

# Privacy, Security, DHS and You – Part1

**SECURE IT!**

Consider your:

-  **Conversations**  
Who - What - Where
-  **Computer**  
Position - Password - Protection
-  **Copies**  
Fax machines - Copiers - Printers

**Presented by:**  
**Department of Human Services**  
**Information Security Office**

# Objectives of this Course:

- What defines information?
- What causes information to be at risk?
- Why must DHS information be secured?
- Who is responsible for securing information during its lifecycle?
- What must everyone do?

# **Section 1:**

**What defines Information?**

DHS information can be generated, transmitted or received from various sources.

The Information Security Office (ISO) is focused on protecting confidential and other sensitive information from inappropriate access or disclosure, and ensuring that all DHS information assets are available to those who have the right and the need to access them.

Information (or 'data') whether it is generated vocally, through sign language, in written form or through digital images is the foundation of the service that DHS provides.

### **Sources of information include:**

**CONVERSATIONS**, whether in person or over the phone-

**COMPUTERS**, including emails, documents, charts or reports we create or receive

**COPIES**, whether they're created via fax machines, photocopiers, printers or are completed by hand.

DHS is concerned with maintaining both the *PRIVACY* and the *SECURITY* of the information that it generates, sends and receives.



## What is Privacy?

Privacy is a right that people have. It's the right that an individual has to keep their information from being disclosed. They also have the right to limit who sees that information. This also includes YOUR right. While we're talking primarily about clients today, we need to acknowledge that all of these privacy protections and rights apply to each of us as individuals, as well. In the United States we live with the constant threat of Identity Theft – every 4 minutes someone has their identity stolen.

## What is Security?

Security is the protection of that right. Privacy is the what, it addresses confidential information in any medium. And Security is the how, it **enables** privacy and addresses confidentiality PLUS integrity and the availability of information.

## “What is the difference?”

Security involves the mechanisms used to ensure the confidentiality, integrity and availability of that information

Privacy is an individual’s right to keep his or her information protected and to determine who should have access to it

### **Honoring Privacy prevents:**

**Identity theft.** According to a recently released report from the Federal Trade Commission (FTC) nearly 10 million people in the United States were victims of identity theft in the last 12 months.

**Protects client information.** We handle confidential client records everyday. It is our responsibility to ensure that this information doesn't fall into the wrong hands possibly resulting in personal or legal damages.

## “Is there a difference between Privacy vs. Confidentiality?”

Are we keeping confidential information private? – or - - Keeping private information confidential?

In accordance with DHS decision, both mean the same thing!

**For example;** take the case of a Social Security number (which everyone has the right to keep Private), in DHS we would strive to maintain the Security of that piece of information by the use of both technological and behavioral safeguards.

Technological safeguards might include the use of access control mechanisms (i.e., use of policies to determine who will be allowed to have access to specific kinds of data that are kept within the DHS informational system). Behavioral safeguards would include the promotion of such employee practices as using strong passwords to gain entry to their computers and locking down their computer terminals when they are away from their desks.

## **Section 2:**

**What causes information to be at risk?**

The DHS-Information Security Office (ISO) must safeguard the CONFIDENTIALITY, the INTEGRITY and the AVAILABILITY of DHS information and DHS information systems.

Confidentiality has to do with keeping information private, in accordance with state & federal laws, DHS policies and contractual obligations.

Integrity of information means that what goes into DHS information must remain untainted or unchanged by anyone who does not have the authority to modify it. Integrity has to do with the reliability and trustworthiness of information.

Availability of information requires that those who have authority to access information can access it readily (i.e., with good response time).

The protection of these three facets of information is, in fact, the responsibility of all DHS employees - -we will discuss this further later in this session. Any action that threatens the confidentiality, integrity or availability of DHS information puts that information at risk.

## HOW is DHS information placed at risk?

DHS information can be placed at risk by unauthorized access to information or information systems such as;

- System access by computer hackers (from inside & outside of DHS)
- Theft or loss of Laptops & Blackberry devices
- Sharing passwords
- Leaving computer stations unlocked
- Leaving confidential “hard copies” (e.g., photocopies, printed documents, faxes, mail, CD-ROMS) in unprotected locations (e.g., unmonitored or unlocked file cabinets, recycling containers & work stations)
- Holding confidential conversations in non-secure locations

Another method of putting DHS information at risk includes the misuse of information or information systems. This is done by;

- Accessing non-job related websites.
- Unauthorized downloading/installation of software/files.
- Listening to internet radio via DHS computers.
- Viewing streaming video via DHS computers.
- Using DHS assets for personal use or gain.

Link to this policies can be found in the ISO webpage.

Mis-directed information:

Accidental release of confidential information to unauthorized recipients by using an incorrect or inappropriate address.

Examples:

Mis-addressed or inadequately addressed mail, e-mail and/or Faxes.

## **Why is mis-directed information a problem?**

Imagine yourself in this situation: You send an e-mail to the personnel department of DHS requesting an advance on your salary. The receptionist meant to forward your e-mail to the group of payroll staff but accidentally chose the Email group next to it that includes about 125 employees. Your e-mail included information such as your social security number. How would you feel about them having that confidential information accidentally distributed?

## **How do you feel about SPAM?**

What starts as a misdirected e-mail can turn into SPAM immediately when a number of unintended recipients use the “reply all” feature in GroupWise.

Mis-directed information can create confidentiality problems, waste time and resources and increase the annoyance factor. The potential for error is compounded by the fact that there are 9,500 employees in the DHS email system - - as well as 32,000 employees from other state agencies.

## ***Test Yourself!***

*Mistakes happen - - -You inadvertently access an illicit Web site from your computer at work. In order to diminish the risk of “infecting” both your computer and the DHS IT system, you should immediately call the:*

Office of Information Services

Information Security Office

Division of Medical Assistance

# How can I avoid sending mis-directed information?

- Do not include unnecessary confidential information in Emails
- Leave confidential information out of the subject line in your e-mail
- Make sure your regular and interoffice mail is addressed accurately and completely
- Comply with state & federal privacy rules and DHS privacy/confidentiality policies
- Comply with state and federal policies regarding use of state computers
- Apply reasonable safeguards to confidential information
- Be aware of identity theft, how it happens and how to prevent it

## ***Test Yourself!***

*The email message you just received includes highly confidential information; client name, address, date of birth, Social Security number. You have no relationship to the client and none to the branch office that sent the message. It dawns on you that you should not have received that sensitive information, and you wonder if others also received it in error. The office which handles misdirected email is the:*

*Office of Communications*

*Children, Adults and Families Division*

*Information Security Office*

## **WHAT is “social engineering” and why should I be concerned?**

Social engineering is the practice of obtaining confidential information by manipulating legitimate users - - it is a technique used by attackers to gain system access or information by exploiting the basic human instinct to be helpful. To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. This activity constitutes an incident for DHS.

## **HOW do they accomplish this?**

By asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

## **WHAT is a phishing attack?**

Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal, often financial, information. Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. This activity constitutes an incident for DHS.

# WHAT do I need to do if I suspect an incident of this type?

Any occurrence that causes DHS information or information systems to be compromised or threatened qualifies as an Information Security Incident. All of the actions cited earlier would qualify as incidents. Any incident should be reported to the ISO. Your responsibilities (as DHS employees) around such incidents will be discussed further along in this session.

## **Section 3:**

**Why must DHS information be secured?**

DHS collects, uses, maintains and exchanges confidential and sensitive information daily. In addition to contractual obligations, it is required by federal law and state laws to take steps to secure confidential information.

Link to this policies can be found in the ISO webpage.

HIPAA protects personal or protected health information (PHI) in any form by getting PHI only to the people who need it and only for necessary, identified purposes. HIPAA is about protecting your information, my information and our client's information.

Aside from State and Federal regulations, it is the right thing to do. DHS has developed policies to guide employees regarding who has access to information and to whom it can be shared. We need to protect everyone's privacy and their personal information, just as we want our own protected.

## WHAT happens if we violate these protections?

As with any violation, there are penalties that occur. Listed are those HIPAA penalties;

- \$100 per violation, even if it's inadvertent
- \$25,000 in fines for more comprehensive rule-breaking.
- \$250, 000 in fines and 10 years in prison, or both for individuals and organizations that knowingly violate HIPAA statutes.

# What is the DHS General Privacy Rule?

DHS policies cover not only health information about clients, but also child welfare information, food stamp eligibility, vocational rehabilitation records, and much more. Although the federal HIPAA rules are applicable only to Protected Health Information (PHI), the decision was made by administrators at DHS to apply HIPAA-style protections to all confidential client information.

DHS may not use or disclose confidential information unless the disclosure is either authorized by the client or is specifically permitted or required by HIPAA, other state or federal law or DHS Privacy regulations.

Within DHS you will see “use” and “disclose” referenced

**To Use is to:** share, apply, utilize, examine, and/or analyze inside the agency

**To Disclose means to:** release, transfer, and/or divulge outside the agency

DHS has determined itself to be a “covered entity” under HIPAA. As a result, DHS has developed policies around HIPAA.

All these policies are listed on the ISO webpage. All information contained in this presentation is a direct reflection of one or more of these policies.

It is **your responsibility** to become familiar with these policies

## True or False:

HIPAA requirements can be superceded by State or Federal or DHS privacy regulations.

True

False

“The answer is “true.” If a state law offers more protection for the client’s information, then state law “trumps” HIPAA. Whichever law is more stringent (stricter) is the one that prevails.”

## **Section 4:**

**Who is responsible for securing information during its lifecycle?**

Any person or system that sees, stores, processes, uses or destroys DHS information is responsible for its protection. That includes;

- The Department
- Information Security Office (ISO)
- Employees
- Managers
- Office of Information Services (OIS)
- DHS Auditing Office
- Business Partners

# Who is responsible for Information Security?

You are! Everyone has a role in protecting information

## *The ISO's role:*

- Develop and manage Information Security policies, standards and procedures.
- Ensure the security of the DHS IT infrastructure.
- Oversight of information security practices at DHS.
- Response to Privacy and Security incidents.
- DHS Business Continuity Management Program.

# Who is responsible for Information Security?

## *The Departments Role:*

- Accept and manage accountability for its business applications and systems Include information security in employee training and appraisal process.
- Encourage/ provide a culture of security.
- Cooperate with other organizations (gov't, business partner) in order to secure DHS information.

# Who is responsible for Information Security?

## *Board members and Executives role;*

- Ensure security management responsibilities are assigned and managed.
- Sponsor the communication of DHS privacy and information security policies, standards and procedures.
- Support Business Continuity Efforts.
- Know current security status of its organizations and decide whether identified security risk should be mitigated, accepted or transferred.
- Support correction of security risks identified by auditor
- Encourage/provide a culture of security.

# Who is responsible for Information Security?

## *The Employee Role:*

- Must know and abide by DHS privacy and information security policies, standards and procedures, including information classification.
- Must know and abide by HIPAA privacy and security laws and regulations.

# Who is responsible for Information Security?

## *Managers Role;*

- Must know and abide by DHS privacy and information security policies, standards and procedures including information classification
- Must know and abide by HIPAA privacy and security laws and regulations
- Must ensure all staff, volunteers, contractors know and abide by information security policies, standards and procedures- periodic assessment.

## **Managers' responsibilities include:**

- Completing the Individual User Profile Form (IUP780) annually on every Employee.
- Report all incidents that are reported to you to the Information Security Office.
- Understand and comply with all DHS Privacy and Security Policies and discuss them with your staff.

# Who is responsible for Information Security?

## *OIS Role (Systems/Applications)*

- Assist in the development of information security technology standards.
- Manage the implementation of information security technology standards.
- Works with ISO to ensure proper security controls are in place for DHS IT.
- Implement effective access controls, such as user authentication and encryption.
- Protect data at rest.

# Who is responsible for Information Security?

## *Business Partners Role;*

- Must know and abide by standards and procedures, as established in DHS/Business Partner contract(s)

## ***Test Yourself!***

***The office you work in uses one generic password for the four support staff, which is kept on a "sticky" on the front of the reception desk computer. You remember a policy and something about not sharing passwords. For clarification and guidance on the policy you call the:***

***Information Security Office***

***Your RACF Data Steward***

***Your supervisor***

***1&3***

The department's approach to information security is to apply risk management practices to both products (deliverables) and business and technical processes. We ensure that confidentiality; integrity and availability issues are equally and formally addressed.

A Quick Review of "CIA"

## **Confidentiality**

- Do not divulge information outside the DHS prescribed limits.
- Only Individuals who have been authorized can disclose client information. For more information see DHS rules & policies for exception.
- Once authorization to disclose had been obtained, only disclose the least amount of client information necessary to accomplish the purpose of the disclosure
- Laws require that DHS keep client and employee confidential information safe and secure

## **Integrity**

- Information must be updated and kept safe to ensure accurate data

## **Availability**

- Information must be readily available to authorized users.
- Streaming video, radio transmissions from the Internet and downloading large files slows the network down, and slows down response time for employees to get to their necessary information

**If confidentiality, integrity and availability are not met, this creates a risk for clients and for the department!**

## **Risk to client**

- ID Theft
- Other personal intrusion
- Personal injury in domestic violence case
- Delayed eligibility for services
- Reduced trust in DHS to protect their interests

## **Risk to DHS**

- Office for Civil Rights (OCR) Complaint
- Legal Action
- Unwanted media attention
- Fines as a result of violations from HIPAA, IRS etc.

## **Section 5:**

**What must everyone do?**

## **Everyone must report incidents!**

By reporting all incidents, no matter how small, you will help guide the department in their efforts to prevent future incidents that could put DHS information at risk. Every incident that is reported whether by a client or an employee must be investigated

- If you come upon confidential information laying in open view on someone's desk - - that's an incident
- If you notice someone's computer screen is not locked and you are viewing confidential information about an employee or a client - - that's an incident
- If you are at the copier/printer and there is confidential medical information about a person still on the printer - -that's an incident
- E-mails with confidential information in them that was not intended for you is a "mis directed" e-mail incident
- Laptop thefts if they contain client or employee information are incidents and must be reported
- Inappropriate use of state computer systems (visiting inappropriate websites) is considered an incident and must be reported

***Doing nothing is a violation of the DHS Privacy/Security Incident Response (PSIRP) Policy***

Link to this policies can be found in the ISO webpage.

## How can clients report incidents?

Privacy complaints may be made to:

- DHS Governors Advocacy Office (GAO)
- DHS-Privacy Program
- Office for Civil Rights (OCR) *Contact info for these 3 are on the form 2090 and in the contact info section.*
- DHS field Office

Clients have the right to use any of these processes to report an incident.

Security incidents may be reported to your manager, who then needs to report it to the Information Security Office. If the incident is regarding your manager you may feel free to directly contact the ISO.

The process for Privacy/Security Incident Response is as follows:

- Report the incident
- The Information Security Office will respond and consult
- Documentation will take place
- Process Improvement and mitigation steps are put in place

If confidential information you are responsible for is stolen or compromised, contact the Information Security Office immediately at 503-945-6812 or email [DHSINFO.security@state.or.us](mailto:DHSINFO.security@state.or.us) and a staff person from our office will be assigned to follow up.

## **Guidelines for SECURING CONFIDENTIAL INFORMATION when you are away from your DHS office/facility;**

- If the information must be left in a vehicle for a short period of time, make sure the information is not visible from outside of the vehicle and make sure the vehicle is locked.
- Regardless of its form (e.g., electronic, paper or computer media), never leave confidential information unattended. If possible, keep the information within your sight.
- Obtain approval from your manager before removing confidential client information from the workplace.
- Determine if the work could be accomplished without taking the information off-site.
- Place it in a locked trunk, where possible.

## Steps to take to reduce risks –

In your everyday work, there are many things you can do to help protect and secure DHS confidential information. Here are a few tips.

- Secure confidential papers in your cubicle, if possible in a locked file when you leave for the day.
- Do not leave confidential papers unattended in the fax, printer or copy machines.
- Keep conversations at a volume level that will protect information
- Change your password frequently and use a “strong” password that is difficult to decipher. A password that’s not found in the dictionary and has a combination of numbers and letters is much harder to crack.
- Guard your password carefully. Do not share it with anyone else or post it in a visible area that others can easily see or find.
- Since data will be backed-up on a regular basis, make sure your data files are stored on the network server and not on your hard drive.

# Steps to take to reduce risks –

Take precautions when sending sensitive or proprietary information via email. Password protect documents if needed.

Always lock your computer when you are away from it. To lock most computers, users need to hit ctrl-alt-del simultaneously, then hit enter.

Make sure all computers are cleansed (of software, etc.) before the computer is allocated to another employee. Contact the Office of Information Services (OIS) to delete files and information.

Always get web content approval from the Communication Office, and never post confidential or personal information on web pages.

Only disclose the least amount of information necessary to accomplish the purpose of the disclosure.

Only those individuals who have been authorized by the client to share information may do so.

Report all security and privacy incidents to your manager and to the Information Security Office (ISO) (See section 2 and the remainder of this section for descriptions of these incidents)

Link to policies are provided in the ISO webpage.

# HOW do you reduce your risk both for yourself and the department?

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

Don't send sensitive information over the Internet before checking a web site's security.

Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information.

Congratulations  
Go forth and do good!