maxQ®

Artificial Intelligence

Data Industrialization Security

A White Paper

Table of Contents

It is time for medical organizations to re-assess the potential consequences of complacency, and equip their security teams with the resources they need to keep their staff, and ultimately their patients safe.

Introduction

MaxQ AI is a leading healthcare artificial intelligence (AI) company innovating diagnostic solutions where patient assessment, speed to diagnosis, and healthcare economics converge. We leverage medical imaging data to develop software-based medical devices for prioritization through identification, annotation, and negative triage. This effort requires a heightened sense of information security standards, granular data privacy, and integrity measures. In 2017, MaxQ AI began using the phrase ‘Data Industrialization’ to represent the end-to-end life cycle for data mining and treatment in support of software-based medical devices. This white paper explores the methods we use to help ensure the utmost security during Data Industrialization within the use of our products.

The Importance of Embracing Standards

The stakes are high in ensuring patient safety. Medical device companies need to vertically integrate security into the entire scope of procurement, third-party services, development, testing, manufacturing, and application deployment. MaxQ AI has implemented a multi-year security roadmap strategy that fine-tunes our responsibilities within the medical device community above and beyond having a Quality Management System (QMS) or stringent Software Development Life Cycle (SDLC) procedure. Instead, we have embraced the ISO 27001 ISMS security standard, which requires an annual third-party audit of all business processes including—but not limited to—systems, development, production, manufacturing, Human Resources, Mobile IoT, and physical security. MaxQ AI recognizes that the best way to maintain a commitment to the standards is to adopt a stringent method which requires recertification annually.

Can Standards Live Together?

MaxQ AI Regulatory, Quality, IT, and Security teams agree that an emphasis on higher-level security standards is necessary to improve our quality of care and delivery for our global channel partners. Standards cohabitation is one of the most significant barriers to adopting ISO 27001, and others, such as ISO 13485. Understanding how to use them within a single business process is key to resolving potential conflict in process areas such as risk management, where the approach is from varying vantage points.

Security By Design

In addition to our adherence to standards, MaxQ AI has committed to security by design. For MaxQ AI, this means policies and procedures outlined upfront—supported by a recognized standard such as ISO 27001—to define the general framework and prioritization of security solution roadmaps and deployments.

Solution

Data Industrialized Security

AI is predicated upon access, curation, conditioning, experimentation, and ongoing learning of data. MaxQ AI uses a four-stage 'Data Ops Platform' that delves into each phase and facet of Data Industrialization. The platform is comprised of these modules:

- Data Collection Module
- Data Conditioning Module
- Machine Learning/Deep Learning (ML/DL) Module
- Runtime Module

Technical Information

Data Collection Module

MaxQ AI's Data Collection Module provides the compliance attestation traceability from curation through data cohort design. We undergo data privacy audit/agreement (DPA) checks annually from our channel partners, attesting to the highest standards. Data collected is scanned for vulnerabilities that may reside within the 128-bit pre-amble header. MaxQ AI applies data integrity tools to prevent tampering with medical imaging, and other features to ensure end-to-end traceability as the data is compiled for use towards a final product.

Data collected without proper authorization and attestation is doomed to impact product approval—whether it is in pre- or post-market review(s). Furthermore, without data privacy, integrity, and tracing controls, a medical device is not future-proofed to adhere to current and pending compliance or supplier quality audits.

Data Conditioning Module

MaxQ AI's data conditioning module provides the most advanced truthing and annotation capability with data security and integrity features that meets the ISO 27799 Healthcare Informatics standard. After data collection and secure transfer, a data cohort is created, including truthing and annotations. Ensuring the integrity and traceability of such procedures is eminently clear from a development perspective, where clinical disputes are managed via required source data traceability to back up claims (such as Intellectual Property or Clinical).

Machine Learning/Deep Learning (ML/DL) Module

MaxQ AI understands that selecting a well-known machine learning/deep learning platform (PaaS) service requires Identity Management (Im), Multi-Factor Authentication (MFA), encryption, compliance attestation, and integrated data controls. Our adoption of maintaining strict data security and integrity of the experiments not only safeguards our processes but may assist as a part of an overall patient safety program.

Runtime Module

MaxQ AI focuses on an automated, zero-click, seamless integration into the radiologist's current workflow that automatically routes to the ACCIPIO® platform from the CT or Picture Archiving and Communication System (PACS) equipment. Patient studies are processed without intervention, and the results are returned to the PACS, worklist, originating CT scanner, or any combination thereof. All personal information is deleted after processing so that no Protected Health Information (PHI) is maintained on the ACCIPIO platform.

Key Findings

How Do You Keep Track Of It All?

Maintaining a standard is not hard. It is made easier with productivity and collaboration tools where data is instantly available, with role-based access (RBAC) account administration. MaxQ AI's tool selections are part of our 'security by design' strategy to deploy and efficiently maintain our standards documentation in real-time. We also offer our channel partners and auditors this information as proof positive of our standards adherence.

Data Industrialization – Where does it lead MaxQ AI?

While more and more healthcare systems morph towards the utilization of AI, patient data integrity will be governed by best practices and industry standards. Major manufacturers of medical systems may take an interest in our innovations, but integrating and deploying systems is another story. Demonstrating our industrialized data platform, life cycle management, standards, and compliance enables confidence by both MaxQ AI partners as well as our final end-customer, the acute care facility, to deliver better outcomes based on standards, security, and integrity.

MaxQ AI—The Trusted Brand

At the end process, the results are used in a clinical setting to assist in managing patient care. As such MaxQ AI's, and any medical device manufacture's, main responsibility is the quality and security of the product. This is a core value for the entire MaxQ AI organization. We take great pride in our leadership in this area, with key milestones as detailed below:

- FDA Breakthrough Status, Class II FDA Cleared and IMOH Approved, Class IIb CE Marked and TGA Approved
- ISO13485, FDA QSR, ISO14971, IEC62304, IEC62366 Standards Certified
- GDPR Compliant
- Supports HIPAA Compliance
- ISO 27001 Information Management Security System Certification
- Data truthing by board-certified physicians
- FDA Pre-Certification Member

ACCIPIO is integrated and sold through the following Channel Partners:

GE Healthcare

FUJIFILM

PHILIPS

IBM Watson Health

NUANCE

SAMSUNG NeuroLogica

Blackford

terarecon

To learn more, visit www.maxq.ai or follow us on LinkedIn

Schedule a demo at maxq.ai/scheduledemo/

MaxQ AI Global Headquarters
96 Yigal Alon Street, Entrance A
Tel Aviv, Israel 6789140

COMPREHENSIVE • SEAMLESS • SECURE

*References available upon request: 146

Accipio Ix™: FDA 510(k) Cleared, CE Marked, TGA Approved, IMOH Approved
Accipio Ax™: CE Marked, TGA Approved; U.S. Investigational Use Only*, Not Available for Sale in the U.S.
Accipio Ax Plus™: Investigational Use Only*, Not Available for Sale
Accipio Ax Pro™: Investigational Use Only*, Not Available for Sale
Accipio Dxg™: FDA 510(k) pending, Not Available for Sale
Accipio Dx™: Investigational Use Only*, Not Available for Sale. *CAUTION- Investigational Device, Limited by Federal Law to Investigational Use