

Welcome to the Wisconsin Department of Health Services Privacy & Security Training

Privacy and Security Awareness

Why Are You Being Asked to Take This Training?

- To safeguard confidential information
- To maintain the confidentiality of confidential information that staff handle whether it is in electronic, paper, or verbal formats
- To meet the expectations and garner the trust of our clients and of the public
- To adhere to Department policies and procedures and state and federal laws



Published Horrors

Following are some examples of recent improper disclosures which illustrate why confidentiality is so important:

- In the biggest loss ever of personal information compiled by state government, a computer disk containing data on 2.9 million Georgians was lost in shipping. State officials, who blame Dallas-based Affiliated Computer Services for the lost CD, said it contained names, Social Security numbers, birth dates and addresses of people on Medicaid and PeachCare for Kids, but no medical information. (04/07)



Published Horrors (Continued)

- A laptop was stolen containing data of all American veterans who were discharged since 1975 (including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses) from a Veteran Administration employee's home. Theft of the employee's laptop and computer storage device housed data for 26.5 million veterans. (5/06)

DHS Commitment to Privacy

- Protect the confidentiality of health and confidential information reported to and maintained by DHS
- Preserve the privacy of all clients' confidential information
- Ensure reasonable safeguards of all electronic and paper information

Privacy & Wisconsin Laws

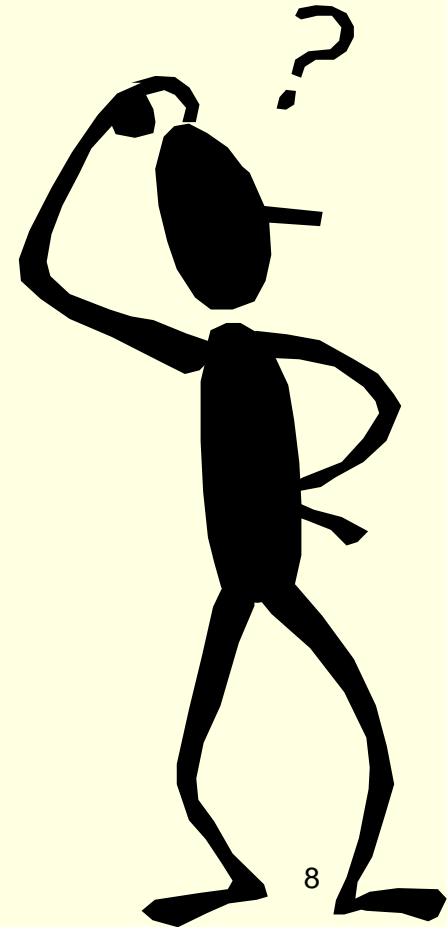
- Wisconsin's "identity theft" laws (Wis. Stat. §134.98):
 - Require that individuals be notified if security of their confidential information has been breached if deemed material (meaning that the acquisition of confidential information does create a material risk of identity theft or fraud to the subject of the confidential information)

What is Confidential Information?

- Confidential information means all information regarding an individual including personal, demographic, financial and health information that is required to be kept confidential by State and federal privacy laws, including but not limited to HIPAA, Titles XIX, XXI and other titles of the Social Security Act and provisions in Chapters 46, 49, 51, 51.30, 69, 146 and 252 of Wisconsin Statutes.
- The information can come from any source or be in any form to be considered confidential.

Why Comply with Confidentiality Laws?

- It's the law!
- Public expectations that we will maintain confidentiality of information
- There can be severe penalties for non-compliance
- Potential withholding of funding
- Possible litigation
- Public relations and business risk issues



Minimum Necessary Standard

- Who has access to confidential information and the “need-to-know” principle:
 - One must make reasonable efforts to limit the use and disclosure of, and requests for confidential information, to a minimum amount necessary to accomplish the intended purpose
 - Access information **only on a need-to-know basis**. Ask: “What information do I need to know to do my job?”



Privacy & Security Incidents

Incidental Disclosures

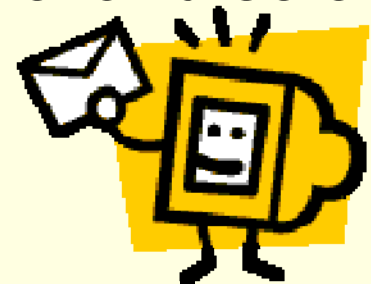
- If reasonable steps are taken to safeguard a client's information and a visitor happens to overhear or see confidential information that you are using, you will likely not be liable for that disclosure
- Incidental disclosures are going to happen...even in the best of circumstances
- Take actions to minimize even incidental disclosures

Reasonable Safeguards to Avoid Incidental Disclosures

- Keep your voice low
- Move to a private area when discussing confidential information
- Do not leave confidential information where others can see or access it

Reasonable Safeguards to Avoid Incidental Disclosures (Continued)

- Cover papers and shield computer screens in public areas to make them secure as possible. Don't allow unauthorized individuals (i.e., visitors, friends, or family members) to view your computer screen as you access confidential information.
- When using a computer, if you need to walk away, you should **ALWAYS**:
 - Log off **OR**
 - Lock the computer screen (Ctrl-Alt-Del and select lock)



Reasonable Safeguards to Avoid Incidental Disclosures (Continued)

- Don't leave documents containing confidential information unattended in fax machines, printers, or copiers
- Store confidential documents in filing cabinets and lock at end of day
- When disposing of confidential documents, either shred or put in locked recycling bin for destruction

Examples of Accidental Disclosures

- Sending an email to the wrong person that contains confidential information
- Emails sent out externally are not secure unless encrypted or secured (more information on this later)
- Sending a fax to the wrong number if that document contains confidential information
- Disclosing data to someone who didn't have the right to receive it
- Sending information to the wrong address if the document contains confidential information
- Loss of an electronic file, report or paper printout containing confidential information

Intentional Disclosures

- If you ignore the rules and carelessly or deliberately use or disclose confidential information, you can expect:
 - DHS action
 - In some cases, you may be held liable under Wisconsin statutes

Examples of Intentional Violations

- Improper use of passwords – sharing, posting or distributing personal password or account access information
- Allowing a co-worker to log-on with your password because it provides access to more or different security levels your co-worker doesn't have
- Attempting to learn or use another person's access information

Examples of Intentional Violations

(Continued)

- Discussing confidential information in a public area or elevator
- Selling health or personal information or inappropriately providing it to the news media or any unauthorized person
- Accessing information that you do not have a “need to know” for your job because of personal curiosity or as a favor to someone else

When to Report Privacy & Security Violations?

- **All accidental and intentional violations, known and suspected, must be reported immediately to your contract manager.**
 - So they can be investigated and managed
 - So they can be prevented from happening again in the future
 - So damages can be kept to a minimum
 - To minimize your personal risk

Incidental disclosures need not be reported, but if you're not sure, report anyway

When to Report Privacy & Security Violations? (Continued)

- In some instances, management may need to notify affected parties of lost, stolen, or compromised data. If you learn of inappropriate disclosures:

Immediately notify your contract manager.

Safeguarding Confidential Information is Everyone's Responsibility

- Protect it at all times
- Do not share it with anyone unless there is a need to know to accomplish the work of this Department
- Constantly monitor your actions: If I do this, will I increase the risk of unauthorized access?
- Only access the minimum amount of confidential information needed to do your job



What Can You Do to Safeguard Confidential Information?

- Take all reasonable precautions as described in the following slides to safeguard confidential information including:
 1. Protecting your passwords
 2. Using strong passwords
 3. Practicing good email security – do not send emails containing confidential information without protecting that information in an appropriate manner
 4. Preventing viruses
 5. Storing media securely
 6. Disposing of confidential paper and media in a secure manner
 7. Practicing good workstation etiquette
 8. Protecting verbal communications

Bottom Line

- Consider the client's perspective and give them control over how their information is used. How would you feel if it were your information?
- Avoid situations in which the client would object to how their information was used or shared
- Implement appropriate security measures to maintain the integrity of client data, ensure its availability, and keep it confidential

