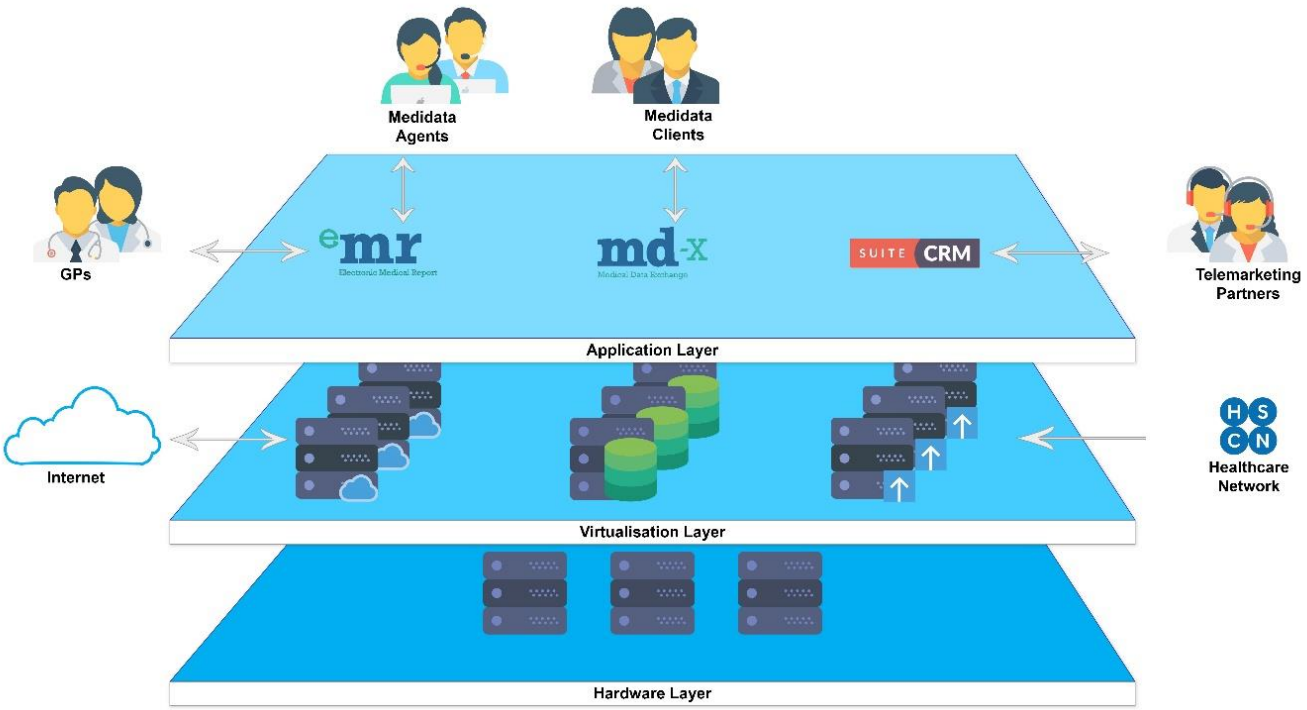
IT Scoping Document

January 2019

An overview of the IT Operations and Application infrastructure for MediData Exchange Limited.

This document will cover the Application Infrastructure, Internal IT, Connectivity, Security Processes, Accreditations and Partners.



1. Application Infrastructure

- **Overview**
  Refers to the physical and virtualised infrastructure that operates MediData's applications. The Infrastructure is operated by Flexiion and is hosted by Dediserve a division of iomart plc within an iomart data centre in Maidenhead, Berkshire, UK.
- **Hardware**
  i. **Development & Testing (Dev/Test) platform**
  The Dev/Test platform are dedicated physical servers operated by Flexiion on behalf of MediData. During development and testing, servers are being hosted within this environment. These servers are high performance blade servers running with SSD storage, multiple multi-core processors and high-performance memory.
  ii. **Production platform**
  The Production platform uses dedicated physical servers operated by Flexiion for the sole use of MediData and for their Application environment and some limited internal IT requirements. These servers are high performance blade servers running with SSD storage, multiple multi-core processors and high-performance memory. In addition to the existing public internet connections, the Production hardware is also connected to the restricted HSCN, connecting MediData to its Primary care customers (NHS environment), which is covered in more detail within connectivity.
- **Virtualisation Layer**
  The Application environment makes extensive use of virtualisation technology, to deploy the servers, services and networking needed to deliver the Applications. The underlying technology is KVM. The primary management and orchestration tool is OnApp.
- **Application environment configuration**
  The Application environment is comprised of Linux Web Servers, a Windows API Server and a cluster of Linux Database Servers to ensure resilience and continuity. These servers have been built during the development and testing processes and have been converted into templates for production, to allow for reliable rollout and recovery in production.
- **Update / Upgrade Process**
  Stable Critical & Security Updates are performed regularly. Further updates to OS or services will be performed within the testing environment prior to being converted to a template for rollout in production.

- **Business Continuity / DR**
  All servers running MediData's applications are regularly and automatically backed up. The physical infrastructure running the application environment will have additional hosts added during production rollout to provide high availability in the event of hardware failure.

- **Connectivity**
  i. **Internal Network**
  MediData's hardware has redundant 1 Gbps internal networking.
  ii. **Public Internet**
  MediData's hardware has multiple public internet facing 1 Gbps connections. The data centre itself has multiple diverse connections from multiple suppliers.
  iii. **Health & Social Care Network (HSCN)**
  MediData has installed an HSCN connection (Circuit ID – mllhscn00073) into the iomart data centre to connect the production environment to the NHs healthcare network. Two circuits have been supplied by MLL Telecom, a primary 50Mb/100Mb Ethernet circuit, with a secondary 80Mb/20Mb EoFTTC circuit.

2. Process & Policies

- **MediData Security Considerations and Processes**
  i. **Data Transit**
  All data transit occurs via HTTPS connections with 3rd party certificate authentication.
  ii. **Data at rest**
  Data is stored on hardware which is dedicated to MediData. Encryption is used across the infrastructure on data storage volumes.
  iii. **Application Security**
  All MediData's applications use usernames and passwords in conjunction with dual-factor authentication to further improve security.
  iv. **Physical Infrastructure Security**
  MediData's applications are hosted on dedicated infrastructure which is hosted within a Tier 4 data centre with the strictest security processes and policies. Access to the site is strictly supervised and by appointment only, with verifiable identification. The site has 24 x 7 security and multiple entry checkpoints to prevent unauthorised access.
  v. **Network Security**
  MediData's infrastructure employs a range of best practice security processes including, but not limited to; multiple firewalls, non-standard access ports,

VLANs to ensure proper network segregation, IP whitelisting, HTTPS-only connections.

vi. **Internal IT**
Through the use of a Remote Desktop solution, no data resides on local devices safeguarding against the loss of computers / tablets.

vii. **Data Destruction**
MediData follows industry regulations (DPA & GDPR) on data retention periods and accordingly the removal of any data. All stakeholders are notified when decisions need to be made regarding the retention of personal data (Patient online access). In the event of any hardware being replaced / upgraded all storage devices will follow strict destruction procedures.

viii. **Office Security**
MediData's office has 24/7 security and CCTV with smart card access to the building and offices within it. MediData's offices are locked and no data or information is stored on site.

- **Data Flow**
The core principal relating to the data flow is that data is only stored where it is authorised to be; within the GP Operating System (EMIS), within MediData's application or with MediData's client's systems. It is never downloaded to a GP surgery or MediData staff device, e-mailed or produced in hard copy during the process of completing a request.
The data flow, through using the application, is as follows:

i. **MediData Client raises a request**
MediData's client raises a request for a medical report, through MediData's application(portal), MDx. This information will include personal information about the patient. This data is stored within MediData's application.

ii. **Request is raised with the patient's GP**
MediData's application will raise a request which will be sent through to the patient's GP. The GP will be notified with limited information and will be required to login to the MediData application to retrieve the request in full.

iii. **Request is completed**
The patient's GP will then process the request within MediData's application drawing information in from the GP Operating System (EMIS) in redacted form. The GP will then manually review the form amending / adding anything relevant to the request before signing off the report within MediData's application.

iv. **Complete report is returned to the client**
Notification of a completed report is sent to MediData's client. The client would then login to MediData's application and review / download the completed report.

- **Accreditations**
Across MediData's infrastructure, business and partners the following accreditations apply.
  i. **Cyber Essentials** – Cyber Security
  ii. **NHS Digital/ IG Tool Kit Level 3** – ODS code: 8JQ49
  iii. **HSCN Connect** – Health & Social Care Network – 2 IP addresses
  iv. **EMIS accreditation** – ODS code: YGM41
  v. **BS 25999-2** - Business Continuity Management
  vi. **ISO 9001** – Quality Management System
  vii. **ISO 14001** – Environmental Management System
  viii. **ISO 20000** – IT Service Management
  ix. **ISO 22301** – Societal Security / Business Continuity System
  x. **ISO 27001** – Information Security Management System
  xi. **OHAS 18001** – Health & Safety Management System
  xii. **PCI DSS Compliance** - Payment Card Industry Data Security Standard

3. Internal IT

- **Desktops/Laptops**
All staff members have company-issued computers. The company's Management Team or those involved in field work use Laptops and anyone who's office-based uses desktops. The devices are locked down to prevent installation of unauthorised applications. These devices are supplied via Dell and are configured by MediData's IT Partner, 5 Rings.
- **Internal Network**
Within MediData's office the company has a wired-only local network providing access to the internet. At home office, off-site and Swansea University the majority of connectivity is via WiFi networks.
- **Remote Desktop Services**
MediData operates a Remote Desktop service for day to day working. All user's login to a server hosted within Flexiion's infrastructure to access desktop services. This server is operated by MediData's IT partner, 5 Rings. This server is setup with Microsoft Office applications, Anti-Virus, strict firewall and security rules and policies.

- **E-mail / Communication**
  i. **E-mail**
  MediData utilises Microsoft's Office 365 for e-mail services.
  ii. **Chat**
  MediData uses Skype & Slack for chat services internally and with key suppliers and Chat Box to assist users setting up eMR.
  iii. **Presentations**
  Zoom is used for presentations and demoing of MediData's systems.
  iv. **Support**
  Team Viewer is used to provide support to GP surgeries where necessary.
- **File Storage**
  MediData utilises Microsoft's OneDrive for Business for document storage and sharing. Files are only shared with users that need access with the most sensitive and internal documents only being available to the Management Team. Documents stored by the company are limited to internal documents and those that relate to the business or business relationships with clients. Patient data is stored within our partner's systems (EMIS) or within MediData's application in report form.
- **CRM**
  As part of MediData's operations the company will use a CRM to store and manage information about clients and GP practices. This information will be accessed and updated by members of the MediData team and by MediData's clients via MediData's application. The CRM in question is Really Simple Systems a cloud-based CRM. Connection to this is via a secure API. Rules have been implemented to prevent unauthorised access and removal of the data from the system.
- **Backup Services**
  All company documents are saved within OneDrive for Business; however, backups are performed daily on the Remote Desktop Server as well as company laptops.
- **Connectivity**
  i. **Leased Line**
  MediData, provided by RapidSwitch, has access to a 100 Mbps EAD circuit installed into their primary office location in Brunel House, Cardiff.
  ii. **DSL**
  MediData, provided by RapidSwitch, has two (2) Multipath ADSL connections installed into their primary office location in Brunel House, Cardiff. These are primarily to provide some backup in the event that the Leased Line connection drops.

iii. **SD WAN**

MediData, provided by RapidSwitch, has deployed an SD WAN (Software-Defined Wide Area Network) solution into their primary office location in Brunel House, Cardiff. This solution aggregates the connections (Leased Line and DSL) to provide greater speed but primarily automatic failover in the event of an outage. The service will also allow for further connections from other office locations and offices to be connected to form a company WAN.

4. Additional Services

- **VoIP**

  MediData has deployed a VoIP phone system provide by Merlin Communications. Each staff member has an internal extension, with either a computer-based phone or physical Grandstream handset. Inbound numbers are routed internally for to the phone system and answered in house. Some calls are recorded for compliance, training and quality purposes and these are stored securely with Flexiion and removed in accordance with data retention guidelines.

- **Office Space**

  MediData operates from several locations:

  i. **Brunel House, Cardiff**

  This is MediData's primary business location and where the majority of the staff are based. The company has a private office within the building with dedicated equipment and services.

  ii. **Business Continuity site, Cardiff**

  MediData has an agreement in place for immediate use of an office for Business Continuity purposes in the event that the Brunel House location is unavailable.

  iii. **Swansea University**

  Swansea University has been heavily involved in the development of the MediData business and applications and MediData has office within the University campus.

  iv. **Home Offices**

  Some of the Senior Management Team are primarily home based. They use company supplied laptops, mobile devices. Connections are typically via consumer broadband services with the Team accessing e-mails and company documents.

5. Partners

- **5 Rings** - www.5ringsgroup.co.uk
  5 Rings are a telecoms and IT Service provider who MediData have outsourced their in-house IT to.
- **EMIS** - www.emishealth.com
  EMIS are one of the largest providers of healthcare technology services to the UK market. MediData have partnered with EMIS to enable access to patient records within the network of practices that use their systems.
- **Flexiion** - www.flexiion.com
  Flexiion is a long-standing partner of MediData who provide a range of Hosted Services to the business.
- **Iomart** - www.iomart.com
  Iomart plc is the parent company for MediData's partners; Rapidswitch and Dediserve. Iomart are a plc which operate several Data Centres around the world and have a range of subsidiaries which provide services to their clients from those sites and others. Flexiion manage the relationships with iomart and their subsidiaries.
  i. **RapidSwitch**
     RapidSwitch provide several connectivity services for MediData but are primarily a Hosted Infrastructure and Service provider.
  ii. **Dediserve**
     Dediserve provide Hosted Infrastructure services for MediData.
- **MLL** - mlltelecom.com
  MLL Telecom are a telecoms business who are providing the HSCN connection for MediData's production environment.
- **Mohara** - www.mohara.co
  Mohara are the lead development partner for MediData, working extensively on the project and application ecosystem.
- **Osborn Technology Partners** – www.osborntp.com
  Osborn Technology Partners is a long-standing partner of MediData who have provided, and continue to provide, technical services and consultancy to the business.