

Privacy/Security

UPDATE

DEPARTMENT OF HUMAN SERVICES

ISSUE NO. 13

JAN. 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/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



Authenticating YOU on the Phone

Recently, the DHS Privacy Program received a request from one of the Oregon Health Plan (OHP) managed care plans regarding authenticating phone callers. Here's the request, word for word:

We receive calls from caseworkers, advocates, etc. and we really have no effective way of knowing who they are and are less able to help. Our first requirements in authentication, if we are not speaking with the member directly, are to receive either a verbal approval (like in a three-way conversation) or a valid authorization. We also check for legal documents to know whether we have received guardianship papers, legal custody, etc. But in the event that we have none of this, and the caller is identifying him/herself as being from the state, would it be possible to receive the following?

- caller name
- department the caller represents
- phone number where the caller can be reached, preferably the general office number
- member's name, first and last
- member ID number
- member date of birth

Like DHS, OHP managed care plans are HIPAA-covered entities and are thereby subject to all of the regulations of the HIPAA privacy rule. While we don't want, in any way, to delay services to our clients, we need to be mindful of the privacy concerns of our community and other partners. DHS promotes that same level of concern and caution. You may want to check out the May 2004 *Privacy Update* article on authenticating callers, under News and Publications, at <http://www.oregon.gov/DHS/admin/infosec/>. When phoning an OHP managed care plan to assist a client, have the information that is noted above readily available.

Take the Privacy Quiz

Test your privacy knowledge. Check your answers to the quiz by accessing the Information Security Office (ISO) Web site at [http://www.oregon.gov/DHS/
admin/infosec/privacyquiz_answ.shtml](http://www.oregon.gov/DHS/admin/infosec/privacyquiz_answ.shtml). All of the questions and answers have been addressed in previous *Update* issues.

While you're there, wander around the ISO site and discover the privacy and information security resources available to you.

"QUIZ" cont. next page...

PRIVACY update

"QUIZ" cont. from page 1

- 1. A DHS client should not be asked to sign a blank authorization form.**
True False
- 2. It is okay to fax a client-signed Authorization for Use and Disclosure of Information form to the record holder.**
True False
- 3. The federal HIPAA Privacy Rule is the most stringent (strict) privacy law we need to consider when making a decision about use or disclosure of confidential information.**
True False
- 4. Which of the following disclosures can NOT be made without an authorization signed by the client?**
 - a. reporting child abuse
 - b. response to court orders
 - c. request for alcohol/drug treatment records
 - d. reporting fraud or abuse of public funds
- 5. The HIPAA Privacy Rule requires that the DHS Notice of Privacy Practices (form #2090) be given to all of our contracted partners and providers.**
True False
- 6. The term "Phishing" is most closely associated with:**
 - a. catching something for dinner
 - b. identity theft
 - c. computer viruses
 - d. water purification
- 7. Which of the following scenarios are considered reportable (to the Information Security Office) privacy incidents?**
 - a. confidential or protected documents not disposed of properly
 - b. theft of documents or computer equipment containing confidential client information
 - c. misdirected email message containing confidential client information
 - d. all of the above
- 8. Documents containing confidential information are to be recycled in the box or container under your desk.**
True False
- 9. The term "Hover Bubble" is most closely associated with:**
 - a. helicopters
 - b. chewing gum
 - c. micromanagers
 - d. GroupWise email addresses
- 10. Email messages are exempt from disclosure in a public records request.**
True False

Privacy Contacts

Privacy Officer

Jane Alm, (503) 947-5255

Privacy Coordinators

Linda Weight

CAF/Field Services, (503) 945-6119

Donna Weaver

SPD/Field Services, (503) 945-5977

Marilee Bell

SPD/DD, (503) 947-5262

Anita Miller

OMHAS, (503) 947-5522

Ronald Barcikowski

CAF/OVRS, (503) 945-6734

Steve Modesitt

Public Health, (971) 673-1293

Maynard Hammer

State Hospitals, (503) 945-2866

Genevie Rosin

GAO, (503) 945-6726

Linda Grimms

Legal Counsel, DOJ, (503) 947-4540

Terry L. Grover

Health/OMAP, (503) 947-5488

Gloria Anderson

CAF/Child Welfare, (503) 945-5700



Are You Accessing DHS Information

The Information Security Office recently revised the DHS Information Access Control Security policy. The policy was revised to ensure the confidentiality, integrity and availability of information assets stored with DHS systems. It protects those systems so that only authorized users have access to DHS information assets.

What changes do managers and contract administrators need to be aware of?

New forms have been developed to support DHS managers and contract administrators in their efforts to identify and authorize specific computer access for users:

- The “Individual User Profile/Stand-Alone” form (IUP-DHS 0780)
- The “Individual User Profile/Cluster Specific” forms (HS-DHS 0781; OMAP-DHS 0782; CAF-DHS 0783; and SPD-DHS 0784)
- The “DHS Contract Systems Information Exchange Assessment” form (DHS 0785)

Two new procedures outline the steps necessary for DHS managers and contract administrators to grant access to DHS computer systems:

- The DHS-090-003-01, Individual User Profile-Internal Access (DHS Employees/Authorized Partners”
- The DHS-090-003-02, Individual User Profile-External Access (Contracting Business Entity)

How are we implementing this revised policy for staff?

Managers are to begin using the Individual User Profile (IUP) forms for all DHS internal users, and complete the process of identifying existing users and their authorized level of access over the course of one year (could be linked to new hires, annual staff performance evaluations, anniversary dates, position description changes, etc., but are not limited to these events).

What about partners’ access?

DHS will require the same commitment from external partners. This will be an evolving requirement. The Contract Administrator will work with the Business Contacts and their partners at time of contract renewal, or when a new contract is developed to achieve proper access controls for our partners.

ID Theft Tips

One of the easiest ways to get information is to simply ask for it. Scam artists and identity thieves call or email people to get their personal information. If you see any of these scams, don’t respond.

Phishing Schemes

These scams usually show up in your email inbox with a message from the “System Administrator” telling you to perform urgent maintenance on your account, requiring your account number and other personal information.

Nigerian Email Scam

This scam has been used for over 10 years and is sent out to victims via letter, email and fax. Don’t let it tug at your heart strings.

Auction Fraud

Auction fraud (eBay and Yahoo) was the second most reported consumer fraud complaint to the FTC, totaling 51,000 auction complaints in 2002.

ID Theft Protection or Credit Repair Scams

The Federal Trade Commission (FTC) has warned that some companies claiming to be identity theft prevention services are scam artists. Don’t give personal information over the phone or online unless you are absolutely sure about the company.

“You’ve Won a Prize!” Scam

We all want to be winners. But if it sounds too good to be true, it is. Ask for a number to phone them back, or ask that they send you something in writing.

What Else Can You Do?

Adopt a “need to know” approach to your personal data. Utilize the one free credit report yearly. Use FTC resources (877-438-4338 or www.consumer.gov/idtheft).

Security Reminder

In the event that you either directly experience or witness an information security incident, please note the following:

What is an information security incident?

It can be a variety of things. Some of the more common examples are: a virus on your computer, staff sharing passwords or downloading software from the Internet. An incident is an event that threatens the confidentiality, integrity, and availability of DHS information or systems. For more information, see all of our incident examples:

http://www.oregon.gov/DHS/admin/infosec/incdnt_ex.shtml.

When do I report an information security incident?

You should immediately report all privacy and security incidents. See DHS Procedure AS-090-005-01, Privacy and Information Security Incident Reporting Procedure.

How do I report a privacy/information security incident?

Report to your supervisor, if available. If an incident involves an immediate supervisor, or if the supervisor is not available, report the incident directly. You may also contact the Information Security Office (ISO) or OIS Customer Service and Support Office (Service Desk). Incidents may be reported verbally, over the phone, printed in email or by fax.

dhsinfo.security@state.or.us; phone: 503-945-6812

Information Security Office; fax: 503-947-5396

dhs.servicedesk@state.or.us; phone: 503-945-5623

What are the benefits of an incident program?

- Minimizes loss or theft of information
- Provides a consistent process for gathering information
- Provides help for staff and partners to recover quickly and efficiently from incidents

Security Tip of the Month

When requesting help with your **RACF ID** and/or your **FACIS ID**, in order to prevent redirecting and to improve your customer service time, send those requests via email to:

SECURITY-REQUESTS, CAFRACF

(rather than DHS, INFOSECURITY).



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.