A compliance journey to the cloud – how to build a medical cloud platform regulatory- and ISO27000-compliant
Carl Zeiss Meditec
Company Snapshot

- Headquarters in Jena, Germany
- Around 3,000 employees worldwide
- Listed on the TecDAX
- 59% of shares held by Carl Zeiss AG

- Significant sales growth over the last five years
- Strong level of profitability (mid-term outlook: 14–16% EBIT margin)

Revenue in € million
- 11/12: 861.9
- 12/13: 906.4
- 13/14: 909.3
- 14/15: 1040.1
- 15/16: 1088.4
- 16/17: 1189.9

EBIT in € million
- 11/12: 122.9
- 12/13: 133.8
- 13/14: 120.7
- 14/15: 130.6
- 15/16: 154.3
- 16/17: 180.8
As a world-leading medical technology company, we drive progress in medicine, enabling doctors to achieve the best possible outcomes for their patients.

**Microsurgery**
- Complete product range of visualization solutions for minimally invasive surgical treatments (e.g. Neuro, ENT, spinal, dental)
- Intraoperative diagnostics to enhance effectiveness and safety of surgical procedures complete with cutting-edge video technology and three-dimensional imaging

**Ophthalmic Devices**
- Comprehensive solutions to diagnose and treat eye diseases
- Systems and consumables for cataract, retinal and refractive surgery
- Focus on networking of systems and the integrated management of data, to make workflows in hospitals and medical practices efficient

---

© 2018, Carl Zeiss Meditec AG. All rights reserved. – Thorsten Bischoff
You should always have the full perspective
… and do not look through the fog
Cataract surgery in the past
Markerless toric IOL alignment
The Reference Image is the starting point of a markerless toric IOL workflow: an image of the eye is taken along with the keratometry measurement. Both, reference images and keratometry data are transferred to the ZEISS CALLISTO eye® computer-assisted surgery system.
Cataract surgery today – data management, diagnostic and surgery planning

ZEISS FORUM

- Streamline your workflow
- Decide with confidence
- Simplify your environment
Cataract surgery with CALLISTO eye and LUMERA 700

Z ALIGN® – Toric Assistant

Use the reference axis from the ZEISS IOLMaster® 500 and target axis in your microscope eyepiece to ensure precise toric IOL alignment without corneal markers.
Business Motivation – attending surgeons and referring ophthalmologists

How does the patient data come into the operating room today?

Around 70 % to 80 % using an USB stick or manual data entry at the microscope

This is not safety neither secure!

The surgeon needs a solution which helps him to fulfill his liability.
System Architecture – EQ Mobile

Site A – Practice/Hospital

- IOL Master
- FORUM/ EQ Mobile Plugin
- via LAN

Site B – Practice/Hospital

- Personal mobile device of surgeon
- CALLISTO eye/ LUMERA 700
- wireless
AWS Cloud Native Services – Secure EQ Mobile Architecture

- EQ Mobile
- Get Data Key
- Decrypt Data Key
- AWS Key Management Service
- Mobile User
- Authenticate
- Amazon Cognito
- Load
- Amazon API Gateway
- AWS Lambda
- Read Index
- Write Index
- Load/Store
- Amazon DynamoDB
- Update Trigger
- Amazon S3 bucket
- AWS Lambda
- Decrypt Data Key
- Load/Store
Following highly regulated personal data and medical data are collected and processed. The data is needed and processed for administration, billing and as well as maintenance of said service.

**Personal data:**
- People Master Data (e.g. first name, last name)
- Registration data (e.g. user name, password)
- Contact data (e.g. E-Mail, IP-address)
- Specific usage data (e.g. registration status/login, logging of uploads and downloads, reports)

**Patient data:**
- Surgery planning and surgery report
- Diagnose data, keratometry data
- Patient demographic data (e.g. first name, last name, date of birth, …)
- Reference images
Medical regulations

EU Medical Device Regulation (MDR)

BfArM
Medizinproduktegesetz (MDR)

ISO 13485:2016

IEC 62304

HIPAA
Health Insurance Portability and Accountability Act

FDA
U.S. Food & Drug Administration

CFDA
China Food and Drug Administration

aws
Regulations for personal data and cybersecurity

- Privacy Act 1988
- Australian Privacy Principles (APPs)
- Federal Data Protection Act 2018 (BDSG 2018)
- Data Protection Act & Public Health Code

Cybersecurity

Data Protection Act & Public Health Code
Real start of the journey

- We have a secure software, but
- now we have to establish Operations, because of data saving and data processing in AWS
- We have only a tiny feeling about the compliance
- More and more practice and hospitals ask after GDPR and ISO 27001 conform products
- Hospitals become critical infrastructure and request from the suppliers an Information Security Management System (ISMS) and ISO 27001 certified suppliers

→ We need an ISMS and a 27001 certificate
ISMS: Make or buy

• We need the 27001 certificate in 12 months!
• Is this possible within a bigger company with existing processes, quality management system and with all internal stakeholders?
• Do we have the competence to build an ISMS?

Project partners:

direktgruppe  
direkt gruppe is commissioned to build together with us an ISMS and to consult us to be conformable to the compliance

aws  
Technology partner to consult and review our secure AWS infrastructure that complies with the requirements and to introduce the ISO 27001 certification

The Austrian TÜV TRUST IT (TTIT) is involved as a certification specialist via direkt gruppe
How to get an ISO 27001 certificate?

Requirements / expectations for information security

Management Initialization
- Definition of context
- Initiate Management Commitment
- Create Security Policy set
- Build security Organization
- Planning Resources
- Staff training

Analysis
- Definition of Risk Management Methodology
- Analysis of current state
- Identify Security and Compliance requirements
- Threat and Risk Assessments
- Identify Measures

Planning - Realization
- Create the security framework
- Build and realize the security strategy
- Definition of organizational and technical measures
- Configure and implement measures

Operation / continuous improvement
- Regularly Awareness Campaign
- Measurement and evaluation of results
- Carrying out regularly Audits
- Build continuous improvement
- communication

Certificate ISO 27001
- Execute certification audit
- Implement corrective actions from certification audit
- prepare Re-certification

Source: TÜV Trusted IT
Hands-on Information Security Management System

QMS for medical products

IS Strategy
Carl Zeiss Meditec

New Policies and SOPs based on ISO 27001

AWS 27001 certification
highly regulated medical and personal data can be processed in the cloud, but the practice/hospital needs the help of the manufacturer to comply with the regulations and the compliance.
Summary

• Regulatory and Compliance requirements are solved
  • for EQ Mobile and another solution
  • Best prepared for further products and their requirements

• ISO 27001 Certificate was given by third party TÜV Trust IT
  • as approval for best design of solution using AWS services on sensitive personal data

• EQ Mobile Rollout
  • After successful rollout to the pilot markets Germany, France, Australia, US
  • Global rollout to United States, Europe, United Kingdom, Canada, Japan, New Zealand, South East Asia, India, Korea, Brazil, Mexico
Take away

Business enabler – ISO 27001 certificate:

- Marketing: Unique selling proposition to the competitors
- Increase your competitiveness - e.g. demand in tenders
- Minimize IT risks, possible damages and follow-up costs
- Lowering costs
- Speak the language of customers IT departments
- Compliance proof
- Reduce your liability risks
Thank You … and Questions

… for best cooperation!