

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 18

APRIL 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/privacypolicy.htm](http://www.dhs.state.or.us/policy/admin/privacypolicy.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*



ID theft Consumer Education Kits available in English and Spanish

Each year, millions of consumers have their identities stolen. Identity theft is a serious crime and can cost people a great deal of time and money, regardless of their economic needs or status. ID thieves can be successful even if you don't have much money in your bank account.

While there is no foolproof way to avoid ID theft, there are ways to minimize the chances of becoming a victim, as well as the damage, should a theft occur. Many people just don't have all the information they need. That is where you come in. There are opportunities to raise awareness and educate clients, co-workers and communities. The Federal Trade Commission (FTC) offers a Consumer Education Kit to help you "get the word out."

The Consumer Education Kit includes a 10-minute DVD and a CD with resources for making a presentation, and a "How-to Guide" about educating others who may be vulnerable. Consumer Education Kits and brochures are available in English and Spanish through the FTC.

The DHS Privacy Office has a limited number of the brochures available. If you would like more information on these brochures or education kits, you can either contact the DHS Privacy Office at dhs.privacyhelp@state.or.us or you can go directly to the FTC Web site at <http://bulkorder.ftc.gov:10937/index.php?showcat=Identity+Theft%2C+Privacy%2C+and+Security%3A+Privacy+and+Security>.

Reduce ID Theft: Deter, Detect, and Defend

Clients filing privacy complaints

DHS clients have the right to file privacy complaints with the federal government. In fact, the DHS Notice of Privacy Practices (form #2090) gives them four options for filing complaints:

1. The office where they're receiving services
2. The Governor's Advocacy Office
3. The DHS Privacy Office
4. The Office for Civil Rights (OCR) in Washington, DC.

Contact information is provided for each option. OCR is the federal compliance agency for the HIPAA Privacy Rule. In the four years since HIPAA went into effect, over 25,000 complaints nationwide have been filed with OCR. Nine of those complaints came from DHS clients. That's not many when you consider the number of staff and clients DHS has. Two of them turned out to actually be against DHS partners, but seven were ours to investigate. The investigations involve interviews with staff and managers, reviewing months of case notes, evaluating signed authorizations, checking staff training records to ensure that they had participated in HIPAA privacy training, and many personnel hours.

In five of the seven complaints, DHS prevailed. Detailed investigation showed that we had not breached the clients' privacy. We were not so fortunate with the other two, as we were found to have inappropriately disclosed confidential health information to an unauthorized recipient. DHS was not fined or sanctioned at that time. At this point, we don't know if DHS will be granted that same grace in the future, or if OCR will exercise its lawful right to impose penalties.

"Snail Mail" alert

In this age of electronic and instant messaging, we don't think much about "snail mail." For those of you who don't recognize the term, it refers to mail sent through non-electronic methods such as the US Postal Service. The DHS Privacy Office recognized some privacy issues in our handling of mail, and a task group reviewed our current mail processes and is preparing a department-wide awareness and education program. Be watching for information on how you can reduce mail-related privacy risks through improved processes.

Here's one helpful hint that you'll be hearing about: Mail addressed to "Human Services Building, Main Mail Room, 500 Summer St. Salem, OR 97301" leaves much to the imagination. There are 1500 employees in the Human Services Building, representing all DHS divisions and programs. Take a look at the printed labels your office uses on a regular basis. Make sure that the information on the label is complete enough to ensure that the mail will reach the intended recipient. Be watching for more on this subject.

Privacy Contacts

Privacy Officer

Jane Alm, (503) 947-5255

Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Gloria Anderson

CAF/Child Welfare, (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

OMHAS, (503) 945-6083

Steve Modesitt

Public Health, (971) 673-1293

Joni DeTrant

State Hospitals, (503) 945-2981

Terry L. Grover

Health/OMAP, (503) 945-6536

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



Protecting our information assets

The Department of Human Services is a large and complex agency. As we carry out our mission of assisting people to become independent, healthy and safe, we all depend on each other to do our individual pieces of that work with integrity.

DHS staff, volunteers and our partners are responsible for protecting our information assets. At times, that means making sure the department can obtain the information it needs to accomplish its mission.

DHS uses information in many forms. In many cases, even when DHS is the originator of information and therefore “owns” it, the information’s use is controlled by federal and state regulations.

However, in some cases, DHS is not the information owner and must protect the information assets according to the contract we have with the owner.

For example, a CAF unit recently needed access to some federal information. However, the federal government would allow access to the information only if DHS could provide information on how we responded to an audit from another, non-CAF business unit.

This is just one example of how the actions of one business unit can affect the mission of another.

The Information Security Office works with business units to improve the agency’s ability to

meet information protection requirements—federal, state and contractual. To do that, we address:

- physical and environmental security
- human resource security
- access control
- business continuity planning and disaster recovery

- information security incident management
- other important security concerns
- encryption

In order to continue to protect our information assets, all of us need to understand these requirements, which will allow DHS to develop and implement department-wide strategies.

Coming Attractions to ISO's Awareness and Education Program

The Information Security Office has recently hired **Nasreen Khan** as the Awareness and Education program coordinator. Nasreen has been involved in developing computer-based modules for delivering awareness and education to DHS staff.

Module for new employees:

The first Computer Based Module (CBT) will be completed and available to new DHS employees in late April. Currently, DHS staff are required to enroll for the Privacy/Security DHS and You Netlink within 30 days of hire—this will still apply, however, the Netlink will be replaced with the enhanced version that new employees can access from their desks. Hospitals, training centers and group homes will be able to maintain the current practice of acquiring the content for classroom delivery.

Future attractions include:

- ***Privacy practices (Part 2) in May 2007:*** required training for new employees regarding privacy practices for employees who have direct client contact
- ***Business Continuity Planning - DHS and You! May 2007:*** Business Continuity Planning overview for DHS and employee responsibilities

The latest BCP buzz?

Are you new to Business Continuity Planning (BCP)?

- ◆ Have you thought about what would happen if your normal daily business operations were interrupted by a disaster?
- ◆ Have you determined what business functions (processes) need to be operational following a disaster, and have you planned how to resume those operations?
- ◆ Could you communicate with your employees if a disaster occurred during or after work hours?
- ◆ Are your vital records protected from harm that could be caused by a disaster?

These are some of the issues being considered by the BCP program.

Individuals in each area of DHS have been responsible for acting as liaisons with the BCP program team and for providing input to the BCP process. They coordinate their own units' preparation of detailed backup and recovery procedures and will manage the testing and training activities as well. DHS BCP coordinators have made many accomplishments, including:

- ◆ Serving on the BCP project team
- ◆ Acting as DHS coordinators and plan managers for their divisions
- ◆ Identifying users of the eBRP electronic management tool
- ◆ Identifying daily business functions (processes) and completion of the "function vs. process" education module
- ◆ Working on data- collection templates for eBRP in order to begin electronic plan development

- ◆ Completion of six-month DAS BCP academy course
- ◆ Completion of alternate site request worksheet to assist in HSB re-location strategy development
- ◆ Participation in meetings to coordinate and implement planning activities with ISO

What's next?

April: Begin to review and verify "plan templates" which include information the coordinators have provided ISO over the past year.

May: Divisions will begin the task of identifying "work-arounds" for functions (processes).

June/July: Coordinators will identify eBRP users and ISO will coordinate training. Users will update and maintain plans.

July: Monthly user group begins—users will gain access to eBRP, their division data and their preliminary plan information.

What can managers do?

- ◆ Know who your coordinator is and regularly meet with him or her
- ◆ Ask your coordinator for updates
- ◆ Consider policies that may be affected by planning efforts and inform your coordinator
- ◆ Discuss at staff meetings what continuity planning can affect
- ◆ Standard business continuity approaches such as cross training and working from home must be reviewed and implemented where weaknesses are found

You can visit www.oregon.gov/DHS/admin/infosec/ for complete program information and a list of coordinators, or for more information, contact Patty McCary, ISO/DHS BCP Program Manager

DHS BCP program coordinators

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

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

Manager: Kelli Heflin, 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/OMHAS, 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

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.