Reliable, Secure, Confidential and Safe Integrated Healthcare Record sharing

Janette Bennett – Clinical Director Asia Pacific
BT Health

August 2009

BT Health

Objective

- To discuss lessons learnt from designing and implementing reliable, secure, confidential, safe integrated records from BT's experience in the UK and Hungary

- Enabling Australia to avoid pitfalls and progress implementation plans for integrated health records

Our Experience

UK
- NHS National Programme for IT – Clinical Information Systems, Electronic Health Records, Central Clinical Services, EMPI, VPN, Smart cards, Data warehouse and Pay for Performance services
- Various clients – infrastructure, staff comms, COINS, professional services, NHS Direct/ NHS 24 infrastructure services

Germany
- AOK voice-network to connect its 60,000 employees in 1,600 sites

Hungary
- HEFOP – Electronic health records, telemedicine
- 2million population 30 Institution

US
- Meriter Hospital – staff comms
- Integrated US Healthcare Org - network infrastructure
- Kaiser Permanente - Wireless Hospital

France
- CIP CPS – hosting services for healthcare professional card

Netherlands
- MOH & Science – hosting patient identifier programme
- Bloodbank Sanguin –Managed LAN
- KNMP – Infrastructure, helpdesk

Singapore
- CareLine Department of Emergency
- CareLine Clinic management system
- SingHealth DR & Security solutions
- KKH Desktop & helpdesk outsourcing
- Alexandra hospital service management on apps and infra
- NHG 1-Health portal

Spain
- Ministry of Health – IT services

Australia
- Clinical Risk eHealth Assessment

National and Local NPfIT

National Providers

National Network

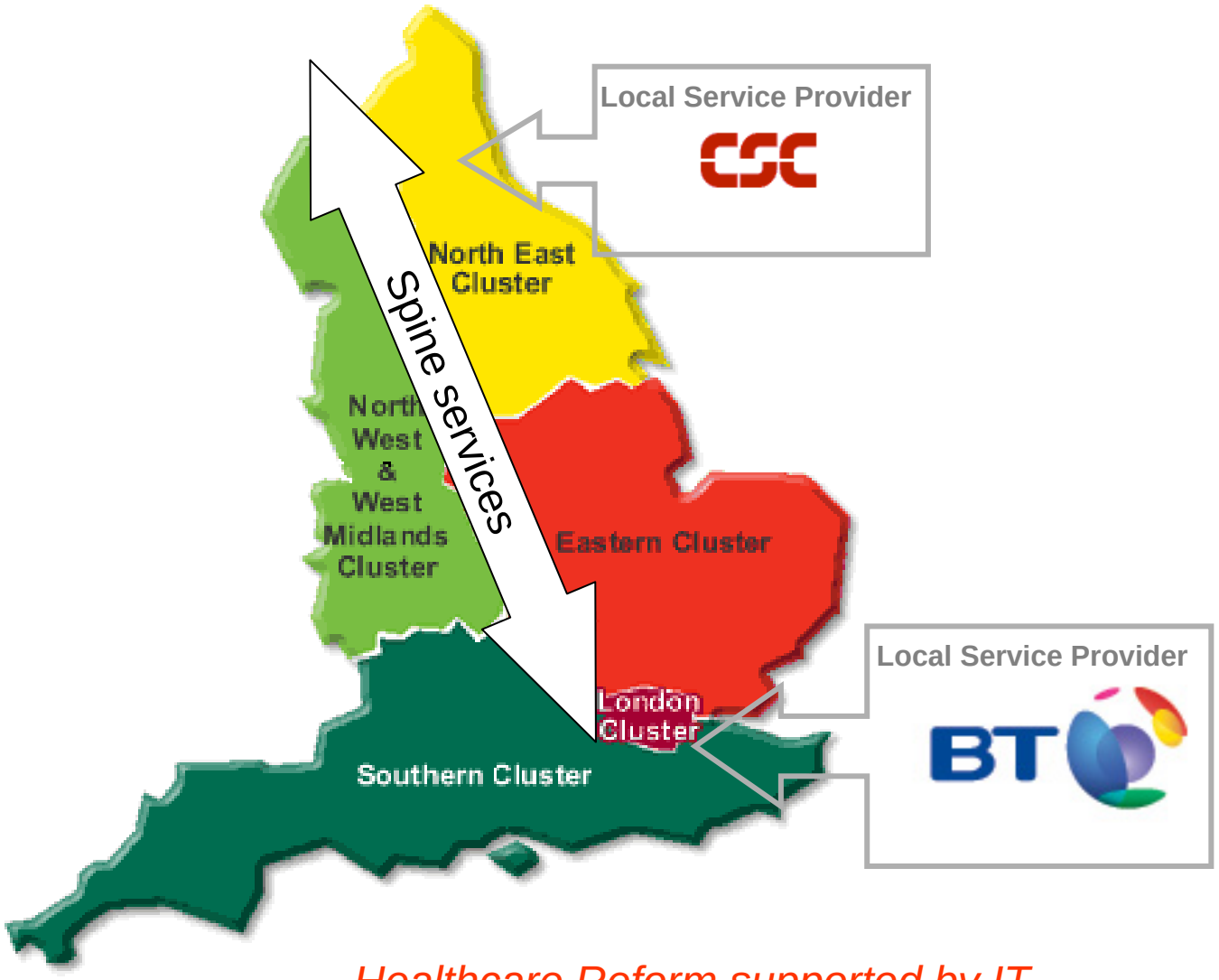
BT

Care Record Service
National Service
Operations Centre
GP 2 GP
Electronic prescription service
QMAS
SUS

BT

Electronic Booking Service

Atos Origin



Healthcare Reform supported by IT

BT

NPfIT

At £12.7 billion, according to Gartner[1] the

- is the largest civil IT project in the wor
- affecting 1.3 million healthcare worker
- more than 50 million patients

BT Technical solution uses:

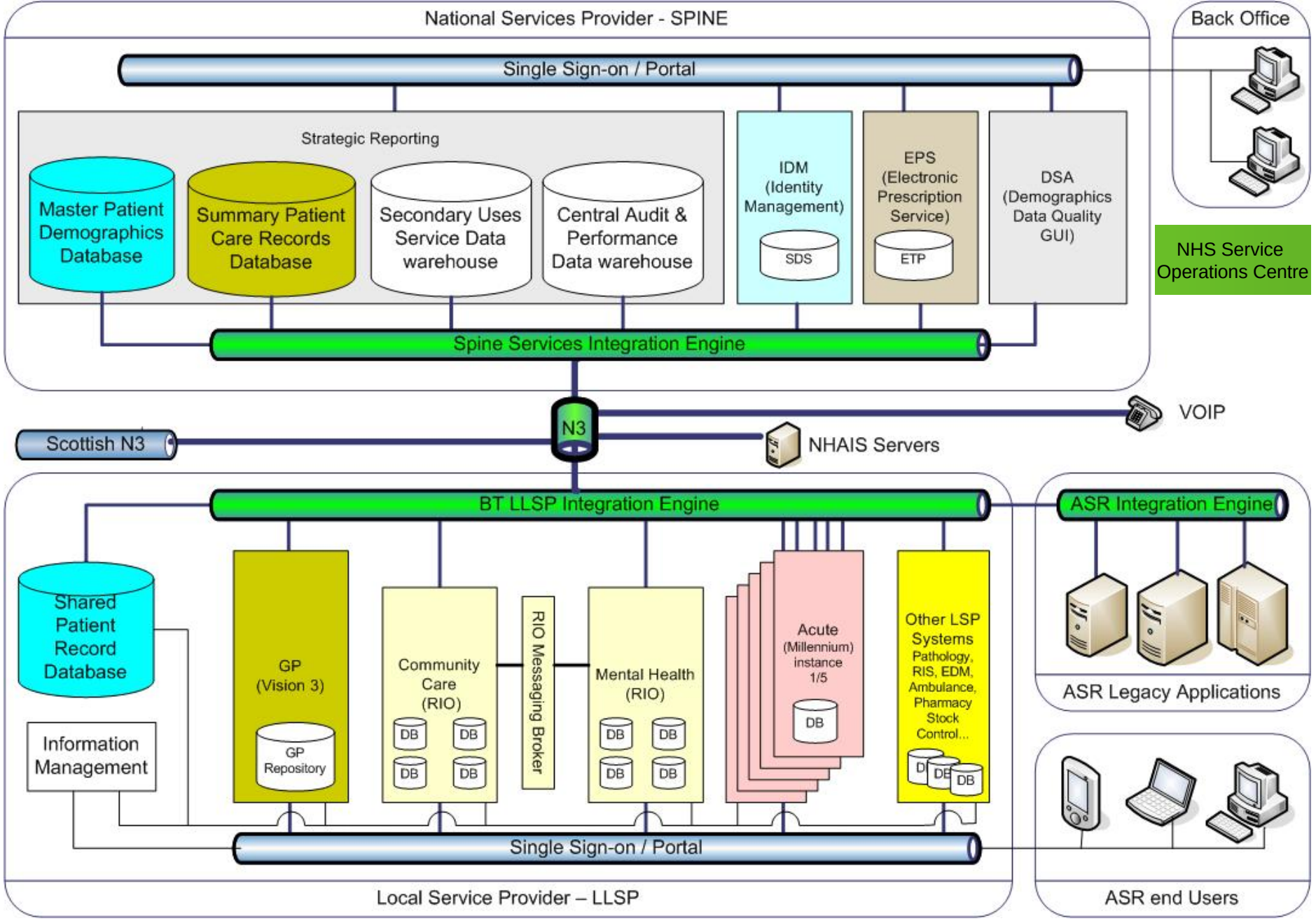
- a blend of COTS products and bespoke Java code through Java EE Technologies
- Service Orientated Architecture (SOA)
- Web Services (SOAP),
- Health Language 7 v3 (HL7 v3) formatted message embedded in ebXML

Pattern based,

- a blend of using both synchronous and asynchronous messaging patterns, facades and orchestrated patterns to deliver complex services to both internal and external services

[1] Gartner 19 May 2008 ID Number: G00155414 Case Study: Architecting an Emergent Business Ecosystem at the U.K. National Health Service. Brian Burke

BT



Reliable

BT

Dec 08

Secure & Confidential

Authentication services

- Spine Security Broker (SSB)
  - management of card and token security
- Card Management System - eHealth ‘Smart’ Card (CMS)
  - management of dual authentication process and access

Clinical service & data security services

- Access Control Framework (ACF)
  - Legitimate Relationship Service (LRS)
  - Role-Based Access Control (RBAC)
  - Workgroups
  - Sealed Envelopes

Identify the Healthcare Professional, role and responsibility

Reliable, Safe: Personal Demographics Service

Interrelated services to assure and improve data quality and accuracy

- PDS Manage Practice List Service centrally manages GP practice lists
- PDS Records Tracking Services tracks and controls paper and electronic records of patients between physical locations.
- PDS NHS Number Issuing Service for new patient records ensuring no duplicate or incorrect NHS numbers are issued or allowed into PDS.
- This unique identifier also sent to remaining legacy systems to ensure forward and backward linking of new and legacy data
- The PDS Tracing Service allows end user to search against the PDS database.
- PDS Data Quality Service uses data from legacy systems and institutions such as the Royal Mail
- Data Migration Service - data is migrated and cleansed from legacy systems
- PDS reports nearly 100 daily.
- NHS Numbers for Babies (NN4B) - creation of NHS national identifiers within hours of birth
    - And more….

Safe -Identify the person

BT

Lessons Learnt: Secure and Confidential

- Where secondary data usage is planned make public the extent of data already held, how that data it is held and why
- Explain and consult on the controls planned to ensure the confidentiality and security of integrated data held for secondary usage
- The patients' right of and mechanism for being informed over their data being accessed must be explicit and agreed
- Each jurisdiction will need to carefully plan the governance of information guardianship and associated processes; audit, breaches
- The concerns of Professional groups must be addressed, and any change in practice and education of staff planned for
- The impact and composition of legislation must be assessed and a public debate held before healthcare IT solutions are integrated

Role Based Access – clarification and standardisation

- Not all healthcare professional groups have centralised publishable registers. These need to be in place to enable a full ACF
- Complexity and diversity of healthcare roles needs to be acknowledged and implications understood before the technical solution is tailored

BT

Lessons Learnt: Reliable and Safe

- Early implementation of a single Patient Master Index (PMI) if it does not exist is crucial
- New data quality issues such as duplicate registrations will occur and back office type functions are always needed at local and national levels to resolve them
- The concept of personal accountability and responsibility for data quality needs to be embedded into the culture of all those involved in health care data input
- Technical solutions need to be constructed in such a way that they mutually enforce data quality
- Demographic data grows stale over time for reasons such as postcode changes for the same property, gender change of the individual or name change through deed poll or marriage. Continual monitoring and improving of data quality is essential.
- Business continuity plans must be in place to address integrated solutions, not just local solutions

Regional NHS London LSP

1 Strategic Health Authority

1 Ambulance Trust

2 Care Trusts

10 Mental Health Trusts

13 Care Communities

31 Primary Care Trusts

32 Acute Care Trusts

1,660 GP Practices

29,000 Hospital Beds

135,500 Hospital and Community Staff

7,200,000 Population+ commuters & tourists

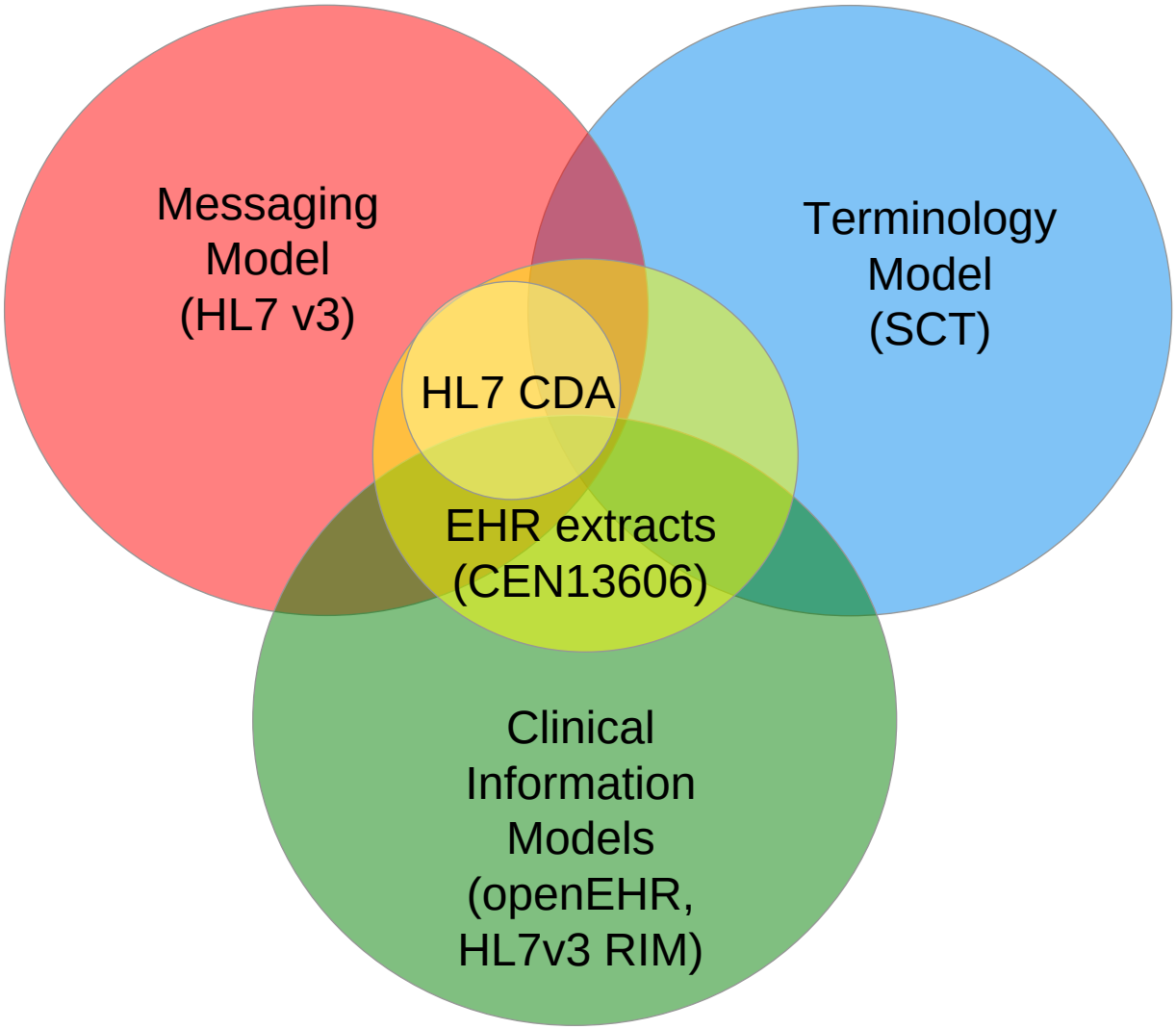
Lessons learnt now used in the South

Lessons Learnt: Reliable, Secure, Confidential, Safe

- Sharing protocols often reflect local service circumstance which will include electronic and other communication media requirements.
- Technology is merely the enabler of change. Change management and clinical transformation is crucial in providing continuous services
- Integrated solutions and shared clinical data are new ways of working. Governance structures need to reflect these changes and new ones created where these are absent
- A collaborative approach needs to be fostered with organisations newly adopting health IT standards and involve clinicians as much as possible
- As much standardisation as possible
- Health is not a greenfield site and careful migration plans acknowledging the constraints of existing legacy solutions needs to be explicit to assure semantic as well as technical interoperability and data transference.
- Clinical Risk Management.

BT

Standards and interoperability



Lessons Learnt: Safe

Emerging International Standards:

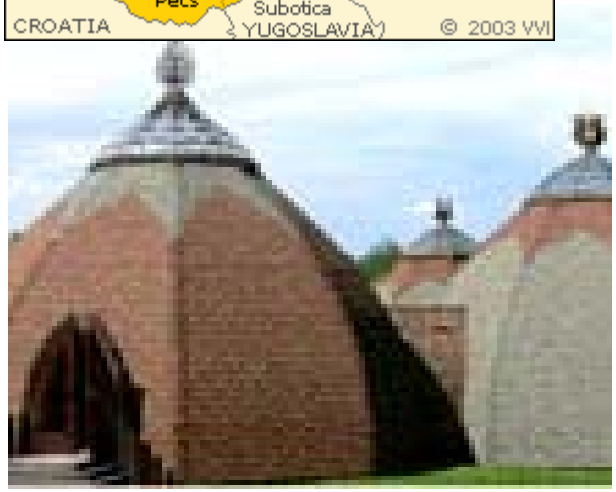
- **ISO/TS 29321 Health Informatics — Application of clinical risk management to the manufacture of health software.**
  - Technical Specification for all manufacturers of health software products and describes the risk management processes required to ensure patient safety in respect to the manufacture of any health software products, whether or not they are placed on the market as an off-the-shelf or configurable product and whether or not they are for sale or free of charge.

- **ISO/TR 29322 Health informatics — Guidance on the management of clinical risk relating to the deployment and use of health software systems.**
  - Technical Report considers the risk management processes required to ensure patient safety in respect to the deployment and use of health software products either as a new system within a health organisation or as changes to an existing system's environment. Addressed to those persons in health organisations responsible for ensuring the safety of health software in health organisations.

Informed by and informing BT's Clinical Risk Management Processes.

Regional: Hungary IKIR

- Developed under EU “IT Development in Healthcare in the Disadvantaged Regions: (HEFOP 4.4.1 initiative).
- The solution connects:
  - 38 health care institutions in Southern Transdanubia, Northern Hungary and Northern Plain
  - 15,000 medical practitioners
  - Population of 1.5 million
- The EHR is a
  - central index service with federated clinical information in repositories
  - a different architecture to the UK but TMS based.
  - similar to that used by other countries with state or regional autonomy of health services.
- The information fully accessible between domains, but not collated as a care summary.
- Patients able to access the solution via a portal and can check data held

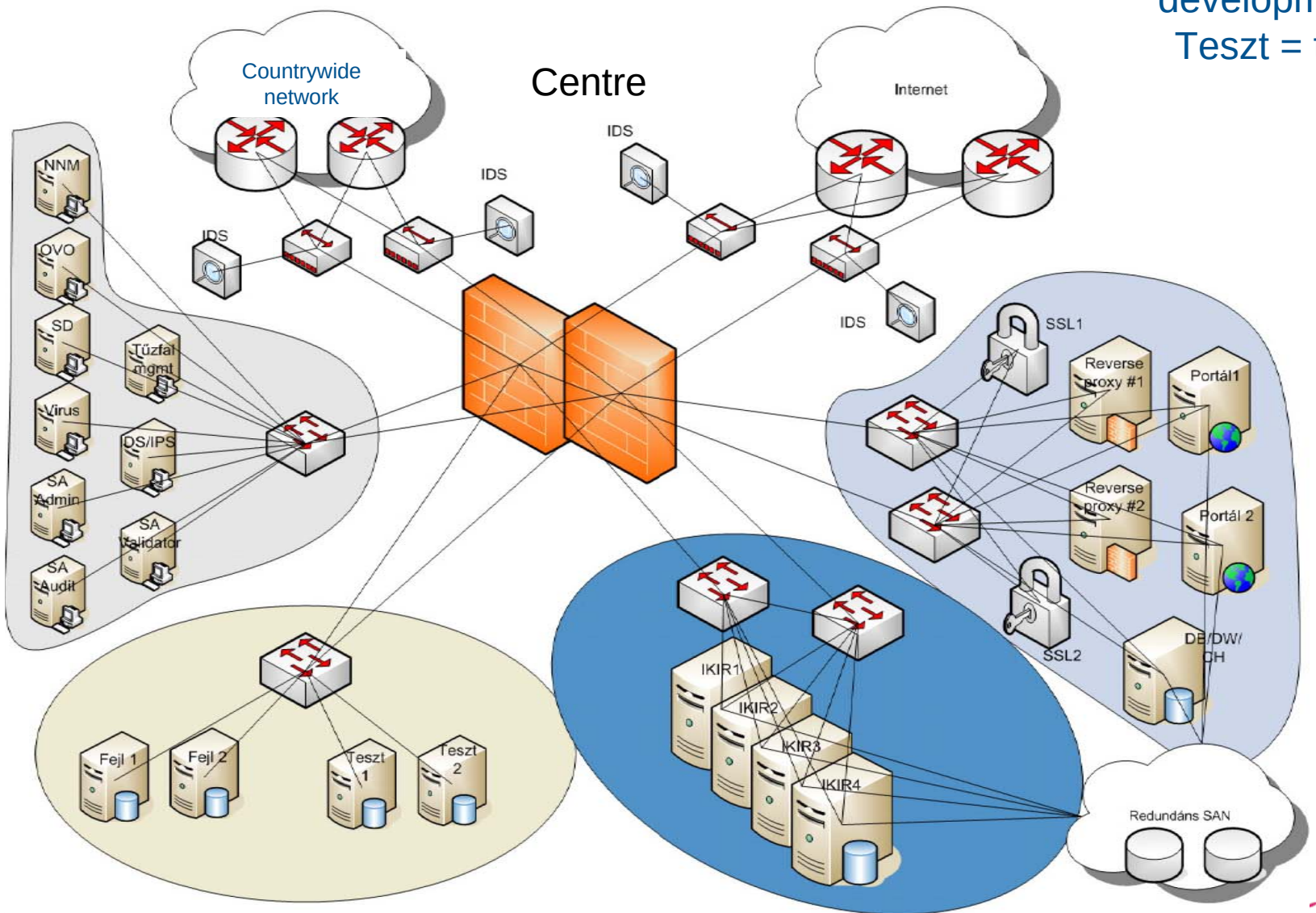


Regional: Hungary cont.

- The core of the system is a message-transmitting engine which
  - supports the secure transmission between healthcare institutions,
  - searches and downloadings documents,
  - handling appointments,
  - transmitting healthcare service requests and answers.
- The solution is predicated on Hungarian healthcare ICT standards, most of which are imbedded within ISDO standards.
- The TMS is different to that used within the UK as the business rules must be peculiar to each country or region.
- The patient registers through a Government Electronic Portal, using its authentication technology.
- The registration is then cross validated against the National Health Insurance Service at a local primary care service and this becomes their record “home” organisation.
- All services now have local components (KRM modules) held in each institution.
- Messages are transferred to the local IKIR servers that are connected to the local hospital information system.

www.kezelnet.hu

Fejl = development)
Teszt = test



Lessons Learnt: Reliable, Secure, Confidential, Safe

- Whilst the TMS needs contextualising to meet country specific rules the principles of adherence to standards and the rigorous verification of conformance and compliance, remains a fundamental requirement
- Data Protection Law had not been tested in earnest and there were multiple opinions on its interpretation.
- The current business solution has been the creation and utilisation of another identifier number that is derived from the unique healthcare ID and this is held in the IKIR service - not categorised in existing law.
- Technical integration brings into focus the need for standardised understanding and representation of clinical information held.
- Policy and process need to be addressed alongside evolving ehealth plans
- Solutions must be tailored to local legislation with the flexibility to adapt to policy development
- Mandation and adoption of international and national standards is imperative for safe transference and retrieval of data
- Standardisation of clinical content must be undertaken if semantic integration is to be achieved

Lessons Learnt: Summary

- Products and services need to fit within a broader national strategic context and framework of standards conformance, compliance and accreditation to avoid the recreation of patient data silos and the resultant clinical risk, and ensure a long term return on investment.
- The demand that all of these services be reliable, secure, confidential and safe is unchanged whether such a service be performed locally, regionally or at a national level.

Bringing it all together