CHARLTON REGULATORY CONSULTING

Specialist Software Medical Device Consultancy

Dr Iain Charlton CEng

iain@charltonregulatory.com

## About

Charlton Regulatory Consulting aims to give Your Organisation the medical device, privacy and security knowledge it needs to create and manage medical device and healthcare software and services.

I provide consulting and contracting services in regulatory compliance within the SaMD and healthcare software industry. Having created and managed software and systems within this field, I have the experience necessary to help understand and overcome the unique challenges faced by SaMD and and healthcare software service companies in the combination of medical device regulations, privacy and security regulations, and the overlap of quality, risk management, security, privacy and business continuity management standards.

I have direct experience obtaining and maintaining quality management certification to ISO 13485, and achieving CE marking, UKCA marking, De Novo clearance and 510k clearance of novel Class I and Class IIa software devices. I am experienced in creating systems and processes in line with the state of the art quality and risk management standards in SaMD, ISO 14971, IEC 62304, IEC 62366-1, IEC 81001-5-1, the IEC 80001 family, and the US Quality System Regulations and guidance.

I also have direct experience obtaining and maintaining security management certification to ISO 27001 and SOC2 type I and type II. I have developed privacy management systems to ISO 27701 and business continuity management systems to ISO 22301. Having held the role of company Data Protection Officer, I possess in-depth knowledge of the UK and EU GDPR, the US HIPAA regulations, and the UK and EU NIS (Network and Information Systems) Regulations.

I can provide advice and assistance within the UK healthcare sector, ensuring that clients achieve and follow NHS quality and data protection standards for healthcare technology such as DCB0129, DSPT and DTAC, as well as related standards for healthcare apps such as NHS guidance and WCAG.

My regulatory experience is underpinned by over a decade of technical experience developing SaMD and healthcare software, so I have a relatively unique comprehension of the design and production of software, as well as a broad and thorough understanding of the requirements of the standards and regulations. This gives me the insight and understanding necessary to work with technical teams to create processes and design documentation.

Alongside my technical development experience, I have also produced high quality user facing documentation, instructions for use and training material for many audiences.

# Services

The services we can offer businesses in the SaMD and healthcare software space are:

- **Providing advice on regulatory strategy for SaMD and healthcare software**
  Consultation on regulatory pathways and finding routes to market, as well as helping to create strategies for growth and adoption of quality, privacy and security processes as businesses adapt and expand.
- **Providing advice and help in implementing, maintaining and improving business management systems**
  Consultation and assistance in the implementation of policies and processes, staff training and internal auditing activities across quality, security, privacy and business continuity management systems.
- **Preparing regulatory filings under UK, EU and US medical device regulations**
  Assistance planning software medical device design, clinical evaluation and filing activities as well as offering support in creating design documentation and regulatory filings.
- **Technical planning and implementation**
  Helping to plan technical solutions to quality management and software production problems and providing technical support in commissioning, integrating and customising systems such as Atlassian Confluence and Jira, the Google suite, Microsoft 365, and other off the shelf eQMS and design tools.
- **NHS Standards**
  Help with the DSPT, DCB0129 and DTAC standards required to work with NHS Trusts.
- **Labelling and user documentation**
  Advice on product labelling and instructions for use, providing regulatory review of labelling and writing user documentation if needed.

# Skills and Experience

## Regulatory and Standards Compliance

- Detailed knowledge of the UK Medical Device regulation 2002, EU Medical Device Directive 93/42/EC and EU Medical Device Regulation 2017/745, EU In Vitro Diagnostic Medical Device Directive 98/79/EC and EU In Vitro Diagnostic Medical Device Regulation 2017/746
- Knowledge of the EU AI Act 2024/1689
- Knowledge of the U.S. Quality System Regulation (21 CFR 820)
- Creation and management of medical device technical documentation for CE and UKCA marking for SaMD
- FDA De Novo application and 510k clearance of novel SaMD
- Creation and management of ISO 13485 and 21 CFR 820 compliant quality management systems
- Medical device clinical, AI and cybersecurity risk management (ISO 14971, BS/AAMI 34971, AAMI TIR57, IEC 80001-1 and -2, ISO/TR 80002-1)
- SaMD development (IEC 62304, IEC 62366-1)
- Secure software development (IEC 81001-5-1)
- Clinical evaluation (MEDDEV 2.7/1, ISO 14155, UK REC approval, basic knowledge of IRB approval)
- Labelling and instructions for use (ISO 15223-1, ISO 20417) and eIFUs (EU regulations 207/2012 and 2021/2226)
- Creation of ISO 27001 and ISO 27701 compliant information security and privacy information management systems
- Knowledge of ISO 22301 based business continuity management systems
- HIPAA and HITECH compliance of security and information management systems, supporting signing of BAAs
- Implementing and achieving SOC2 certification of security and information management systems
- Knowledge of UK DPA and UK/EU GDPR, with experience as DPO in a complex data controller and processor environment
- Knowledge of the EU and UK Network and Information Systems Regulations (the NIS Directive, DSP Directive and UK NIS Regulations) and compliance with the ENISA technical guidelines for DSPs
- Implementing NHS standards compliance (NHS DCB0129 Clinical Risk Management, Data Security and Protection Toolkit, DTAC)
- Knowledge of Web Content Accessibility Guidelines (WCAG) and the EU web accessibility directive

## Quality Management

- Principal ISO 13485 and CE marking audit representative, from stage 1 and 2, through full certification cycles
- Creating and maintaining policies, processes and procedures
- Vigilance activities including MIR, FSCA, HHE and communicating with Competent Authorities
- Management and registration of economic operators in the UK and EU
- PMS report and PSUR writing
- Creation and management of training and competence systems and resources

## Security and Privacy Information Management

- Principal ISO 27001 audit representative, from stage 1 and 2, through full certification cycles
- Creating and maintaining policies, processes and procedures for ISO 27001, HIPAA and SOC2 compliant systems
- Creation and management of training and competence systems and resources

## Leadership

- Establishing and growing engineering and quality assurance teams
- Establishing best practices and standards for quality, security and data protection
- Creating technical platforms and tools to support engineering teams
- Leading CE marking of novel SaMD and healthcare software
- Leading building quality, privacy and information security systems from the ground up
- Onboarding and training quality and security management leads and staff

## Software and Development Tools

- Support and development ticket management systems (ZenDesk, Jira, Gitlabs)
- Wiki and knowledge management systems (Confluence, and other wiki systems)
- Microsoft tools (Sharepoint, Teams, Flow), including configuration of automated Flow configurations
- Google tools including scripting, customisation and some administration
- Cognidox document management
- Source code control systems (Git, Subversion, Mercurial)
- CI/CD systems (Jenkins, Gitlabs Runners)
- Electronic signature tool introduction and configuration (DocuSign)
- Cyber security feeds and database APIs (MS-ISAC, CISA, NIST NVD)
- Previous extensive experience of C++ application and GUI implementation (15 years)
- Experience with shell scripting and Python
- Some experience Javascript development stacks (Javascript, node.js, SQL)
- Windows and Linux development experience

# Previous and Current Clients

## April 2023 – Present: Radley Scientific

Supporting MDR CE clearance of bone cement removal medical device firmware.

## Mar 2024 – Present: Holberg EEG

Supporting MDR CE clearance and FDA 510k clearance of AI enabled EEG analysis medical device software.

Supporting improvements to software development, cybersecurity and general quality management processes.

## Jan 2024 – Present: Zola Health

Regulatory support and advice on route to market for novel decision support software.

## Aug 2023 – Present: Odin Medical

Improvements to software and cybersecurity processes and procedures.

Regulatory support for new AI enabled products and design changes to existing AI enabled product range.

Supporting FDA 510k clearance of AI enabled software products.

## Jun 2023 – Present: Sonio

Supporting SOC2 type I and type II clearance.

Audit and gap analysis against EU GDPR, creating compliant GDPR policies and procedures to remedy.

Support for 510k clearance cybersecurity documentation for AI enabled medical device software.

## Sep 2023 – Oct 2023: iQ Endoscopes

Software cybersecurity support for 510k clearance of endoscope firmware.

## Mar 2023 – Jul 2023: Taika 3D

Advising on ISO 13485 quality management system implementation.

## Dec 2022 – Nov 2023: Oxehealth

Supporting MDR and FDA 510k clearance of an AI enabled software device.

# Employment History

## 2022 – Present: Charlton Regulatory Consultants

**Director and Regulatory Consultant** www.charltonregulatory.com

## 2004 – Present: IMechE Medical Engineering Division

**Unsalaried Volunteer Position, Vice President for 1 year** www.emhd.org.uk

As a volunteer, I focus on the institution's role in education and professional development, organising and running the annual student competition for five years, and short seminars on human movement analysis.

## 2013 – 2022: Oxehealth Ltd

**Head of Engineered Compliance** www.oxehealth.com

Having joined Oxehealth on day one, I have had many roles, from building and managing the initial engineering team and technology foundations, general operations management, building the product, demonstrating to customers and investors, recruitment, HR, medical device technical file management, quality and security system management, and leading the regulatory and compliance team.

My duties included:

- New product assessment, classification and clearance (CE, UKCA, De Novo, 510k)
- Reviewing and advising on the regulatory landscape (changes to medical device and security regulations, applicability of new regulations e.g. NIS, DSP and web accessibility directive)
- Medical device and economic operator registrations (UK and EU, some experience of U.S)
- Management of the quality and security compliance team
- Being the company Data Protection Officer and Person Responsible for Regulatory Compliance
- Creation and maintenance of product technical files
- Clinical evaluation of new products
- Medical device clinical and cyber security risk management
- Overseeing and monitoring software production processes
- Production of product accompanying information ((e)IFUs and training resources)
- Overseeing, managing and monitoring post-market activities
- Product and process non-conformance management and correction
- Creation and improvement of the company quality management management systems
- Creation and improvement of the company information security management systems
- Being the main representative in all ISO 13485 audits
- Management of compliance with UK NHS standards (DCB0129, DCB0086 DSPT, DTAC)
- Leading new certifications (ISO 27701, ISO 22301)
- Leading quality management review
- Overseeing information security and privacy information review
- Supporting commercial engagement and tender applications on quality, security and data protection matters
- Leading process change as the company scales

### 2001 – 2013: Vicon Motion Systems Ltd

**Chief Biomechanical Engineer** www.vicon.com

As a software engineering lead for Life Sciences products, I was responsible for the full lifecycle of new and legacy medical software products.

My duties included:

- Project management (Waterfall, Agile, Lean, Kanban)
- Software design and development (C++, STL, Boost, Qt, MFC, C#, Python, OpenGL)
- Software test management
- Biomechanics research & development
- Scientific publication and presentation at international conferences
- External supervision and lecturing of Oxford undergraduates and postgraduates
- Supporting ISO 13485 audit of the software production processes

### 1995 – 1998: Cundall Llp

**Mechanical Engineer (Heating and Ventilation)** www.cundall.com

As a design engineer, I was responsible for all aspects of the design of mechanical services for new build and refurbishment projects, including:

- Project management
- Budget estimation
- Health & Safety risk assessment
- Design documentation and specification
- On-site coordination

## Education and Qualifications

### 1998 – 2003: Doctoral Thesis

University of Newcastle upon Tyne

*"A Model for the Prediction of Forces Transmitted at the Glenohumeral Joint"*

### 1992 – 1995: First Degree

University of Durham

First Class B.Sc. (hons) Mechanical Engineering