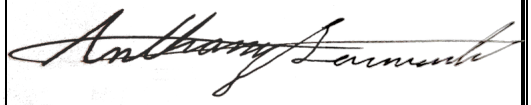
Security Compliance Standards

APPROVALS

	Name	Signature
Prepared by:	Ben Stockett	 ID: D16B59D1-7210-4BB2-8936-8AFDA230EA95 Reason: Authored by <ben.stockett@ligermedical.com> November 10, 2025 10:41 AM MST
Reviewed by:	Anthony Laurienti	 ID: 9A1C62F2-0C2E-4470-A471-65EA99937F52 Reason: Reviewed by <anthony.laurienti@ligermedical.com> November 12, 2025 07:09 AM MST
Reviewed by:	Richard Dixon	 ID: 55A680EF-D780-4A7F-8224-6AFC6DC535EF Reason: Reviewed by <richard.dixon@ligermedical.com> November 10, 2025 10:46 AM MST

1.0 PURPOSE

To define Liger Medical's data security and compliance standards for the EVA and Iris systems, ensuring protection of patient and user information and adherence to HIPAA, GDPR, and ISO 13485 requirements.

2.0 SCOPE

Applies to the EVA and Iris products and associated cloud system, and personnel involved in the handling, processing, or storage of patient and user data.

Security Compliance Standards

3.0 REFERENCES

External References	
Document Title	**Document Reference**
HIPAA Regulation	https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
GDPR Regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

Security Compliance Standards

Delivering Digital Health Peace of Mind: Liger Medical's Security and Compliance Standards

CONTENT

Security Compliance Standards

4.0 ABOUT LIGER MEDICAL

Liger Medical is creating the next generation of smart medical solutions. Our EVA and Iris systems combine biomedical optics with the power and connectivity of mobile technology. Our portable, easy-to-use, and point-of-care visualization and assessment tools can be used everywhere, under nearly any condition, from advanced hospitals to low-resource settings to rapidly improve cervical cancer examinations. The EVA and Iris systems use secure software for superior image and video capture, application of annotations or filters to highlight tissue abnormalities, remote consultation and ongoing quality assurance and training purposes. This ensures cervical cancer examinations are effective, sustainable, and lead to ongoing cost-savings. Our products can also be used for secure, reliable, and simple sexual assault forensic examinations.

Contact:

sales@ligermedical.com
+1 801 256 6576
https://ligermedical.com

5.0 INTRODUCTION

Delivering Peace of Mind

As an enterprise-level medical device and software provider, we understand user and patient data security is nothing less than critical. Our users include some of the world's leading medical institutions for whom maintaining user and patient data security is a top priority. Therefore, we believe in providing full transparency regarding our security standards and practices.

In Summary

The EVA and Iris systems are used for visual imaging and documentation in multiple clinical settings. These products combine the functionalities of a digital colposcope and camera for cervical cancer examinations and sexual assault forensic examinations.

6.0 APPLICATION-LEVEL SECURITY

The EVA and Iris systems include digital magnification, an illumination source, a dedicated Android device, and a secure app and online portal. Images and data captured by our devices at the point-of-care are transmitted to HIPAA-compliant online storage, which are hosted by Google Cloud Platform.

Security Compliance Standards

Security by Design

We make great efforts to ensure the security of data processed on behalf of our users. Our products contain numerous privacy security features, including:

- Patient information collected is accessible only through our apps and online portal.
- Protected Health Information (PHI) is stored encrypted at rest.
- PHI is stored in a secure HIPAA-compliant environment (see section 9).
- Transfer of information from the device to the cloud server is done through a secure, encrypted, HTTPS session and TLS connection.
- Patient information does not transfer between devices, even if the same user logged into multiple devices.
- Patient information is identified per organization, so there is no crossover between information from different organizations.
- All events on the online storage are logged for audit purposes.

The Online Portal

The online portal allows for peer review, quality assurance, and audit of patient information collected by the different providers.

Users can access the information stored on the cloud through the online portal. The portal is accessed through an internet browser in a secure HTTPS session.

Our online portal contains numerous security features, including:

- A username and password for login.
- Different access permissions for users and admins.
- Events log for audit purposes.

Security Testing

As part of every software release, we run a set of tests to verify that data access is properly restricted based on user roles and permissions. Combined with manual testing and regression checks, this process helps identify and prevent security issues.

Security Compliance Standards

7.0 DEVICE LEVEL SECURITY

Our Devices

- A designated device with an Android OS is provided with the EVA and Iris systems.
- Wi-Fi connection is required for application updates and transfer of PHI to our online storage.

The EVA and Iris systems can be used at the point-of-care without an internet connection. PHI will be securely stored on the device and transferred over an HTTPS encrypted channel to the online storage once connection is established or data can be transferred directly to an electronic data management system or to a computer.

Password and PIN

A password is chosen in the initial set-up and app installation. The password policy requires at least 8 characters with a capital letter, non-capital letter, a number and a special character.

After these steps, a security PIN is selected for all future access to the app (according to customer decision), both when the device goes into idle mode or is shut down.

Passwords are chosen by the user and are unknown to our staff.

User Credentials

Each organization can have as many users as needed (a user for each provider is recommended). Users receive different levels of data clearance and access levels according to their position.

8.0 INFRASTRUCTURE

We implement multiple and varied infrastructure security measures to protect customer information from unauthorized access, loss, alteration, viruses, trojans, and other similar harmful code. This includes:

- Swift and regular updates of operating systems, hardware and any third-party software to avoid security vulnerabilities.
- Use of firewalls to limit access and protect the EVA and Iris systems.
- Hardening of all external-facing applications according to industry best practices.
- Backing up customer data with strict encryption rules.
- All communication between remote locations is conducted via encrypted channels.

Security Compliance Standards

Administrative access to our production environment is limited to a restricted number of individuals. Access to additional individuals is given only in extreme circumstances, for a specific purpose, and is limited in duration. Such access to these additional individuals is given only after the explicit approval of the customer.

9.0 CLOUD STORAGE AND HIPAA

As part of our HIPAA-compliance, we have implemented an advanced security incident and event management solution to audit, monitor, aggregate, and correlate security alerts ensuring swift discovery and response to potential security incidents.

A HIPAA-Compliant Solution

Our cloud solution allows for multiple actions, including secure case sharing, data insights, remote consultations, and quality assurance of provider activities.

As a company, we make constant efforts to ingrain good practices among our employees when it comes to data security and privacy. These efforts stem from an ongoing security awareness framework, one that mandates and audits the implementation of all security procedures within the company and aids in assuring the distribution of security principles.

In addition, we try to service our clients most effectively by handling as minimal data as possible and restricting it as much as possible.

We chose Google Cloud Platform as our strategic HIPAA-compliant data facility and have a Business Associate Agreement in place. All our client-recorded data is stored on secure servers located in the United States.

For detailed information about Google's compliance, please visit their website.

Physical Security and Business Continuity

Google's data centers are ISO 27001 and SOC2 compliant.

Security mechanisms in the data centers include:

- Controlled access and 24-hour security.
- Room security via biometric systems and video surveillance mechanisms.
- Strictly limited server-room access to authorized personnel and escorted visitors.
- Environmental controls for equipment and data protection, like fire detection and suppression systems, power redundancy and temperature control mechanisms.

Security Compliance Standards

Google's infrastructure has the highest level of availability, redundancy and incident response mechanisms that provide us with the infrastructure to deploy a resilient IT architecture.

10.0 GDPR COMPLIANCE

Liger Medical is GDPR-compliant across all our applications and as your partner, we want to help you make your process as seamless as possible so that you don't have to worry about compliance and can focus more on running your business.

Data privacy and data security are two sides of the same coin. As our customers tighten their data security measures, we would like to extend a helping hand. We're streamlining the processes for our cloud applications by implementing IT policies and procedures that provide end-to-end security.

11.0 ISO 13485 COMPLIANCE

We are ISO 13485 certified. We view this certification as an independent assurance to our customers of our commitment to the quality of our internal processes as well as provide medical devices and services to consistently meet customers' and applicable regulatory requirements and controls.

These controls are systematically evaluated and updated by internal parties and by external auditors, to ensure that we continually meet both our own internal needs and those of our customers.

12.0 OUR COMMITMENT

We have always honored users and patients' right to data privacy and protection. Starting with collection and processing of only necessary personal and health information, we make sure to always minimize this collection to not go beyond what is required for the functioning of our products.

Over the years, we have demonstrated our commitment to quality assurance and operating according to industry standards and best practices as a medical device and data collecting company, as we've become ISO 13485 and HIPAA-compliant.

Security Compliance Standards

DOCUMENT HISTORY

Date	Revision	CN #	Description of Change	Author
11/10/2025	A	0731	New Document	BRS

DocuSeal

Audit Log

Envelope ID: 361

Verify

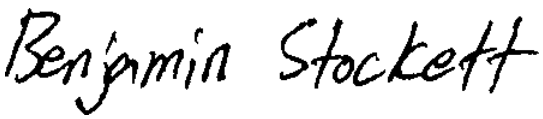
POL-GEN-001.A_Security Compliance Standards.pdf

Original SHA256:
K9ABeSjcpWFVX0oE_ULqas4FqXY6WTTj50gHTsMqPbo=
Result SHA256:
BSgU8l_aJy15PBoM2xbI99WDmN4vUpQR6NLPDT3715w=
Generated at: November 12, 2025 07:09 AM MST

First Party
ben.stockett@ligermedical.com

IP: 67.207.42.131
Session ID: 4b51f8f4fbdffa273fef3f6909d942ad
User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
Time zone: Atlantic/Reykjavik

SIGNATURE FIELD 1

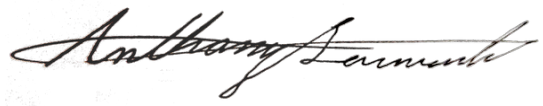


REASON
Authored by

Second Party
anthony.laurienti@ligermedical.com

Email verification: Verified
IP: 136.36.118.50
Session ID: 996896f0ae7abab923a67c33e51de95c
User agent: Mozilla/5.0 (X11; Linux x86_64; rv:144.0) Gecko/20100101 Firefox/144.0
Time zone: America/Denver

SIGNATURE FIELD 2



REASON
Reviewed by

Third Party
richard.dixon@ligermedical.com

Email verification: Verified
IP: 67.207.42.131
Session ID: 4ab0a3b6d9203fa1c3d7784a5d477893
User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Time zone: America/Denver

SIGNATURE FIELD 3

REASON
Reviewed by

Event Log

November 10, 2025 10:41 AM MST	**Email sent** to ben.stockett@ligermedical.com
November 10, 2025 10:41 AM MST	**Email sent** to anthony.laurienti@ligermedical.com
November 10, 2025 10:41 AM MST	**Email sent** to richard.dixon@ligermedical.com
November 10, 2025 10:41 AM MST	**Form viewed** by ben.stockett@ligermedical.com
November 10, 2025 10:41 AM MST	**Submission started** by ben.stockett@ligermedical.com
November 10, 2025 10:41 AM MST	**Submission completed** by ben.stockett@ligermedical.com
November 10, 2025 10:46 AM MST	**Email link clicked** by richard.dixon@ligermedical.com
November 10, 2025 10:46 AM MST	**Form viewed** by richard.dixon@ligermedical.com
November 10, 2025 10:47 AM MST	**Submission started** by richard.dixon@ligermedical.com
November 10, 2025 10:47 AM MST	**Submission completed** by richard.dixon@ligermedical.com
November 12, 2025 07:08 AM MST	**Email link clicked** by anthony.laurienti@ligermedical.com
November 12, 2025 07:08 AM MST	**Form viewed** by anthony.laurienti@ligermedical.com
November 12, 2025 07:09 AM MST	**Submission started** by anthony.laurienti@ligermedical.com
November 12, 2025 07:09 AM MST	**Submission completed** by anthony.laurienti@ligermedical.com