Data Security Statement

LAST UPDATED: July 15, 2025

This Data Security Statement applies to the products, services, websites and apps offered by Loma Linda University Health except where otherwise noted. We refer to those products, services, websites and apps collectively as the “services” in this Statement. This Data Security Statement also forms part of the user agreements for Loma Linda University Health customers, students and patients.

Loma Linda University Health values the trust that our customers place in us by letting us act as custodians of their data. We take our responsibility to protect and secure your information seriously and strive for complete transparency around our security practices detailed below. Our Privacy Policy also further details the ways we handle your data.

Information Security Management Program

Loma Linda University Health’s Information Security Management Program (ISMP) consists of a dedicated staff of Information Security professionals who are led by our Executive Director of Information Security. Since we are both a medical and academic organization, our ISMP meets the data security and privacy requirements under applicable laws and regulations such as HIPAA, HITECH, FERPA, GLBA and GDPR. Furthermore, our ISMP is designed based on industry best practices, standards and control frameworks that are recognized globally.

We practice a risk-based and continuous improvement approach to preventing unauthorized access, use, transmission, disclosure, disruption, modification, storage or destruction of information. We perform continuous analysis of threats and vulnerabilities, combined with the implementation of industry standard security controls across people, process and technology. We collaborate with numerous internal

stakeholders and external partners, while providing visibility and transparency through education, meaningful performance metrics, reporting, and scorecards.

ISMP Practices

Our ISMP comprises practices that are embedded in the day-to-day operations of our business. We assess the effectiveness of these practices on an on-going basis and track any necessary corrective action plans to completion. Below are the categories of our ISMP practices.

1. Organization of Information Security

The Information Security Office maintains the security of the organization's information and information assets.

2. Security Policy

We provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to information security through the issue and maintenance of information security policies.

3. Risk Management

We develop and implement an Information Security Risk Management Program that addresses Risk Assessments, Risk Mitigation, and Risk Evaluations.

4. Access Control

Access to information, information assets, and business processes are controlled based on business and security requirements.

5. Human Resources Security

Processes are in place to ensure that employees, contractors and third-party users are suitable for the roles for which they are being considered, to reduce the risk of fraud, theft, or misuse of facilities. Our workforce receives information security awareness, education, and training on a routine basis.

6. Compliance

The design, operation, use, and management of information systems adheres to applicable laws, statutory, regulatory or contractual obligations, and any security requirements.

7. Asset Management

Management requires ownership and defined responsibilities for the protection of information assets.

8. Physical and Environmental Security

Controls are in place to prevent unauthorized physical access, damage, and interference to the organization's premises and information.

9. Communications and Operations Management

Operating procedures are documented and made available to the workforce who need them. Controls are implemented for the following:

- Third Party Service Delivery
- System Planning and Acceptance
- Protection Against Malicious and Mobile Code
- Information Back-Up
- Network Security Management
- Media Handling
- Secure Exchange of Information
- Electronic Commerce Services
- Systems Monitoring

10. Information Systems Acquisition, Development, and Maintenance

Security is embedded and an integral part of information systems analysis and specification, including in applications, cryptographic controls, security of system files, development and support processes, and technical vulnerability management.

11. Information Security Incident Management

Information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

12. Business Continuity Management

    Strategies and plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if Loma Linda University Health learns of a security breach, we will notify affected users so that they can take appropriate protective steps. Our breach notification procedures are consistent with our obligations under applicable country level, state and federal laws and regulations, as well as any industry rules or standards applicable to us. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers all information necessary for them to meet their own regulatory reporting obligations.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems. We offer TLS to secure the connections to our websites, but you are responsible for ensuring that your systems are configured to support that feature.