Policy Name: VI.1 Privacy and Data Protection Policy	**Section:** V Quality Management	**Programs: All**
	Standard/Area:	**Review Date:**
File: P Drive VI.1 Privacy and Data Protection Policy.doc	**Effective Date: 8/25**	**Revision Date**:

Section I: Intent

MVCS is committed to protecting the privacy and personal data of employees, contractors and clients of MVCS services. This policy is intended to protect privacy, provide clear roles, processes, and timelines for handling data and data systems.

Section II: Policy

MVCS will safeguard the privacy, confidentiality, and security of all Personal Information (PI), Protected Health Information (PHI), Behavioral Health Information, and Education Records managed by MVCS across Behavioral Health Services, Early Childhood Education (ECE), and Community Support Services.

This policy applies to all MVCS employees, contractors, volunteers, interns, vendors, vendors' personnel, and any other persons or entities acting on MVCS's behalf (collectively "Covered Persons"). This policy covers data and records in any format (electronic, paper, oral) relating to MVCS clients and participants across all program areas, including telehealth, in-person services, and program coordination activities.

Definitions

Personal Information (PI): Information that identifies an individual (e.g., name, address, SSN, financial data).

Protected Health Information (PHI): Individually identifiable health information held or transmitted by MVCS in any format that is protected by HIPAA.

Behavioral Health Information: PHI and other information relating to behavioral health conditions, treatment, or services.

Education Records: Records maintained by MVCS that are directly related to a student and are created or received by MVCS as part of an ECE program and are considered "education records" under FERPA.

FERPA: Federal law governing access to and disclosure of Education Records.

42 CFR Part 2: Federal confidentiality regulations governing certain substance use disorder treatment records and disclosures.

Psychotherapy Notes: Personal notes created by a mental health professional documenting sessions; given heightened protections under HIPAA.

Program Data Steward: A designated MVCS staff person responsible for data governance within a specific MVCS program area (Behavioral Health, ECE, or Community Support).

Business Associate (BA): A person or entity that performs functions involving PHI on MVCS's behalf and is bound by a Business Associate Agreement (BAA).

Minimum Necessary: The standard to disclose or use only the minimum amount of information needed to achieve a legitimate purpose.

Data Breach: Unauthorized acquisition, access, use, or disclosure of PI or PHI that compromises security, confidentiality, or integrity.

Education Records Release: Disclosures of Education Records must comply with FERPA and applicable MA FERPA regulations, including parental or eligible student consent where required.

Section III: Procedures

1. Roles and responsibilities

   MVCS Privacy and Compliance Office (Privacy Officer): Oversees the privacy program, implements this policy, conducts risk assessments, and serves as the primary contact for privacy inquiries, complaints, and incident responses.

   Program Data Stewards (for Behavioral Health, ECE, and Community Support Services): Manage data inventories, access controls, and data quality within their program area; coordinate with the Privacy Officer on privacy impacts.

   IT Team: Implements technical safeguards (encryption, access controls, monitoring, vulnerability management) and enforces system security across all MVCS platforms.

   Supervisors/Managers: Ensure staff adherence to privacy requirements within their teams; review disclosures and handle program-specific privacy considerations.

   All Covered Persons: Adhere to this policy; complete required privacy training; report suspected privacy or security incidents promptly.

2. Data collection, use, and minimization

Data collection: MVCS collects only information necessary to provide services, ensure safety, coordinate care, support education activities, and comply with legal obligations.

Use: PHI/PI/Education Records are used for treatment, care coordination, billing, program evaluation, quality improvement, and mandated reporting. Any use beyond these purposes requires appropriate authorization or waiver under applicable laws.

Data minimization and purpose limitation: Collect and retain only data needed for the stated purposes; document purposes clearly in notices and consent forms.

Client/parent consent and authorization: Obtain valid consent/authorization for disclosures not otherwise permitted or required by law. FERPA-consented disclosures govern Education Records; 42 CFR Part 2 and HIPAA consent govern PHI related to behavioral health and substance use treatment; ensure cross-program disclosures are aligned with the appropriate legal framework.

Special considerations for sensitive data: Psychotherapy notes require explicit authorization unless otherwise allowed; Substance use treatment records under Part 2 require stringent protections; Education Records under FERPA have specific consent and disclosure rules.

3. Notices of privacy and client/parent rights

Notice of Privacy Practices (NPP): MVCS provides clients/parents with a clear NPP describing how PHI and Education Records are used and disclosed, client/parent rights, and how to exercise those rights. The NPP is provided at intake and available upon request.

Rights include:
- Access to PHI and Education Records in MVCS custody (and for Education Records, rights generally held by parents/eligible students under FERPA; certain jurisdictions may grant access to students at certain ages).

- Right to request amendments to PHI/records that are inaccurate or incomplete (per HIPAA and FERPA as applicable).

- Right to an accounting of disclosures (where applicable under HIPAA; FERPA disclosures have separate procedures).

- Right to request restrictions on certain uses/disclosures (to the extent permitted by law).

- Right to receive confidential communications and to request alternative disclosure methods.

- Right to file privacy complaints and receive timely responses.

Special provisions for minors: Where applicable, MVCS complies with state and FERPA requirements for minors, including assent/consent, parental access, and state law obligations.

4. Confidentiality and disclosures

a) Permissible disclosures without authorization:
- To the client/parent or client/parent's authorized representatives.
- For treatment, payment, and health care operations with safeguards and BAAs in place (HIPAA).
- When required by law (e.g., reporting to public health authorities, child welfare, or as required by a court).
- In emergencies to protect the client or others from imminent harm.
- To contractors or business associates performing services on MVCS's behalf under a BAA.

b) FERPA-specific disclosures for Education Records: Disclosures must comply with FERPA, typically requiring parental consent or an exception (e.g., directory information, study under school-approved procedures, or other permitted FERPA disclosures).

c) 42 CFR Part 2 disclosures: Subject to Part 2 consent requirements and restrictions, including disclosures limited to the minimum necessary and to recipients who will use the information only for the stated purpose.

d) Cross-program considerations:
- When MVCS coordinates care across Behavioral Health, ECE, and Community Support Services, disclosures should be limited to the minimum necessary and may require cross-program data sharing agreements that delineate purposes and protections.
- If an Education Record is involved in a cross-program care plan, FERPA-compliant procedures govern the disclosure, with accommodations for parental or eligible student consent as required.

e) Psychotherapy notes and other sensitive data:
- Psychotherapy notes require separate authorization for most uses and disclosures, except as otherwise allowed by HIPAA.

f) De-identified and aggregate data:
- May be used or disclosed for research, program evaluation, or quality improvement if data are de-identified in accordance with HIPAA and FERPA exemptions where applicable.

5. Data security and technical safeguards

MVCS adopts a layered, defense-in-depth approach across all program areas, with administrative, technical, and physical safeguards.

a) **Administrative safeguards**:
Designate a Privacy Officer

Conduct regular risk assessments and privacy impact assessments for new programs, technologies, or cross-program data integrations.

Maintain written policies and procedures for privacy, security, incident response, vendor management, data retention/disposal, and FERPA data handling where Education Records are involved.

Establish processes for privacy inquiries, access requests, and complaint handling across programs.

Require ongoing privacy and security training for all Covered Persons, including FERPA-specific training for ECE staff.

b) **Technical safeguards**:
Access control with role based permissions, unique credentials, and MFA for sensitive systems.

Encryption of PHI and sensitive Education Records at rest and in transit (e.g., TLS; strong encryption standards).

Network security: Firewalls, IDS/IPS, secure configurations, ongoing patching, and vulnerability management.

Audit logging and monitoring for access/disclosures; periodic audits.

Data loss prevention (DLP) and endpoint protection on devices accessing PHI or Education Records. Secure telehealth platforms with privacy protections; explicit consent for recordings; recordings stored securely with access controls if used.

c) **Physical safeguards**:
Secure storage for paper records; locked facilities; restricted access to devices and records; secure destruction of records when no longer needed.

5 Data retention and disposal

Retention: MVCS retains PHI under HIPAA-defined timelines consistent with clinical, billing, and regulatory requirements. Education Records retention follows FERPA/MA education data retention standards and school-partner requirements, with appropriate alignment to MVCS's educational activities and timelines.

Disposal: Secure destruction of PHI and Education Records when no longer needed (e.g., shredding for paper records, secure deletion for electronic records).

Documentation: All retention and disposal activities are documented and reviewed in governance meetings.

6. Third-party vendors, contractors, and business associates

   BAAs: MVCS enters into BAAs with entities handling PHI and any cross-program data handling. FERPA-compliant data sharing agreements are used when Education Records are involved (e.g., with schools or education partners).

   Due diligence: Conduct risk assessments, security questionnaires, and contract reviews before engaging vendors, ensuring they meet MVCS's privacy and security standards.

   Oversight: Monitor vendor performance, require remediation of any gaps, and include breach notification terms.

7. Research, quality improvement, and data sharing

   Research/QA activities require approvals and data use agreements; use of de-identified data or limited data sets with appropriate data-use provisions.

   Education Records used in research must comply with FERPA, with parental consent or eligible student consent where required.

   Cross-program data sharing for program evaluation should be governed by data-sharing agreements that specify purposes, data elements, access controls, and review processes.

8. Telehealth and remote care

   Use secure, privacy-preserving telehealth platforms with end-to-end encryption and access controls.

   Ensure that cross-program telehealth services respect program data boundaries (PHI vs Education Records) and applicable consent requirements.

   Prohibit recording of sessions unless explicitly authorized with appropriate consent; store any recordings securely, with access restricted to authorized personnel.

9. Training and awareness

   Mandatory privacy/security training for all Covered Persons at onboarding and annually thereafter.

   Targeted training for roles handling high-risk data (Part 2 data, psychotherapy notes, FERPA-regulated Education Records).

   Ongoing campaigns on phishing, social engineering, secure handling of PHI and Education Records.

10. Incident response, breach notification, and corrective action

    MVCS maintains a formal incident response plan to detect, respond to, recover from, and report privacy incidents.

    Contain and mitigate incidents promptly; conduct root-cause analysis.

    Notify affected individuals, regulators, and other stakeholders as required by HIPAA breach notification rules and Massachusetts breach notification requirements (M.G.L. ch. 93H and 201 CMR 17), within mandated timeframes.

    Implement corrective actions to prevent recurrence and document lessons learned.

11. Privacy governance, monitoring, and audit

    Regular risk assessments and privacy impact assessments for new systems/processes, including cross-program data flows.

    Internal audits of privacy and security practices with issue tracking and remediation.

    Annual policy reviews and updates to reflect legal, technological, and operational changes.

    External audits or certifications may be pursued as appropriate for trust and accountability.

12. Rights of individuals and complaint handling

    MVCS provides accessible channels for clients/parents to exercise privacy rights (access, amendment, restrictions, complaints).

    Complaints are acknowledged promptly, investigated, and resolved or escalated as needed.

    Individuals may contact regulatory authorities (e.g., Massachusetts Attorney General, or federal HIPAA authorities for PHI concerns) if concerns are not resolved satisfactorily.

13. Policy enforcement and disciplinary measures

    Violations may result in disciplinary action up to termination, legal action, and penalties under applicable laws.

    Third-party violations may trigger contract remedies, including termination of agreements.

14. Policy exceptions and amendments

    Exceptions require approval by the Privacy Officer or Privacy and Compliance Committee and must be documented with rationale.

    Policy updated at least annually or as laws/operations change.

15. Training and onboarding for new technologies or processes

    Privacy/security risk assessments, approvals, updated BAAs, and staff training completed before deployment of new technologies or data processes that involve PHI or Education Records.

Section IV: Distribution and Training

The Policy and associated attachments are distributed on the MVCS shared Drive (P) and also on the Employee Portal. Notifications related to new, amended, or reviewed policies will be communicated to MVCS leadership and program directors for dissemination to their staff as appropriate. The policy may be directly disseminated to appropriate staff and/or staff groups via email notification after initial dissemination to leadership as per direction of the CEO or designee. The dissemination will be performed by the Chief Operating Officer.

Section V: Legal, Regulatory, Accrediting, and Other Related References and Resources

- HIPAA and HITECH (PHI and security/privacy safeguards for health information).

- 42 CFR Part 2 (substance use disorder treatment records; confidentiality protections for disclosures and consent).

- FERPA (Family Educational Rights and Privacy Act) for Education Records pertaining to MVCS's Early Childhood Education programs.

- Massachusetts data privacy and security requirements (notably 201 CMR 17 and related breach notification requirements under M.G.L. ch. 93H and related provisions).

- Any other applicable federal, state, or local privacy and security laws and regulations. Applicable local, national, and international employment and privacy laws (e.g., GDPR, CCPA, LGPD, FCRA where relevant)

Appendices (examples and templates)
- Appendix A: HIPAA/MA breach logs

- Appendix B: Notification templates for breach