Washington State Department of Social & Health Services
Transforming lives

DEVELOPMENTAL DISABILITIES ADMINISTRATION
Olympia, Washington

TITLE:	DSHS-ISSUED ELECTRONIC DEVICES	13.06

AUTHORITY

45 C.F.R. Part 164	HIPAA—Security and Privacy
Chapter 42.56 RCW	Public Records Act
Chapter 70.02 RCW	Medical Records—Health Care Information Access and Disclosure
WAC 292-110-010	Use of State Resources

REFERENCE

DDA Policy 8.06, *Telework for DDA Employees*
DSHS Administrative Policy 5.01, *Privacy Policy—Safeguarding confidential Information*
DSHS Administrative Policy 5.02, *Public Records Requests*
DSHS Administrative Policy 5.04, *Records Retention*
DSHS Administrative Policy 15.15, *Use of Electronic Messaging Systems and the Internet*
DSHS Information Security Standards Manual
State Government General Records Retention Schedule
Department of Social and Health Services Records Retention Schedule

PURPOSE

To establish procedures for the use and handling of DSHS-issued electronic devices—including smartphones, laptops, and tablets—to comply with state and federal privacy law, record retention requirements, the Washington State Public Records Act, and the rules of civil and criminal discovery.

SCOPE

This policy applies to all DDA employees in all work environments—whether in the office or elsewhere.

DEFINITIONS

Confidential information means information protected by state or federal law, including information about DSHS clients, employees, volunteers, interns, providers, or contractors that is not available to the public without legal authority.

DSHS-issued electronic device means a device capable of storing information—such as a computer, laptop, tablet, cellphone, smartphone, or other device—owned or issued by DSHS.

Protected health information (PHI) means individually identifiable health information about a client that is transmitted or maintained by a DSHS Health Care Component in any form or medium. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe can be used to identify the individual. The fact someone is, or has been, a DDA client is a piece of PHI. Individually Identifiable Health Information in DSHS records about an Employee or others who are not clients is not PHI. See Administrative Policy 5.03 for provisions relating only to PHI of Clients.

Public record, as defined by RCW 42.56.010(3), means any record prepared, owned, used, or retained by DSHS to conduct business in any format or medium, including electronic data and metadata. Department public records include client records and may include information exempt or protected from production or disclosure to the general public.

POLICY

A. All DDA employees must handle DSHS-issued devices in a manner that minimizes physical and cybersecurity risks.

B. Devices subject to the Public Records Act and discovery

1. If stored or transmitted on a state-owned device, text messages, voicemail messages, email messages are public records and subject to public records disclosure or legal discovery unless privileged or specifically exempt by law.

2. If an employee conducts state business on a personal device, the device may be subject to public records disclosure or legal discovery unless privileged or specifically exempt by law.

PROCEDURE

A. Secure DSHS-issued electronic devices

1. Physical security requirements

a. DSHS-issued electronic devices must not be left unattended at any time

unless physically secured. Devices must be in a locked location when not in use.

b. Do not leave a device with confidential information in an unattended vehicle unless the vehicle is locked and the device is not visible from outside the vehicle.

c. Additionally, every effort should be made to ensure the security of the device, which can include:

i. Parking the vehicle in your line of sight;

ii. Parking in an area with foot traffic, such as near the front door of a restaurant;

iii. Parking under street lights or well-lit areas;

iv. Activating a car alarm if available;

v. When traveling safeguard laptops or tablets containing confidential information; and

vi. Do not leave mobile devices or hard copy information unattended in places where unauthorized access to information is likely to occur, i.e. common areas with public access, vehicles, client residences etc.

d. A locked vehicle parked inside a locked residential garage is considered adequate, unless multiple tenants have access to the garage.

2. Cyber security requirements

a. At all times, follow DSHS Administrative Policy 15.15, *Use of Electronic Messaging Systems and the Internet.*

b. Do not disable programs or applications installed by IT.

c. Do not download or install programs or applications without permission from IT.

d. When prompted by IT to install an update on a DSHS-issued electronic device, do so.

B. Client Privacy

1. Employees must understand how DSHS categorizes information.

a. **Category 1, Public Information** – Public information is information that does not need protection from unauthorized disclosure, but does need protection from unauthorized change that may mislead the public or embarrass DSHS.

b. **Category 2, Sensitive Information** – Sensitive information is not specifically protected by law, but should be limited to official use only, and protected against unauthorized access. Manuals and computer system documentation that is not classified as confidential should be classified as sensitive.

c. **Category 3** – Confidential information is information that is specifically protected by law. It generally includes:

i. Personal information about clients, regardless of how that information is obtained;

ii. Information concerning employee payroll and personnel records;

iii. The source code of certain applications/programs that could jeopardize the integrity of Department information or result in fraud or unauthorized disclosure of information if unauthorized modification occurred;

iv. Proprietary business information.

d. **Category 4** – Confidential information requiring special handling is information for which:

i. Especially strict handling requirements are dictated by statutes, regulations, or agreements.

ii. Serious consequences could arise from unauthorized disclosure, ranging from life threatening to legal sanctions. HIPAA and IRS information, as well as information stored in the Criminal Justice Information System, all fall under Category 4, and there are

different requirements depending on which regulation covers the data. Examples of Category 4 information include:

A) Protected Health Information (PHI), as defined at Administrative Policy 5.01, *Privacy Policy - Safeguarding Confidential Information*, and by the HIPAA Security Rule;

B) Information identifying a person as being, or ever having been, a DDA client;

C) Federal wage data; and

D) Location of an abused spouse.

2. Phone and Video Calls

a. When discussing confidential information, do so in a place where others who are not authorized to know the information cannot overhear.

b. When using a video conferencing tool to discuss Category 3 or Category 4 information, the connection must have sufficient level of security given the category of information being discussed on the call.

3. Texting

a. Any text message sent or received using a DSHS-issued electronic device is a public record. Text messages sent or received in the course of employment that contain information relating to the conduct of government or the performance of any governmental function may be construed as public records under the Public Records Act and subject to retention and disclosure requirements—even if sent or received on a privately owned device. This means that under certain circumstances personal devices may be subject to inspection under the Public Records Act, subpoenaed by a court, or both.

b. Because text messages are not encrypted, employees must not text Category 3 or Category 4 information in any form.

c. Text messages that identify a client are prohibited—even if the recipient is the client. A text message to a client, such as “Running late. See you in

fifteen minutes" is acceptable because it does not contain information that might identify the client or reveal Category 3 or Category 4 information.

4. Photographs

   a. An employee must not photograph a client without the client's written consent, unless doing so is necessary to document potential abuse, neglect, abandonment, or financial exploitation under chapter 74.34 RCW.

   b. An employee must not distribute a photograph of a client, a client's relative or household member – or a client's employer – without the client's written consent, unless doing so is necessary to provide evidence of potential abuse, neglect, abandonment, or financial exploitation under chapter 74.34 RCW.

EXCEPTION

Any exception to this policy must have the prior written approval of the Deputy Assistant Secretary.

SUPERSESSION

None.

Approved: /s/: Shannon Manion Date: 5/27/2021
Interim Deputy Assistant Secretary
Developmental Disabilities Administration