

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 14

APRIL 2006

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



HIPAA Enforcement Rule

The federal Department of Health and Human Services (DHHS) has implemented the final Enforcement Rule, effective March 16, 2006. It establishes rules of procedures and requirements for imposing Civil Money Penalties (CMP) on entities that violate HIPAA standards.

What does the Enforcement Rule cover?

All HIPAA rules that come under the HIPAA Administrative Simplification Provisions. That includes Privacy, Security, Transactions and Code Sets, and National Provider Identifiers (when it is final), and any future rules.

When would DHS, or any covered entity, be impacted by the Enforcement Rule?

A person who believes a covered entity is not complying with the administrative simplification provisions (HIPAA) may file a complaint with the designated federal agency, which then initiates an investigation regarding the complaint, or the DHHS secretary may conduct compliance reviews (audits) to determine whether covered entities are complying with the applicable administrative simplification provisions.

Which federal agencies enforce the rules?

The Office for Civil Rights enforces the Privacy Rule, and the *Centers for Medicare and Medicaid Services* enforce the Security Rule; Transactions and Code Sets; and National Provider Identifiers

What are the amounts of Civil Money Penalties?

The DHHS secretary may not impose CMP—(i) In the amount of more than \$100 for each violation; or (ii) In excess of \$25,000 for identical violations during a calendar year. The rule specifies that a separate violation occurs each day the covered entity is in violation of the provision.

Could DHS be required to pay?

Yes. To date, there have been six privacy complaints filed with the Office for Civil Rights against DHS. We have resolved them without sanctions or monetary penalties. Now that the Enforcement Rule is final, the end result could be different with the next privacy complaint. DHS has not yet been informed of any Security or Transactions and Code Sets complaints filed with the Centers for Medicare and Medicaid.

A summary of the rule

You can access a summary of the Enforcement Rule on the DHS Information Security Office Web site at [www.oregon.gov/DHS/admin/
infosec/docs/hipaa_enf_rule.pdf](http://www.oregon.gov/DHS/admin/infosec/docs/hipaa_enf_rule.pdf)

Document retention schedule and HIPAA

QUESTION: There's something in the HIPAA Privacy Rule that talks about retaining documents for 6 years. That's confusing. In my DHS program area our rules and policies require that we retain documents for only three years. What's the story on this?

ANSWER: Follow the program-specific rules and policies that define your retention schedule. You are correct, though, that the HIPAA Privacy Rule makes mention of a 6-year retention schedule. (164.530 Administrative Requirements) But that applies only to a very narrow, very specific set of documents.

Those include policies, procedures, and other documents that a covered entity writes in response to compliance with the federal HIPAA Privacy Rule. The only part of DHS affected by this 6-year retention schedule is the Privacy program within the Information Security Office.

Healthcare operations – a business necessity

There are times when business processes, or changes in business practices, necessitate the use of confidential information. We often refer to that as “live data,” meaning that it is current, confidential information in our computer systems, and the activity or project could not be completed without it.

In other words, fake or de-identified data would not work. It is unavoidable that the information will be viewed by a DHS technician who would not, under other circumstances, have access to it. HIPAA refers to this as healthcare operations, and allows for the use of confidential information in this type of activity.

We are still required to apply reasonable safeguards to protect the information. Any confidential information that might be printed out as test pages must be properly disposed of and not left vulnerable to casual viewing. If your program area has an upcoming project that may involve live data, you may contact the Information Security Office for guidance. See "Resources" panel on the Update's front page for contact information.

Origin of Amber Alerts

Although CAF is Oregon's child protective office, statewide Amber Alerts do not originate from CAF, or from any other program area in DHS. Law enforcement and broadcasters use the Emergency Alert System (EAS) to air a description of the missing child and suspected abductor. This is the same concept used during severe weather emergencies. Therefore, if you receive a request via email or other source to initiate a statewide Amber Alert on a child, don't forward the message. Talk with your manager or program area director for guidance.

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

Vacant

OMHAS, (503) 947-5522

Steve Modesitt

Public Health, (971) 673-1293

Maynard Hammer

State Hospitals, (503) 945-2866

Terry L. Grover

Health/OMAP, (503) 947-5488

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540



State-operated community programs and Business Continuity Planning (BCP)

Information Security Office personnel were recently given a tour of several state-operated group homes for persons with disabilities by DHS-SPD staff member, Conrad Bozlee.

Our purpose was to look at their operations with an eye toward Business Continuity Planning (BCP) concerns (in keeping with our role as the DHS lead on BCP preparations).

We came away with an appreciation for the planning and work entailed

in their day-to-day operations. Their planning and preparations for occasional program camping trips were particularly instructive!

The tour generated some ideas on mapping of their existing processes for program outings and for emergency evacuation as a way to identify gaps in planning for scenarios such as power outages, workplace unavailability and possibly workforce unavailable.

We will continue to work with them and other DHS programs to promote BCP efforts.

If you would like to know who the BCP representative is for your DHS office or cluster, you may view the BCP Project Team Roster at www.oregon.gov/DHS/admin/infosec/contacts.shtml#bcp

If you have questions for the Information Security Office about BCP, you can contact DHS project manager, Patty McCary, at 503-945-6996 or DHS project lead, Richard Templeton, at 503-945-5851.



Family planning for disasters

In the past year we've seen a sequence of major disasters and health hazards, from the tsunami in Indonesia, to hurricanes Rita, Wilma and Katrina in the Gulf states, to the spread of avian flu and threat of a pandemic flu.

These events provide powerful reminders of the value of planning and preparation for major events. The following topics should be addressed in your own plan for protecting your family:

- ❖ Health issues, medications and supplies
- ❖ Evacuation planning
- ❖ Family communication plan

For useful tips on how to address these items in detail, see the following link provided by the Uniformed Services University of the Health Sciences: www.usuhs.mil/psy/PlanningforDisaster.pdf.

For a more in depth review of the subject with an emphasis on pandemic flu, you can view the U.S. Department of Health and Human Services publication, "Pandemic Influenza Planning: A Guide for Individuals and Families" at www.oregon.gov/DHS/ph/spotlight/panflu/docs/planningguide.pdf.

Report on ISO presentation data shows increase

Since its inception in 2003, the Information Security Office (ISO) has conducted 145 presentations to 110 separate groups.

Our communication efforts have successfully provided education and guidance on privacy- and security- related topics to 3,141 DHS staff members, managers and partners.

Presentations given have included the following: Information Security Overview; Secure It!; Managing Resources; Password Policy; Business Continuity Planning; Netlink on Privacy and Security.

The following table provides data to show how the proportion of DHS staff persons reached by ISO's awareness and education efforts has increased in each year of ISO's operations:

Year	Numbers Reached	Total DHS Staff	Percentage of Staff Reached
2003	739	8,509	9%
2004	1,080	9,007	12%
2005	1,322	8,974	15%
TOTAL	3,141	8,830 Average	12% Average

The Information Security Office consults to DHS offices on privacy and security matters.

If your office has an interest in any of the topics addressed in this publication or would like to request a presentation on an issue related

"REPORT" continued...

to privacy and security, you can contact us by phone at (503) 945-5733 or email us at dhsinfo.security@state.or.us.

You can also visit our Web site at www.oregon.gov/DHS/admin/infosec/index.shtml

Security Tip of the Month

Sixty percent of all data created ends up archived.

Are your archives a landfill?



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 other, to any entity outside of the Department.