Transforming Lives

DSHS CA Security For Providers

Pablo F Matute

DSHS Children's Information Security Officer

Washington State Department of Social & Health Services
Transforming lives

Security in Contracts

Data Categories: An Overview

All DSHS-owned data falls into one of four categories:

- **Category 1 - Public** information can be released to the public.
- **Category 2 - Sensitive** information is not specifically protected by law but should be limited to official use and protected from unauthorized access.
- **Category 3 - Confidential** information is protected from disclosure by law.
- **Category 4 - Confidential** information requiring "special handling" is also protected from disclosure by law, regulation, or agreement – and serious consequences could arise from unauthorized disclosure, ranging from life threatening situations to legal sanctions.

- ***DSHS CA Data is always Category 3 and above***

Security in Contracts

Data Categories: Categories 3 and 4

Here are some examples of category 3 and 4 data:

- Examples of **confidential** information include personal information about individual DSHS clients, Department employee personnel records, source code for computer applications, and any other documents or information that could potentially jeopardize the integrity of the Department, enable fraud, or trigger action by law enforcement or regulatory group. Personal information includes things like name, birthdate, and address.

- Examples of **confidential** information requiring "special handling" include information with especially strict handling requirements such as a client's Federal Tax Information (FTI), their Protected Health Information (PHI), a location of an abused spouse, or other potentially life-threatening data.

Security in Contracts

Confidential Data: Not Sure? ASK!

If you ever find yourself in a situation where you have a question about data security requirements, or if you *think* you discovered a breach but you aren't sure, **ask your CA Contracts Manager.**

If you can't reach your CA contract contact the CA IT Security Administrator, pablo.matute@dshs.wa.gov

Remember: it's always better to be safe than sorry.

Security in Contracts

- What encryption means
  - **<u>Workstations and Laptops</u>**
    - The following encryption technologies are approved for use on **workstations and laptops**
    - ***Windows – Microsoft BitLocker (Ultimate version)***
      - Trusted Computing Group (TCG)-compliant BIOS.
      - TPM microchip version 1.2, enabled for use with BitLocker.
    - ***Apple*** –
      - FileVault
      - FileVault 2

Security in Contracts

- **What encryption means**
  - Laptops containing confidential data *must* be encrypted (full-disk) as the risk of theft or accidental loss is high.
  - If a workstation or laptop contains multiple drives – for example, an operating system drive and a data drive – *all* of the drives in the workstation or laptop must be encrypted.

Security in Contracts

- **What encryption means**
  - **Removable Media**
    - It is *especially* critical that **removable media** containing confidential data be encrypted due to the high risk of theft or loss. Examples of removable media include hard disk drives (internal/external), backup tapes, flash drives, optical discs (CDs/DVDs), and memory cards.
  - **Mobile Devices**
    - Like removable media, it is also *especially* critical that **mobile devices** such as smart phones and tablets be encrypted due to the high risk of theft or loss.
    - Information on devices that cannot be encrypted (voice recorders or digital cameras, for example) must be protected using compensating controls approved by your administration's IT.

Security in Contracts

- **What encryption means**
  - **Servers**
    - The following encryption technologies are approved for use on **servers**
    - SQL –Transparent Data Encryption (TDE) or column-level encryption.
    - Linux – Linux Unified Key Setup (LUKS)
    - Other – Database, table, column, row, or file-level encryption depending on technical feasibility.
    - ***These requirements apply regardless of whether it is a development, test, or production environment – if that environment contains confidential data.***

Security in Contracts

Password Security: General Rules

Passwords are the provider's first – and sometimes last – line of defense against unauthorized access to sensitive systems and information.

As a DSHS contractor it is **your job to use strong passwords,** to protect them from disclosure, and to report any breaches *immediately*.

You can protect your passwords by following these basic guidelines:

- Use complex passwords that can't easily be guessed.
- *Never* write your password down.
- *Never* share your password with *anyone* – verbally or in writing.
- *Never* allow a coworker or contractor to assume control over a computer while you are logged in on your account.
- Change your passwords often, *especially* following a breach.

Security in Contracts

Password Security: Minimum Requirements

Minimum password requirements for DSHS contractor information systems may change from one system to the next. Here are some of the general guidelines:

- Workstation passwords must be at least eight characters long and contain at least one special character (**ex:** the "$" symbol) and two of these three character classes: upper case letters, lower case letters, and numbers.
- Passwords must not contain your user ID or any form of your name.
- Passwords must not contain a telephone number, Social Security Number, your child or pet's name, or any other personal information that could be easily guessed by one of your coworkers.

It's important to keep in mind that these are just the *minimum* requirements and *general* guidelines. Whenever possible a **complex password** is best.

You'll learn what a complex password is on the next slide.

Security in Contracts

Password Security: What's a Complex Password?

A complex password is a password that meets the following criteria:

- It's at least fifteen (15) characters long: **L8ther2nite@P4rt3**
- It *isn't* derived from the username – in whole or in part.
- It combines upper and lower-case letters, numbers, and symbols; and
- It *doesn't* include dictionary words, names, birthdays, telephone numbers or any personal identification numbers.

The stronger your password, the less likely it will be that unauthorized use or breach of your account will occur.

Remember: **You are responsible for ensuring the integrity of your account(s)**

Security in Contracts

Workstation Security: Locking Your Workstation

All DSHS contractors are required to lock their workstations, laptops, servers, and *any* other devices when leaving them unattended.

If you're logged in to a Windows-based DSHS workstation it's important that you lock it ( + the "L" key) before leaving your desk for a meeting, a break, or for any other reason that requires you to be more than arm's length from the keyboard. Locking workstations is *especially* important if you have access to any of the following information or information systems:

- Healthcare information
- Famlink Data
- Visitation Notes
- Department information that is considered sensitive or confidential.

Security in Contracts

- **What Secure E-mail means**
  - When communicating with DSHS, always use the secure e-mail system.
  - DSHS CA employees are required to use the secure email system when sending confidential data through providers/contractors
  - Response from providers/contractors and data send by provider/contractor should use the same method
  - Subject [secure] (test)

Security in Contracts

Email Security: Identifying Malicious Messages

Email is the primary method through which most DSHS employees and contractors communicate with each other, clients, and partners.

Unfortunately, email is *also* the primary method through which people with malicious or criminal intent attempt to breach the DSHS or providers network.

Identifying a malicious message can be challenging. Here are some quick tips to help you avoid falling victim to one:

- Be *extremely* cautious about how you handle unsolicited emails.
- *Never* click on links or open attachments in unsolicited emails.
- *Never* respond to emails asking for your username or password.
- If you have *any* doubts about the authenticity of an email, don't open it and notify your contract contact immediately

Security in Contracts

Physical Security: Laptops and Mobile Devices

Many DSHS contractors use laptops, mobile phones, tablets, voice recorders, and cameras to perform some or all of their duties.

Laptops and mobile devices are *very* easy to lose and they're a prime target for thieves because they're small and valuable. It's *extremely* important that you keep these assets secure. Laptops should *always* be encrypted, and you should *never* leave them somewhere that they can be easily lost or stolen.

You **must** report stolen or lost removable media to both your supervisor and your CA's contract contact

Security in Contracts

Physical Security: Removable Media

Removable media – such as USB drives, external hard drives, memory cards, CDs or DVDs, and voice recorders – are *very* easy to lose and they're a prime target for thieves because they're small and valuable.

It's *extremely* important that you keep these assets secure. Sensitive data on removable media should *always* **be encrypted** and you should *never* leave it somewhere that it can be easily lost or stolen. Lock it up, keep it out of sight, and *never* leave it in a State or personal vehicle.

You must report stolen or lost removable media to both your supervisor and your CA's contract contact

Security in Contracts

Voice Mail

Regarding online voicemail through providers such as CenturyLink or Comcast.

Can we use a service like this at our remote offices to run our voicemail or would this be a concern because a voicemail may contain voiced DSHS data in the cloud?

Use any voice mail but do not leave DSHS data on it!

Security in Contracts

Provider Instructions for Breach Situations

ON DAY ONE

Call your local contracts manager and provide a very detailed account of what happened. It may be easier if they do a conference call with you and the staff member who was actually involved in the loss.

- When, where, and how exactly did the incident happen?
- How many people's information was released?
- Exactly what information was disclosed? (It may be easier to ask the provider which documents were taken: Visitation referral, psychological evaluation, quarterly BRS report. Then you can look up those forms and see what's on them.)

Security in Contracts

Provider Instructions for Breach Situations

DAY ONE (CONTINUED)

- What precautions have you taken to prevent the information from being lost or stolen?
- If the situation involved computer equipment provide a police report.

Reminder – Using the same machine for personal and state business, is a bad idea. Steps need to be taken to avoid the loss of privacy, i.e. notify email contacts, change passwords, notify credit card companies about a fraud alert.

Security in Contracts

Instructions for Breach Situations

DAY ONE (CONTINUED)

As soon as possible:

- Notify all affected individuals whose personal information may have been released. Use certified mail so you have a record the letter was received by the client.
- Notify Social workers of the breach.

Security in Contracts

Frequently Asked Questions (FAQs)

Why are SW's sending unencrypted data to the Providers?

CA SW's should always use the secure email system, if a SW sends an unencrypted email with confidential data please contact Pablo Matute at pablo.matute@dshs.wa.gov

Can we store data in the Cloud? If so, what are the requirements?

DSHS data may not be stored on any medium not controlled by the Contractor. Storage on any Internet service such as DropBox, iCloud, Amazon Web Services, or any other Internet based storage system is not allowed. Contact Pablo Matute for more information.

Security in Contracts

FAQs:

Can we use Flash Drives if the data is encrypted?

Yes, just do not have the password typed on the device

Which mobile Devices can be used for data?

All, with a MDM Mobile Data Management solution that can encrypt, locate, change passcode, locate and remote wipe the device. MDM such as Meraki, Air watch, etc.

Security in Contracts

In the Secure Email system, all emails go away after 21 days - can this be fixed?

Messages are retained for 30 days. It's a global setting so it cannot be changed. Because the Secure email system is for secure transport only, and not built for permanent email storage, this was a vendor requirement.

After 30 days no records at all of emails received or sent- not able to show proof

The record of a message being sent would be with the DSHS employee. If the DSHS employee sent the message, then there is a record in their Sent Items folder. If they've received a reply, then the DSHS employee will have that message for reference.

Security in Contracts

Is there a way to track outgoing secure emails?

Yes. Please send those requests to the ISSD Service Desk and include the sender, recipient, and the date the message was sent.

Is there a way to save the secure email in the secure system?

The secure email system is for transport only; it is not designed for permanent message storage. Individual messages can be saved as text files using the "More Actions" drop down menu that is available when viewing a message. Attachments can be saved the same way.

How do I add other people in the email that are not a part of the original secure email?

The *Reply* and *Reply All* options only include the original list of recipients, however, there is an option to forward the message to additional people.

Is there a set up for spell check in secure email?

That is not part of the system, but most web browsers offer some level of spell check abilities.

Security in Contracts

- Questions

Pablo F Matute
IT Security Administrator
Dept of Social and Health Services
Children's Administration
7240 Martin Way E, Lacey, WA 98516-5533
PO Box 45605
Olympia, WA 98504-5605
Mailstop: 45605
PH: 360/486-2342
Cell: 360/688-4169
FAX: 360/407-0985
pablo.matute@dshs.wa.gov