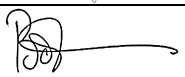
Approval Matrix				
	Name	**Title**	**Signature**	**Date**
Prepared by:	Shahar Libay	Head of AI & Software		30 / 01 / 2023
Approved by:	Leon Boston	CEO		05 / 02 / 2023

Revision History			
Rev.	**ECO**	**Description**	**Date**
01	-	First Issue	N/A
02	-	Second Issue - general updates	N/A
03	-	Third issue - EVA 4.0 (Pro) updates	05 / 02 / 2023

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

CONTENT

1. ABOUT MOBILEODT

MobileODT is creating the next generation of smart medical solutions. Our EVA (Enhanced Visualisation and Assessment) System combines biomedical optics with the power and connectivity of mobile technology. EVA's 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 System uses 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. EVA ensures cervical cancer examinations are effective, sustainable, and lead to ongoing cost-savings. EVA is also used for secure, reliable, and simple sexual assault forensic examinations.

Global Contact:
info@mobileodt.com
US: +1 929 376 0061
Rest of the World: +972 (0)3 757 5959 www.mobileodt.com

2.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 (Enhanced Visual Assessment) System is used for visual imaging and documentation in multiple clinical settings. The EVA System combines the functionalities of a digital colposcope and camera for cervical cancer examinations and sexual assault forensic examinations.

3.APPLICATION-LEVEL SECURITY

The EVA System includes up to 16x digital magnification and illumination device, a designated Android device, and a secure EVA app and online portal. Images and data captured by the device at the point-of-care are transmitted to HIPAA-compliant online storage, which are hosted by Amazon Web Services.

Security by Design

By design, we separate Protected Health Information (PHI) **from non-PHI. We make great efforts to ensure the security of** data processed by the EVA System on behalf of our users.

Our products contain numerous privacy security features, including:

- Patient information collected by the EVA System is accessible only through the EVA app and online portal.
- Protected Health Information (PHI) is encrypted in RSA-256 and separated from patient images for anonymization.

- PHI is stored in a secure HIPAA-compliant environment in Amazon Web Services (see section 5).
- Transfer of information from the phone to the cloud server is done through a secure, encrypted, HTTPS session and TLS connection.
- Patient information does not transfer from phone-to-phone, even if the same user logged into multiple phones.
- 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 EVA 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.

Data Anonymization and Research

Anonymized images may be used by MobileODT for research in medicine, public health studies, and the improvement of our products and technology. We perform data anonymization **by removing personal identifying information from images.**

Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual. This data is stored in a separate storage to ensure that only medical data is used for research.

Penetration Testing and Security Audits

We perform periodic information security penetration tests as well as vulnerability assessment scanning using 3rd-party tools.

4. DEVICE LEVEL SECURITY

The EVA Device

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

The EVA System can be used at the point-of-care without an internet connection. PHI will be securely stored on the cellular 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.

5. INFRASTRACTURE

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 application.
- Hardening of all external-facing applications according to industry best practices.
- Backing up customer data on a daily basis with strict encryption rules.
- All communication between EVA System remote locations is conducted via encrypted channels.

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.

6. 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

The EVA System 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 Amazon Web Services (AWS) 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 AWS's compliance, please visit the AWS website.

Physical Security and Business Continuity

AWS'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.

Amazon'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.

7. GDPR COMPLIANCE

MobileODT 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.

8. 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.

9. 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.

Dropbox Sign

Audit trail

Title	Security & Compliance Standards 10-MR-068 Rev.03
File name	Security & Compli...R-068 Rev.03.docx
Document ID	058da5df093c1e17d03c82869801b64deb96ae1c
Audit trail date format	DD / MM / YYYY
Status	● Signed

Document History

SENT	**30 / 01 / 2023** 09:02:33 UTC+2	Sent for signature to Shahar Libay (shaharlibay@mobileodt.com) and Leon Boston (leonboston@mobileodt.com) from qa@mobileodt.com IP: 82.166.93.77
VIEWED	**30 / 01 / 2023** 13:47:46 UTC+2	Viewed by Shahar Libay (shaharlibay@mobileodt.com) IP: 82.166.93.77
SIGNED	**30 / 01 / 2023** 13:48:58 UTC+2	Signed by Shahar Libay (shaharlibay@mobileodt.com) IP: 82.166.93.77
VIEWED	**05 / 02 / 2023** 14:43:35 UTC+2	Viewed by Leon Boston (leonboston@mobileodt.com) IP: 82.166.93.77
SIGNED	**05 / 02 / 2023** 14:43:59 UTC+2	Signed by Leon Boston (leonboston@mobileodt.com) IP: 82.166.93.77
COMPLETED	**05 / 02 / 2023** 14:43:59 UTC+2	The document has been completed.