Healthcare provision is evolving in developed nations as these countries have populations that are ageing and becoming more demanding and living longer. Demand is ever increasing, with wider range of treatments being delivered both by public and private sector healthcare providers. Regulatory and compliance is important as medical data has to be managed to legislative standards such as HIPAA, EU Data Protection Directive, covering confidentiality and integrity of healthcare information.

At the turn of the century healthcare providers were using primarily paper based charting, this has been replaced in the following decade by electronic medical records (EMR), such as:

- Picture archival and communications systems (PACS)
- Radiology information systems (RIS)
- Radio Frequency Identification (RFID) systems
- Unified communications

Role based secure communications (RBSC) streamlines the identification process for patients, nurses and doctors from different hospitals, regions or countries to secure compliance and simplify communication within current standards and legislation.
Role based secure communications (RBSC)

Business Outcomes

Roles in hospitals are highly specific and well defined.

*For example:*

A surgical nurse has a very different role than a neonatal nurse, and a radiology tech’s role is distinct from a pharmacy technician. Not only are their roles different; the information and communication requirements vary also. This variance is the case for every role in a hospital and healthcare provider.

RBSC takes into account the various roles individuals play in a healthcare organization. RBSC seamlessly provides for the information and communication needs that meet the work-process requirements of that role.

Delivering an interoperable environment for health professionals no matter their geographic location, to secure integrity of processes and implement legislation, can provide healthcare providers with:

- Identity validation for patients, doctors, nurses, administrators, at local and international level.
- Interoperability in the exchange of information between all stakeholders.
- Protection of patient data according to current standards and legislations.
- Traceability and archiving for all interacting parties for compliance audits.
Pressures

Healthcare providers are under pressure to deliver more services, whilst managing costs, to more patients.

What are the issues that healthcare providers face?

- Solutions today do not have the capability to enable healthcare personnel to easily act in multiple roles (doctors, nurse, or administrator) or connect with other individuals and organizations in a secure and transparent way outside the hospital/healthcare-provider internal IT environment.
- This has led to a digital world with multiple secure “fortress environments” where it is difficult to interact with individuals or organizations outside their own fortress.
- For hospital personnel who are working with sensitive patient data, it is crucial to have the capability to send and receive information to ensure who did what, when it was done, in what role and with whom, in each interaction.

Example 1: Challenges of doctors asking for second opinions from other doctors

- When a doctor needs a second opinion from another doctor with specialized skills, sensitive information often has to be exchanged.
- When exchanging this information hospital personnel ship the documents physically from one hospital to the other.
- An authorized individual has to collect the documents and prove their identity with a personal ID at a service center or a post office.
- This process is both cost and time consuming. It takes a long time to get all documentation to the hospital and several people need to be involved to collect and handle the documentation.

Example 2: Challenges of cross border authentication and interoperability

- When a doctor receives a new patient from another county he or she need to have the patient records from their previous healthcare provider. In general medical record systems do not interoperate well with each other, hence a manual process must be initiated.
- This causes problems and risks for both the patient and the hospitals as it is exposed to multiple risks and human errors.

Example 3: Challenges of receiving patient from other countries

- When a patient arrives from another country to get special treatment in the EU, there is no digital method for transferring patient data according to EU data protection Directive as well as legislation.
- Today, the doctor prints the patient journal and then the patient needs to transport the documents to bring them to the hospital in the host country.
- This causes problems and risks for both the patient and the hospital;
- Time aspect, it is a long process to get all the documentation to the host hospital.
- Lost documents, the risk that the patient will lose their documents. Who is responsible and what consequences can this have?
- No time for preparation, there is no way for the host hospital to prepare, or at all know that it is the right documents being shipped with the patient.
Solution

The Lequinox RBSC solution provides a secure capability for information interchange within healthcare organisations and private individuals.

RBSC solution delivers:

- Capability to track and audit communication interactions.
- To provide compliance to legislative standards against every role defined and to protect and secure the communications.
- To enable manual based, paper based communications to be replaced by electronic communications.
- To increase the speed of communications and reducing time and costs associated with paper based systems.

Approach

Based on the Lequinox platform, distributed by Hewlett Packard Enterprise. This is an innovative approach supporting validation of identities, integrity of processes, traceability of digital interaction, and interoperability between different services.

The Lequinox solution can be applied to existing applications and integrated to provide the RBSC capability.

IT Matters

Ability to digitalize identification process for each role (patient, administrator, nurse, doctor) at national and international levels

Traceability of audit logs to support compliance with signed and time-stamped digital logs

Integrity and confidentiality in the acquisition, and in the submission of information by hospitals, patients, public authorities, and healthcare insurance providers.

- Improve speed,
- Quality
- Control of the information submitted

The Lequinox solution is a decentralized and scalable platform and can be configured to support RBSC aligned to national (country) legal and compliance regimes to enable legal protection and accountability
Business Matters

Time efficiencies for the hospitals and patients due to safe transfer and secure storage of patient medical data and reduced administration costs for paper trails and postage.

Efficient use of information and improved quality of collected data helping health professionals to focus on what matters.

Mitigating risks for non-compliance through archiving and traceability as well as the Lequinox role-base access.

Simplifying and speeding up patient data exchanges between different hospitals, regions or countries to manage emergencies efficiently.

Empowering hospitals, health professionals, and public authorities

Speeding up information exchange between different entities with confidentiality.

Our focus:

- Identity validation for patients, doctors, nurses, administrators, at local and international level.
- Interoperability in the exchange of information between all stakeholders.
- Protection of patient data according to current standards and legislation.
- Traceability and archiving for all interacting parties for compliance audits.

Lequinox Overview

With a Lequinox-based solution for role based secure communication.

The medical professional can attach documents which will be locally encrypted on the device used. No information will be uploaded unencrypted in the application, to ensure secure confidentiality of information transfer.

- To be able to open the information, the recipient will need to have access to the application in the specific role to which the information is has been secured (role based access).
- All actions made in the application during the transaction will be distributed to all participants and stored in the hospital/healthcare-provider archive connected to the specific user and role. This allows the hospital to trace who did what, in what role, and when.
- As only identified users can be addressed in the application, the reference policy sets the rules for what credentials need to be fulfilled.
- Once the patient and the healthcare professional have been identified, the information will then be transferred and addressed to the healthcare professional in the specific role for which he/she is acting in on behalf of the patient.
- When the reference policy is set, it is as easy to send secure information between different hospitals, countries, or between two hospitals in the same county or even country.
- Once the patient and the hospital/department/healthcare-professional have been identified, the information will then be transferred and addressed to the authorized healthcare professional or to an organization with full confidentiality.
Benefits

For hospital personnel that are working with sensitive patient data, it is crucial to have the possibility to send and receive information securely, to ensure who did what, when it was done, in what role and with whom, in each interaction. Therefore the communication is in compliance with national legislation for the healthcare sector.

The solution provides all of the above functions, and make it easy for the users to perform today’s physical processes in a digital way, which will make the hospital/healthcare-provider personnel work more efficiently, whilst still keeping the patient information secure.

Digitalizing the process is both cost and time saving. It much faster to get all the documentation to the right recipient in the hospital and only the authorized personnel have access to the information, eliminating human error, lost files, or late arrival of health records.

Full scale interoperability between hospitals, healthcare professional and patients from different countries.

Timeline to deploy

- Lequinox Platform can be deployed either on private hardware platform or through Cloud28+ / HP Helion Network.

- The applications/services can be connected to the Lequinox platform using APIs (REST APIs) and can be easily integrated with minimal interruption to service. Lequinox platform APIs utilize a set of services and functions to facilitate a dynamic integration with the application process.
Hewlett Packard Enterprise – Value Proposition

Hewlett Packard Enterprise Consulting provides services to accelerate, scope, model and implement the Lequinox™ platform. Helping to adapt customer applications to mitigate risks, reduce time and cost overruns, by framing business requirements for the entire project and testing them, at early stages of the IT project. Ensuring a fully functioning process and compliance prior to investment in the application development and integration phases.

Lequinox™ Solution Design & Modelling Service – Base Service

Hewlett Packard Enterprise Consulting team will collect and validate customer requirements, policies, and user roles, adapt the application/business workflow to fulfill customer requirements and integrate with Lequinox™. Develop a simulation model of the proposed solution to demonstrate its feasibility, and provide a Bill of Materials for the proposed Lequinox™ platform based on pre-defined solution sizes.

Developer Workshop – Optional

Hewlett Packard Enterprise Consulting will conduct an application development workshop to provide consulting services on the design and implementation of the proposed solution, and assist application development teams to understand how Lequinox™ works.

A demonstration of working code samples with the available API’s will introduce developers to the available functions, and assist with the understanding of how to integrate their business applications. A review of implementation plans for proposed application integration development is encouraged.

Security Workshop – Optional

Participating within the Lequinox™ framework and sharing personal information with other parties has also security and liability implications. Therefore Hewlett Packard Enterprise Consulting is offering a security workshop to discuss with customers the implications of sharing personal data with 3rd parties, and being a reference provider.

Developer Support – Optional

Hewlett Packard Enterprise Consulting can provide assistance to application development teams who may require additional support with the APIs or integration with the Lequinox environment.

Hewlett Packard Enterprise Helion CloudSystem Accelerator Service

This service focuses on the installation and configuration of the infrastructure. It includes the initial installation of CloudSystem in customer’s Data Centre and the additional Lequinox™ platform installation with appropriated Cloud Service Automation (CSA) Connector.