# CONFIDENTIALITY AND DATA PRIVACY
## Minnesota Sex Offender Program

Issue Date: 3/3/26 Effective Date: 4/7/26 Policy Number: 135-5100

.

**POLICY:** All Minnesota Sex Offender Program (MSOP) staff, students, volunteers and persons or agencies under contract must follow all MSOP and Direct Care and Treatment (DCT) policies on confidentiality and data privacy.

**AUTHORITY:** Minn. Stat. § 13, "Government Data Practices"
Minn. Stat. § 144.651, subd 16
Minn. Rule 9515.3040, subp. 2 (A).
Minn. Rule Chap. 1205
Minn. Stat. § 246C.07, Subd. 3(a)(2)

**APPLICABILITY:** MSOP, program-wide

**PURPOSE:** To ensure compliance with DCT requirements and the laws governing client information and data collected and maintained by the MSOP. To meet data privacy laws and professional confidentiality standards, especially regarding the use and results of physiological examinations and the reporting of previously undisclosed and unreported criminal behavior. To provide procedures allowing for optimal therapeutic relationships, while complying with legal requirements for reporting criminal acts. To preserve confidentiality and protect data privacy of written, electronic, and verbal exchanges.

**DEFINITIONS:**

Data on individuals – data on individuals is defined as government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data is not accessed by the name or other identifying data of any individual.

Client record – set of comprehensive documents created in the course of client care from admission through discharge.

Confidential data – data about individuals to which even the individuals themselves cannot have access, e.g., information from an investigation about welfare fraud or in adoption records. Individuals retain the right to know whether an agency is maintaining confidential data about them.

Private – data about individuals allowed to be disclosed only to the subject of the data or to government entities and employees whose work assignments reasonably require access to the data.

Protected health information (PHI) – private information on individuals that is identifiable health information as described in the Health Insurance Portability and Accountability Act (HIPAA) (1996).

Public – data about individuals allowed to be disclosed to anyone for any purpose, e.g., state employee names and salaries of state employees.

Welfare data – data on individuals collected, maintained, used or disseminated by the MSOP pursuant to Minn. Stat. § 13.46, "Welfare Data."

Data not on individuals – data about non-individuals, such as organizations, facilities, corporations, associations, etc.

Protected nonpublic – data not on individuals made not accessible to the public by statute or applicable federal law.

Data privacy – refers to all information on clients gathered for program purposes.

Data security incident – an incident where private, confidential, or PHI on individuals, or protected nonpublic data not on individuals, unauthorized for release, is disclosed to unintended recipient(s).

Security information – (Minn. Stat. § 13.37, subd. 1(a)) government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. Information qualifying as security information under Minn. Stat. § 13.37 is considered nonpublic data or private data and may not be released to the public. This may include data relating to the client, such as impressions, perceptions, observations and/or opinions. Examples of security information include certain incident reports, policies or procedures.

**PROCEDURES:**

A. Client Information - All data on clients, including information in the client record, is considered private or confidential data and may not be released orally or in writing without written consent or as otherwise authorized under state or federal law. This includes records such as property, grievances, etc. Client names are not public information. (Refer to MSOP Policy 135-5300, "Health Information Record Designation.")

B. Requests for Information Stored at MSOP. Refer to MSOP Policy 135-5170, "Data Request and Copy Costs."

C. Safeguarding Information

1. Staff may only discuss and have conversations about clients in the performance of their duties.

2. If staff members question the appropriateness of sharing information, they must consult with the DCT Health Information Management Services (HIMS) leadership and/or DCT Data Privacy Office (DPO).

3. Staff must request, access, use, and disclose only the minimum amount of information necessary to provide services and benefits to clients.

4. MSOP staff must provide PHI to a client by handing it directly to the client or placing the data in an envelope. Refer to MSOP Policy 105-5030, "Staff Mail" and 420-5030, "Client Mail."

5. Staff must participate in annual training regarding confidentiality and data privacy.

6. As part of new employee training, the DCT HIMS Supervisor/designee collects the employee's signed DCT MSOP Employee Confidentiality Agreement (135-5100a). MSOP retains a copy of each individual's signed agreement in their personnel file, student file, volunteer file, or contractor file.

D. Confidentiality within Treatment

1. MSOP staff may only share information disclosed by clients during sex offender treatment and/or medical treatment to the MSOP staff who need the information to perform their job duties. MSOP may share the information with individuals outside of MSOP under the following circumstances:
   a) Staff may share information on a client as part of the judicial commitment process (Minn. Stat. §§ 253B.23, subd. 4 and 253D.03).

   b) Staff members must immediately report information related to maltreatment of minors to the local welfare agency, police department, or county sheriff. (See MSOP Policy 420-5110, "Reporting Maltreatment of Minors.")

   c) Staff members having knowledge or reason to believe that an identifiable vulnerable adult has been neglected or abused must immediately report that information consistent with Minn. Stat. § 626.557 and MSOP Policy 210-5058, "Vulnerable Adults."

   d) The program or staff may disclose client data as otherwise specifically authorized under state or federal law. Staff who have questions regarding authorized disclosures must contact the DCT HIMS leadership and/or DCT DPO.

2. Each client completes the Notice of Privacy Practices (DCT-3542-ENG) and Notice of Privacy Practices Acknowledgement (DCT-3542A-ENG) upon admission, as outlined in MSOP Policy 210-5100, "Admission to the MSOP."

3. MSOP staff or contracted assessors initiating clinical or other treatment program assessments must first discuss the limits of confidentiality with the client and inform the client information disclosed during the assessment will be documented in the completed report.

4. As part of treatment, each client develops an agreed-upon history of the client's offending behavior. Clients are not required to provide the name(s) of the victim(s), date(s) of the offenses, and/or other identifying information in order to participate in therapy or psycho-educational groups or treatment progression.

E. Documentation of Data Security Incidents
1. Upon notification or discovery of an actual or alleged data security incident:
   a) Physical Data – MSOP staff must:
      1) request the individual(s) confirm the extent they viewed or may have viewed the information, including the envelope and any document(s) related to the data;

      2) secure all items, including the envelope and any documents related to the data security incident (if available) and document on an Evidence Inventory Report (145-1035b) following DCT Security Policy 145-1035, "Evidence Handling by Staff;" and

      3) place the Evidence Inventory Report (145-1035b) and the secured documentation into the evidence locker labeled as "Data Security Incident" (locker number 277 for Moose Lake in the Main Building Evidence Room and locker number 112 for St. Peter/Community Preparation Services (CPS) located in the Pexton Lobby locker room) following DCT Security Policy 145-1035, "Evidence Handling by Staff." Staff must write on the evidence bag the documentation secured is for a data security incident.

b) Electronic Data (including email, fax and Client Computer Network):

1) Email – the sender of the email:

(a) attempts to recall the message;

(b) if unsuccessful, request the recipient(s) permanently delete the message and any attachments, and confirm the deletion;

c) request the recipient(s) confirm whether they viewed the information; and

d) forward all relevant email(s) to the MSOP Due Process and Compliance Specialist/designee.

2) Fax – the sender of the fax:

(a) requests the recipient(s) securely dispose of the fax and confirm the deletion;

(b) request the recipient(s) confirm whether they viewed the information.

3) Client Computer Network – MSOP staff:

(a) identify the file name(s) and location where the data is reported to be stored;

(b) provide the information to MNIT via the Minnesota Service Hub – MSOP VocEd/Client Network Reporting requesting the removal of the information with:

(1) client's username/user ID or the client's full name;
(2) the name of the folder(s) the file(s) is/are located; and
(3) the name of the file(s); and

(c) request the individual(s) or client(s) who discovered the information confirm if they viewed the information.

c) The staff writes a Level 2 Incident Report (410-5300a) (Phoenix) (see MSOP Policy 410-5300, "Incident Reports") using the title "611-Data Event" including the following information, if available:

1) the date and time the data security incident was reported or discovered;

2) the name of the individual reporting the data security incident;

3) the location of the data security incident;

4) a description of the information disclosed;

5) the individual to whom the information was disclosed;

6) the response to MSOP staff's inquiry if the recipient viewed the information;

7) a description of how the information was received (i.e., client mailbox, hand-delivered, verbal, e-mail);

8) any steps taken to retrieve the information; and

9) any other information pertinent to the investigation of the data security incident.

2. The MSOP Due Process and Compliance Specialist/designee collects the documentation and any needed information from MNIT promptly and without unreasonable delay.

F. Investigation of Data Security Incidents

1. The MSOP Due Process and Compliance Specialist:

a) logs the data security incident in the Data Security Incident Tracking Log (135-5100b);

b) opens the evidence bag and visually inspects all of the documentation;

c) scans all documentation, including envelopes and the evidence bag;

d) routes the original documentation to the intended client or staff, if possible;

e) contacts the author of the MSOP Incident Report and/or individuals involved in the data security incident for additional information as needed;

f) contacts DCT Human Resources (HR) of any data security incidents involving disclosure of MSOP staff data, forwards any investigative materials received/obtained, and informs DCT HR of the DCT DPO reporting procedure via the Report a Data Security Incident form (DCT Intranet); and

g) completes an investigation of all data security incidents related to disclosure of MSOP client data promptly and without unreasonable delay if the staff responsible is an MSOP staff (or DCT staff who is unable to complete the steps listed in section E.1.c) above).

h) All other DCT staff follow DCT Policy 135-1072, "HIPAA Breach Notification." The MSOP Due Process and Compliance Specialist contacts the supervisor of the staff responsible for the data security event, forwards any investigative materials received or obtained, and informs the supervisor of the DCT DPO reporting procedure via the Report a Data Security Incident form (DCT Intranet).

2. If the MSOP Due Process and Compliance Specialist, in consultation with the MSOP Operations Manager/designee believes the data security incident should be reported to the DCT DPO, the MSOP Due Process and Compliance Specialist completes the Report a Data Security Incident form (DCT Intranet).

3. Once completed, the MSOP Due Process and Compliance Specialist notifies the the supervisor of the MSOP staff responsible for the data security incident. The supervisor reviews the Report a Data Security Incident form (DCT Intranet) with the staff responsible for the data security incident;

G. Reporting Data Security Incidents

1. Following submission of a Report a Data Security Incident form (DCT Intranet), the MSOP Due Process and Compliance Specialist forwards any supporting documentation, to the DCT DPO.

2. DCT DPO staff review the submitted documentation and determine if the data security incident rises to the level of a data breach requiring notification.

3. If the DCT DPO staff determine the data security incident is a data breach requiring notification, they direct the MSOP Due Process and Compliance Specialist to formally notify the client(s) of the data breach. The MSOP Due Process and Compliance Specialist:
   a) routes a notification letter via US Mail to the individual(s) whose data was disclosed without unreasonable delay (the notification required by this section may be delayed if the MSOP Due Process and Compliance Specialist determines that the notification will impede an active investigation);

   b) retains a copy of the notification letter(s), along with data security incident investigation documentation; and

   c) notifies the assigned supervisor of the MSOP staff responsible for the data breach. The assigned supervisor follows up with the MSOP staff responsible for the data breach within seven business days.

**REVIEW:** Biennially

**REFERENCES:** MSOP Policy 135-5300, "Health Information Record Designation"
MSOP Policy 135-5170, "Data Request and Copy Costs"
MSOP Policy 210-5058, "Vulnerable Adults"
MSOP Policy 420-5110, "Reporting Maltreatment of Minors"
MSOP Policy 210-5100, "Admission to the MSOP"
MSOP Policy 410-5300, "Incident Reports"
MSOP Policy 105-5030, "Staff Mail"
MSOP Policy 420-5030, "Client Mail"
DCT Security Policy 145-1035, "Evidence Handling by Staff"
DCT Policy 135-1072, "HIPAA Breach Notification"
45 CFR Parts 160 and 164 – Health Insurance Portability and Accountability Act (HIPAA)
Rules of Criminal Procedure

**ATTACHMENTS:** DCT MSOP Employee Confidentiality Agreement (135-5100a)
Data Security Incident Tracking Log (135-5100b)

Evidence Inventory Report (145-1035b)
Notice of Privacy Practices (DCT-3542-ENG)
Notice of Privacy Practices Acknowledgement (DCT-3542A-ENG)
Report a Data Security Incident form (DCT Intranet)

**SUPERSESSION:** MSOP Policy 135-5100, "Confidentiality and Data Privacy," 11/7/23.
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

/s/
Nancy A. Johnston, Executive Director
Minnesota Sex Offender Program