

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 20

AUGUST 2007

Resources

Privacy Program

(503) 945-5780

Information Security

(503) 945-6812

Information Security/ Privacy Web site

[www.oregon.gov/DHS/
admin/infosec/](http://www.oregon.gov/DHS/admin/infosec/)

Privacy Help Email

PrivacyHelp, DHS

Information Security Email SECURITY, DHSINFO

Privacy Policies

[www.dhs.state.or.us/policy/
admin/privacylist.htm](http://www.dhs.state.or.us/policy/admin/privacylist.htm)

Information Security Policies

[www.dhs.state.or.us/policy/
admin/infosecuritylist.htm](http://www.dhs.state.or.us/policy/admin/infosecuritylist.htm)

*Send requests for
future Privacy/Security*

Update topics to:

dhs.privacyhelp@state.or.us



Auditory Privacy

Sound travels. Keeping conversations private in an open space cubicle setting can be a challenge. And cubicles are a fact of life in DHS. Policy AS-030-006 states very clearly that no private offices will be allowed.

The federal HIPAA privacy and security rules require us to “provide reasonable safeguards” to protected health information. DHS privacy rules and policies require that we “provide reasonable safeguards” to all sensitive confidential information. Therefore, our challenge is to provide as much auditory privacy as possible with the tools at hand.

Here are some recommendations to enhance auditory privacy in cubicle settings.

- Add signage to indicate a confidential, sensitive area. Create bold signs as reminders to keep voices low and to reduce any unnecessary noise.
- Stagger client appointment times between adjoining cubicles.
- Whenever possible, reserve one meeting room for interviewing should a client become agitated or loud.
- Incorporate a background “white noise” to muffle voice sounds.
- Meet with all office personnel to discuss privacy needs for their particular area of the office.
- Implement weekly or monthly reminders to all staff regarding auditory privacy needs of the office.

The cubicle configuration in our offices is expected to remain as is. We can reduce concerns about auditory privacy by taking personal responsibility for the level of our own voices and by implementing some of the suggestions noted above.

Let's Prevent Smash and Grab Thefts

DHS has recently experienced an increase in the occurrence of theft, from both employee- and state-owned vehicles. Stolen items have included laptops, cell phones and client and employee paper files. These thefts expose highly sensitive, confidential information.

There are several things we can do to reduce “smash and grab” thefts from vehicles:

- Leave confidential information and files in the office, unless it is absolutely necessary to remove them.
- When transporting confidential information in any medium (paper, laptop computer, Blackberry, electronic notebook) keep it with you whenever possible. Take it in from the vehicle overnight (reminder: you must have manager approval before removing confidential information or any other state property from the workplace).
- If it must be left in the vehicle for some time, place it in the trunk or covered in the back of a vehicle without a trunk.

Managers: you need to make confidentiality and data protection a part of your unit’s routine:

- Discuss this topic at staff meetings.
- Create an office procedure for taking confidential information offsite.
- Draft a reminder checklist to be used by anyone taking client or personnel files offsite.

If a theft includes confidential information, report the incident to the Information Security Office: 503-945-6812 or dhsinfo.security@state.or.us



“Snail Mail Alert”

Include return addresses. Make sure the mail you’re sending via shuttle, U.S. Postal Service, or other carrier has a return address. It’s best to put the return address on the inside as well as on the outside of the package or envelope. Mail gets misdirected, clients move, staff people change work locations, and sometimes an entire branch office closes or moves. The only way to ensure that you’ll get an undeliverable item back is to provide a clear return address.

Privacy Contacts

Privacy Officer

Jane Alm, (503) 947-5255

Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Gloria Anderson

CAF/Pro. & Policy, (503) 945-5700

Ronald Barcikowski

CAF/OVRS, (503) 945-6734

Donna Weaver

SPD/Field Services, (503) 945-5977

Marilee Bell

SPD/DD, (503) 947-5262

Diane Duncan

AMH, (503) 945-6083

Steve Modesitt

Public Health, (971) 673-1293

Joni DeTrant

State Hospitals, (503) 945-2981

Terry L. Grover

Health/DMAP, (503) 945-6536

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



Secure Email

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, other regulations and contractual obligations, has provided the Oregon Department of Human Services (DHS) with the opportunity to take additional steps to increase the security of outbound electronic communications to external individuals and partners (those outside of the state email system).

Here's how it works

On July 30, 2007, DHS implemented software that has the ability to automatically scan outbound email (and any attachments) containing Protected Health Information (PHI).

This email is then “encrypted” so that it is unintelligible if the email is intercepted. Instead of receiving email directly to an inbox, recipients receive a notification message that DHS has a secured email waiting for them on a secure server.

The notification message contains a link that will take them, via a secure browser, to that server, where they can then open and read the message.

Any replies they send back are also sent securely because the replies are also stored on the secured server.

In essence, the email never leaves the state system except through an encrypted session.

Process for securing an email

1. Member of the DHS workforce sends an email containing protected health or confidential information.
2. The scanning engine determines if there is any PHI terms and patterns in the email using a weighted process to determine likelihood that the information must be encrypted.
3. The email is saved on a secure server.
4. The addressee (client, external partner, provider, etc) receives a notification message saying the email is waiting for them.
5. The addressee then retrieves the message from the secure server by clicking on the link in the notification message. The link will set up an https browser session, very similar to what you see when communicating with a bank or credit union.

Frequently Asked Questions

QUESTION #1. How can I force a secure email if I'm unsure the system will do it?

ANSWER #1: At times you may want to force an encryption if you feel that the confidential information that you are sending may be missed by a scanning engine.

The following steps will guide you to a forced encryption.

- a. From GroupWise, create a new email message.
- b. In the "To" field of the message, enter the recipient's email address(es).
- c. In the "Subject" of the message, enter “#secure#” (without the quotes), a space, then type in the

“SECURE EMAIL” continued on page 5...

One Record Holder Per Authorization Form

Just a reminder—separate Authorization Forms (#2099) must be completed for each record holder. See Section “B” of the Authorization Form Instructions (#2099I).

There is a reason for this—by listing more than one record holder on a single form, the different record holders are subsequently informed that the client/patient has received services from the others. This does not fit with our “need to know” and “minimum necessary” policy requirements.

If you have questions about this you may contact the privacy contact for your program area. Those names are listed in this newsletter.

ISO's Business Continuity Planning Program

Business Continuity Planning (BCP) is defined as “the process of developing advance arrangements and procedures that enable an organization to respond to an event so that critical business can continue.”

In short, how do we keep doing business during an event like a building fire, power outage etc.? The DHS Business Continuity Program exists to support and guide DHS as we answer this question and develop appropriate plans around our critical functions.

When people hear the term Business Continuity Planning, many focus on large-scale disasters such as the San Francisco earthquake, Hurricane Katrina or the 9/11 World Trade Center tragedy.

However, the more likely events to trigger the need for activation of a BCP are the everyday events such as a power loss (for any reason), a building fire; events that affect only one building.

***Keep in mind that the large-scale disasters will also trigger the continuity plans, but the smaller events are more likely to happen.*

DHS' business continuity planning focus is on our agency functions and our services provided to the DHS clients.

Imagine that you go to work and your worksite is unavailable

- How and where will you continue to do your work?
- What business functions (processes) need to continue and how soon?
- How do you communicate with your employees/managers if a disruption happened during work hours? What about after work hours?
- Are your critical documents protected from the harm that could be caused by a disruption such as a fire?
- How do you carry out the work of your program when the office location, the client files, the telephone system, and the computer systems on which you rely are not available?
- What happens if your key vendors cannot supply their services?

“ISO PLANNING” continued on page 5...

DHS BCP Program Coordinators

Program sponsor: Clyde Saiki,
DHS deputy director, 503-945-5731

Program manager: Patty McCary,
ISO, 503-945-6996

Manager: Kelli Hefflin, ISO,
503-947-5230

Administrative Services

Linda Riddell, Facilities,
503-945-5817

Sharon Domaschofsky, Facilities,
503-947-5018

Dennis Wells, OIS, 503-945-6573

Dave Wallace, OIS, 503-945-5992

Jeremy Emerson, OC&P,
503-945-6878

Kelly Stoll, OC&P, 503-945-5696

Julie Davie, HR, 503-945-6380

Gary Whitehouse, OPA,
503-945-6934

Debby Williams, OPAR,
503-378-5620

Jan Lemen, FDM, 503-378-3477

Children, Adults and Families

Leona Gildersleeve, CAF
Field Admin, 503-945-7000

Irvin Minten, CAF,
503-373-1200 (ext. 543)

Health Services

Maynard Hammer, OSH,
503-945-2866

Dusty Charters, OSH, 503-947-1080

Steve Modesitt, HS/PH,
971-673-1293

Dale Elder, HS/DMAP,
503-945-6589

Robert Furlow, EOTC,
541-276-0810 (ext. 331)

Nick Reed, EOTC,
541-276-0991 (ext. 431)

Edie Woods, HS/AMH,
503-945-6189

Seniors and People with Dis.

Bob Clabby, SPD,
541 276-4511 (ext. 470)

Donna Weaver, SPD, Field Services
Manager, 503-945-5977

Conrad Bozlee, SOCP

“ISO PLANNING” continued from page 4...

The continuity plan is designed to give guidance to employees around these questions (and many more) and to allow the business to resume operations as quickly as possible in case of a disruption.

How does continuity planning help me as an employee?

A business continuity plan will ensure that employees know:

- **WHAT** processes need to continue and in what order they need to be resumed (especially if resources are limited)?
- **WHEN** business functions need to be resumed (not necessarily back to normal), (What will be the BRTO – Business Recovery Time Objective)?
- **HOW** the business is going to continue those critical functions?
- **WHERE** the work is going to get done?
- **WHO** is going to do the work?
- **WHAT RESOURCES** are needed to keep the business processes functioning?

The overall management and coordination of business continuity planning is handled by the Business Continuity Program, which is located in the Information Security Office (ISO).

Each division has a business continuity planning coordinator to

manage the planning within their division.

What is your role?

- Your main role is to be aware that there are efforts happening to ensure we can continue to provide our critical services in the event of a disruption.

How does the plan influence your role?

- Some DHS employees will have roles in a plan during an event. In those cases you will be a part of the training and testing of the plans.
- For those who don't have an active role, you will need to be aware of what you are to do in a disruption, where you are to go, who you are to call etc.
- This will all be outlined in the plan and it is the responsibility of the plan's managers and division coordinators to ensure each employee knows what to do in case of an event.

Do you have a plan for your own family

Although business continuity planning is a business issue, DHS understands that during a large event or disaster, your first thoughts will be with your family and their safety.

Preparing your family for an emergency will help you feel more confident and thus more likely to

be able to perform your tasks for DHS without as much worry for your own family.

(Planning tools can be found on the Information Security Web site.

For a list of DHS business functions and additional information, link to the DHS Business Continuity Planning Web site:

www.dhs.state.or.us/admin/infosec/bcp/

“SECURE EMAIL” continued from page 3...**QUESTION 2. How can I force an “unsecure” email?**

ANSWER #2: There will also be times when you might want to force an unencrypted email because you know the email or attachments does not contain any Protected Health Information, but because of the amount of HIPAA-related information (medical terms, coding, etc.) you think the scanning engine would encrypt the email.

“SECURE EMAIL” continued on page 6...

“SECURE EMAIL” continued from page 5...

Here is how you force an unsecured email:

- a. From GroupWise, create a new email message.
- b. In the "To" field of the message, enter the recipient's email address(es).
- c. In the "Subject" of the message, enter "#u#" (without the quotes), a space, then type in the subject.
- d. Attach any files (if appropriate)
- e. Hit the send button.

QUESTION #3. Is encrypted email sent from DHS “private”?

ANSWER: No. It is still subject to same public record laws as all DHS email, (i.e., it is still a matter of public record).

While this process requires some extra steps, we are making every effort to ensure that there is no significant disruption to your communications with us.

We appreciate everyone's cooperation in helping us safeguard confidential and PHI data.

For additional information, see the DHS Secure Email Web site located at www.oregon.gov/DHS/admin/infosec/secure_email.shtml.

COMING SOON
DHS Business
Continuity Planning
(BCP) training online!

Awareness and Education Program

Privacy, Security, DHS and YOU! Parts 1 and 2

ISO has delivered a monthly NetLink, “Privacy, Security, DHS and You!” that is mandatory for all new DHS employees and volunteers. As of July 2007, “Privacy, Security, DHS and You!” will be delivered through two self-paced computer-training modules!

Module (1), required for all new DHS employees and volunteers, reviews the skills and knowledge needed to identify and counter some fundamental information security and privacy risks and requirements.

Module (2) is designated for all new DHS employees and volunteers with direct client contact and/or routine contact with client information. This module addresses the HIPAA Federal Privacy Rule requirements.

As of July 2007, all new DHS employees and volunteers must complete the “Privacy, Security, DHS and You!” module within 30 days of hire; they can access this training from their desk computers. Individuals in hospitals, training centers and group homes can continue to acquire both modules for classroom style delivery. The course content is available in PowerPoint and PDF format through the ISO Web page:

http://egov.oregon.gov/DHS/admin/infosec/tools_resources.shtml#ae

To access this new CBT, please go to the online DHS Learning Center: <https://dhslearn.hr.state.or.us>

The information provided in the Privacy/Security Update is intended for employees of the Oregon Department of Human Services. It is not intended as advice, legal or otherwise, to any entity outside of the department.