



System-wide Policy: Compliance & Privacy Program

Reference #: SYS-COMPLIANCE-900

Origination Date: May 1998
Next Review Date: March 2027
Effective Date: March 2024

Approval Date: March 2024
Approved By: Audit & Compliance Committee (ACC)

System-wide Policy Ownership Group: Compliance & Privacy Department
System-wide Policy Information Resource: Compliance & Privacy Director

Stakeholder Groups
Compliance & Privacy Department

SCOPE:

Sites, Facilities, Business Units	Departments, Divisions, Operational Areas	People applicable to
Abbott Northwestern Hospital, Buffalo Hospital, Cambridge Medical Center, Allina Health Faribault Medical Center, Mercy Hospital, New Ulm Medical Center, Owatonna Hospital, River Falls Area Hospital, St. Francis Regional Medical Center, United Hospital, Allina Health Group; Allina Health Emergency Medical Services; All other business units	All	All

POLICY STATEMENT:

Allina Health System (“Allina Health”) complies with the laws and regulations applicable to participation in Medicare, Medicaid, and other government-funded healthcare programs and abides by contractual obligations with commercial payers.

Allina Health’s Compliance & Privacy Program (Program) consists of key elements that foster a culture of prevention, early detection, and remediation of conduct that does not conform to the laws, regulations, requirements of healthcare programs or Allina Health’s [Code of Conduct](#). Specifically, the Program facilitates the prevention, detection, reporting, and response to matters including, but not limited to, the following:

- Fraud, waste, and abuse
- Complying with state and federal False Claims laws
- Whistleblower protections
- Responding to governmental inquiries

Allina Health reserves the right to modify, revoke, suspend terminate or change any and all such policies and procedures unilaterally as the company deems appropriate, with or without notice, at any time.

- Business transaction regulatory requirements
- Non-discrimination
- Privacy and confidentiality
- Patient rights
- Patient inducement
- Anti-Kickback Statute
- Conflict of interest and vendor relations
- Excluded providers
- Third-party oversight

The Program meets the criteria set out in the United States Sentencing Commission Guidelines.

Oversight Responsibilities:

Committees: At Allina Health, policy direction and oversight of the Program is provided by internal committees comprised of executive leadership and the Audit & Compliance Committee of the Allina Health Board of Directors.

Chief Compliance Officer: The Chief Compliance Officer is responsible for operating and monitoring the Program. The Chief Compliance Officer reports on the status of the Program, as necessary, to the CEO of Allina Health and, at a minimum, twice annually to the Audit and Compliance Committee of the Allina Health Board of Directors. The Chief Compliance Officer has the authority to report misconduct to the appropriate federal, state, and/or local law enforcement agencies, as deemed necessary.

Standards and Procedures:

Allina Health's [Code of Conduct](#) and Compliance & Privacy Department policies and procedures are integral parts of the Program. The standards set forth in the Code of Conduct are an extension of Allina Health's values and describe the expectations for appropriate conduct to promote and protect the integrity of the organization.

The Compliance and Privacy Department policies and procedures are routinely reviewed and updated and are kept current with changes in applicable laws and regulations. They are available on Allina Health's intranet, the Allina Knowledge Network (AKN).

Training and Education:

Compliance and privacy education and training ensures employees understand their roles and responsibilities as set forth in the Code of Conduct and Compliance & Privacy Department policies and procedures and are knowledgeable about the federal and state False Claims Laws and available whistleblower protections. Upon hire and annually thereafter, all Allina Health employees must complete compliance and privacy education that meets or exceeds the required content of the Centers for Medicare & Medicaid Services (CMS) general compliance and fraud, waste and abuse lessons in accordance with 42 C.F.R. § 422.503(b)(4)(vi)(C) and § 423.504(b)(4)(vi)(C) as well as the Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules (45

Allina Health reserves the right to modify, revoke, suspend terminate or change any and all such policies and procedures unilaterally as the company deems appropriate, with or without notice, at any time.



CFR §164.530 and 45 CFR §164.308, respectively). The Chief Compliance Officer, or designee, reviews the annual compliance and privacy education on an annual basis to ensure the education meets or exceeds the requirements of applicable laws and regulations.

Allina Health Business unit leaders are responsible for ensuring all employees receive the necessary compliance and privacy education and training and that records are maintained. Compliance and privacy education is provided through the following venues:

- New employee education;
- New leader orientation;
- Annual compliance education; and
- Ad hoc, targeted education

Education may be in person, via a remote platform, or via a web-based platform. New employee compliance education must be completed within 30 days of the employee's start date. Any employee, who does not complete the annual compliance education by December 31, cannot work until they finish the education, the Compliance & Privacy Department reserves the right to forgo this rule in the event of unforeseen circumstances.

Monitoring and Auditing:

Ongoing monitoring and auditing activities are guided by an annual risk-based compliance and privacy work plan. The monitoring and auditing activities serve to assess and evaluate the effectiveness of the Program and the underlying standards, and procedures, and to detect criminal and other improper conduct. These activities include, but are not limited to:

- Compliance & privacy reviews on the annual Compliance Work Plan approved by the Audit & Compliance Committee of the Allina Health Board of Directors;
- Provider federal and state exclusion checks;
- Proactive privacy monitoring; and
- Purchasing, key employee, Board Member, provider, and research conflict of interest management plans

Allina Health may engage outside experts to conduct monitoring and auditing activities. Operational leaders, in consultation with the Compliance & Privacy Department, are responsible for the development and implementation of any necessary corrective action plans that result from monitoring and auditing activities.

Reporting and Responding:

All workforce members are required to promptly report any Compliance & Privacy concerns. Workforce members are strongly encouraged to resolve questions and/or concerns by first talking with their supervisor. Individuals may also contact the Compliance & Privacy Department at 612-262-0503 or by e-mail at complianceandprivacy@allina.com. If individuals are uncomfortable with those options, they may also contact Allina Health's Integrity Line, a confidential, 24-hour telephone



resource at 1-800-472-9301, or through their [online report](#). Allina Health's Integrity Line vendor is Ethico, their privacy policy is available at this [link](#).

In accordance with Allina Health's [Code of Conduct](#) and Non-Retaliation policy, retaliation against any person for reporting a Compliance & Privacy Concern is prohibited. Allina Health does not tolerate intimidation, threats, coercion, discrimination, or other adverse action against a person based on this policy or under applicable law and regulation.

Allina Health is committed to reviewing, investigating, and responding to all reported concerns of non-compliance and maintains a documentation repository for reported concerns. Allina Health will take appropriate steps to mitigate potential compliance risks resulting from a Compliance & Privacy Concern. Compliance & privacy will engage other departments and leaders as necessary to investigate the reported concerns to determine if a Compliance & Privacy Violation occurred. Allina Health will report Compliance & Privacy Violations to appropriate entities as required by law.

Enforcement and Discipline:

The Program will be consistently enforced through corrective actions when the results of monitoring and auditing activities or an investigation indicate a violation of the Program, as set forth in the Code of Conduct and Compliance policies, or a law or regulation. When it is determined an employee has violated the Program, law, or regulation, the employee will be appropriately disciplined in accordance with Allina Health's Corrective Action Policy in Workday.

DEFINITIONS:

All capitalized terms have the meanings set forth in the [Compliance Policy Definitions](#)

PROCEDURES: N/A

PROTOCOL: N/A

FORMS: N/A

ALGORITHM: N/A

ADDENDUMS: N/A

FAQ's: N/A

REFERENCES:

Related Regulation and Laws: www.ussc.gov

Alternate Search Terms: N/A

Allina Health reserves the right to modify, revoke, suspend terminate or change any and all such policies and procedures unilaterally as the company deems appropriate, with or without notice, at any time.

Related Policies:

Name of Policy	Content ID	Business Unit where Originated
Outside Interest and Conflicts Management	SYS-COMPLIANCE-909	System-wide
Reporting & Responding to Potential PHI and PII Privacy and Security Incidents	SYS-PSC-701	System-wide
Medical Identity Theft and Fraud Investigations	SYS-PSC-405	System-wide
Corrective Action	HRConnect	System-wide

Policies Replacing:

Name of Policy	Content ID	Business Unit where Originated
N/A		

System-wide Policy