to Records’ Use and Storage

## Module 7 Checklist

* Complete this online module.
* Your homework following the live class session is to:
* Find your agency’s guidance related to the Privacy Act. What systems and types of information are mentioned?
* Identify the types of information in your office that are subject to the Privacy Act.
* Identify the points of contact in your agency who could help you identify and address privacy concerns.

# Live Class Session 7: Identify Privacy Concerns

## Introduction – Notes

## Task Goal

Given a set of records, you will be able to address privacy issues related to Privacy Act records.

### Task Objectives

* Discuss the consequences of privacy breaches
* Describe privacy concerns to your Privacy Officer and Records Liaison Officer (RLO)

## Privacy Act Basics – Notes

## A “record” under the Privacy Act

Any item, collection, or grouping of information about an individual that is maintained by the Department and that contains the name, or an identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. The record may include, but is not limited to, the individual's education, financial transactions, medical history, and criminal or employment history.

## Security Controls

### Administrative Controls

* Training and awareness
* Disaster preparedness and recovery plans
* Records management
* Personnel management
* Policies and procedures

### Technical Controls

* Encryption
* Smart cards
* Strong passwords
* Access control lists (ACLs)

### Physical Controls

* Locked cabinets and rooms
* Selecting secure destruction methods for sensitive records
* Regular inspections
* Security guards
* Picture IDs

## Reporting Risks

Follow agency guidance

Inform your supervisor, Privacy Officer and Records Liaison Officer immediately

## Practice: Breaches – Scenario 1

**Personal data for more than 134,000 sailors was breached, Navy says**

By: David B. Larter, Navy Times, November 23, 2016

 "The personal data of more than 130,000 sailors in a re-enlistment approval database was stolen from a contractor’s laptop, the Navy disclosed Wednesday.

The Navy was notified in October by Hewlett Packard Enterprise Services that a computer supporting a Navy contract was “compromised,” and that the names and social security numbers of 134,386 current and former sailors were accessed by unknown persons, the service said in a news release.

The Naval Criminal Investigative Service is in the early stages of investigating the breach, but in a release said it hasn’t found any malicious use of the data yet.

“The Navy takes this incident extremely seriously -- this is a matter of trust for our sailors," said Navy personnel boss Vice Adm. Robert Burke in a statement. "We are in the early stages of investigating and are working quickly to identify and take care of those affected by this breach."

A Navy official familiar with the investigation said the personal data came from the Career Waypoints database, known as C-WAY, which sailors use to submit re-enlistment and requests to change Navy Occupational Specialties."

## Practice: Breaches – Scenario 2

**IG: IRS Employees Sent Unencrypted Emails Containing Personal Data of** Thousands of Taxpayers. Ian Smith, FedSmith.com, November 20, 2016

“A recent report from the Treasury Inspector General for Tax Administration (TIGTA) found that IRS employees sent unencrypted emails which contained 8,031 different taxpayers’ personally identifiable information.

According to the report, TIGTA found 326 unencrypted emails containing taxpayer data. 275 of the emails were sent internally within IRS, while 51 emails were sent outside of the agency’s network to non-IRS email accounts. Of those emails sent externally, 20 were sent to six IRS employees’ personal email accounts.

The significance of where the emails were sent is relevant to the level of the security risk to the taxpayer data. The report noted that unencrypted emails sent within the IRS internal network were of lower risk because they remained behind the agency’s firewalls which greatly lowers the probability they could be accessed by a third party. However, the emails sent outside of the agency were exposed to greater risk, not only because they were not encrypted, but because they no longer had the protection afforded by the firewall.”

## Practice: Breaches – Scenario 3

**‘Inadvertent’ Cyber Breach Hits 44,000 FDIC Customers**

By Joe Davidson, Washington Post, April 11, 2016

In yet another example of fragile security in federal cyber systems, data for 44,000 Federal Deposit Insurance Corp. customers were breached by an employee leaving the agency.

The breach was outlined in an internal FDIC memorandum obtained by The Washington Post. The March 18 memo said the data were downloaded to a personal storage device “inadvertently and without malicious intent. The FDIC’s investigation, the memo said, does not indicate that any sensitive information has been disseminated or compromised.”

Calling the breach “troubling,” Barbara Hagenbaugh, an FDIC spokeswoman, said “the potential for a breach is especially heightened when sensitive information for over 44,000 individuals is stored without proper security measures.” The incident indicates a serious breach can result from a simple mistake and does not have to be a deliberate cyber theft.

The former employee, who was not identified, left FDIC on February 26 with the personal storage device. Using technology to track downloads to removable devices, FDIC detected the breach on February 29 and the employee returned it the next day. Hagenbaugh said the agency has eliminated the use of portable storage devices for most employees and plans to do that for others. Some of the affected data included names, addresses and Social Security numbers.

## Consequences of Privacy Breaches – Notes

## Activity: Privacy Concerns – Scenario 1: On the Web

You work with your agency’s grants program. In an effort to be more transparent about its use of tax dollars, the agency has decided to post information about the grants it has awarded to the agency website.

You know that your agency’s grants program gives each grant a 15-digit tracking number that is made up of the fiscal year and month of application plus the grant recipient’s 9-digit Social Security number. There is a database that includes the tracking number, the full name of the recipient, contact information (mailing address, physical address, email address, phone number, social media accounts and website, if provided) for the recipient, a brief description of the grant project, and the dollar amount awarded under the grant.

Your supervisor wants to demonstrate how quickly your team can deliver results, so he directs you to work with the Web Program at your agency to post the entire database on your agency website as soon as possible.

He says that by law, the names of grant recipients and the amounts received are public information, so there shouldn’t be any problem.

Do you have some concerns about this project? Think about what you would do in this situation.

## Activity: Privacy Concerns – Scenario 2: Supervisor Notes

As the new Records Contact for your division, you are visiting program offices to get a sense for how records management is working in each office.

An administrative assistant to one of the division managers tells you that there are some files stored in an unlocked file cabinet in the hallway. The bottom drawer of one cabinet contains a number of files on former employees who have left the agency.

The files contain correspondence, notes, employee addresses, notes about the employee’s family members and birthdays, notes about employee performance, and other information from a manager who says she wants to keep the information “just in case” she might need it at a future date. The manager stored the files in the cabinet in the hallway because her own desk is full.

The drawers of the unlocked cabinet are not labeled, and the manager thought no one would look in there because the lack of a label made it look like the drawer was empty. (In fact, the assistant discovered the files while looking for storage space.)

Current agency policy mandates the transfer of unofficial personnel folders to HR upon departure of the employee and mandates storage of current files in a restricted part of the network or in locked file cabinets.

What are the possible records privacy concerns arising from this situation?

How can you address these concerns?

## Activity: Privacy Concerns – Scenario 3: Records Clean-Up Day

Your office is having its annual records clean out campaign this week. Records custodians are busy identifying records with expired retention periods that are eligible for immediate disposal.

After the local records manager's review and approval, individual documents are being shredded on-site while larger case files are boxed for subsequent bulk destruction by recycling.

As you finish at your file station, you note that the inactive personnel folders stored at the file station next door are missing. The file cabinets, which are normally locked, are open and empty.

You silently applaud your colleague's initiative in boxing and moving so many bulky records. However, when leaving the office for lunch you notice that multiple boxes labeled as "Old HR Files" have been placed in an open trash container next to the building.

What are the possible records privacy concerns arising from this situation?

How can you address these concerns?

# Module 7 Assignments

Your assignments for Module 7 are:

* Find your agency’s guidance related to the Privacy Act. What systems and types of information are mentioned?
* Consider your program’s or office’s records. What types of information in your office are subject to the Privacy Act? Which points of contact can help you address privacy concerns?

## Module 7 – Notes