PERSON-CENTRIC INTEGRATED EHEALTH RECORDS

RELIABLE, SECURE, CONFIDENTIAL AND SAFE

Janette Bennett
Director BT Health Asia Pacific

This article discusses two of the many eHealth implementations done by BT: the English National Programme for IT (NPfIT) and Hungary IKIR. BT has found that the interaction between patient and clinician and the needs and pressures of operational managers and policy makers are very similar in any country and setting. Any supporting technical solution, however, always requires contextualisation to the country's legal, financial, economic, demographic, geographic, technological and cultural landscape. There is no 'one size fits all' solution, but experience and lessons learnt are always reusable, especially in the areas of reliability, security, confidentiality and safety of information.

INTRODUCTION

There are many reasons for having reliable person-centric health records.

They can reduce risks of error and clinical misadventure due to a lack of information about the patient and diseases, drug to drug interactions and contra indications. Patients can be better informed and exercise more control over their own health and healthcare living longer and fuller lives, and patients do not have to repeat themselves or risk forgetting things where they deal with several healthcare professionals. According to one estimate, as much as AUD$ 2050 million could be achieved from computer interpretable interoperability. (Sprivulis et al 2007).

Improved efficiency can help the aging healthcare workforce cope with increasing patient workloads, enabling the delivery of more complex care with less staff. As healthcare is increasingly delivered in the home and the community, using telemetry, biometrics and a mobile workforce crossing organisational boundaries, information about patients must be available when and where it is needed, and not tied up in individual organisations or locations.

The benefits, however, need to be balanced against concerns over confidentiality (NEHTA 2008). In finding the balance, the concerns of all those involved in healthcare delivery need to be addressed. Individuals want reliable clinical information immediately, to care for themselves and their family, and clinicians want it to maximise clinical effectiveness, safety and the use of their own time. Others need clinical management information, usually anonymised, for secondary purposes. Operational managers of health services need an overview of complex individual and aggregate patient activity to best use resources such as theatres, beds and community nurses to meet demand. Policy makers considering how and where to invest to improve the health and healthcare experience of those they are responsible for need to know of interventions and outcomes, whether it be in health education or the use of a new cancer drug.

Policy makers and strategists already have access to health data, such as disease registries for cancers, chronic diseases and infections, to identify areas in need of investigation and intervention, but these are silos of information which are not captured in "real time" and do not enable meta analysis. Fast, reliable information is also increasingly important because of the growing incidence of co-morbidity (a primary disease(s) accompanied by others) in aging populations, and because some infections are presenting epidemic consequences. To meet everyone's needs and concerns, information needs to be shared reliably, securely, confidentially and safely.

This article discusses two of the many eHealth implementations done by BT (British Telecom): the English National Programme for IT (NPfIT), and Hungary IKIR. BT operates in over 170 countries and has been delivering health projects in the UK, Spain, Netherlands, Hungary, Singapore and more for several years.

The company has found that the interaction between patient and clinician and the needs and pressures of operational managers and policy makers are very similar in any country and setting. Any supporting technical solution, however, always requires contextualisation to the country's legal, financial, economic, demographic, geographic, technological and cultural landscape. There is no 'one size fits all' solution, but experience and lessons learnt are always reusable, especially in the areas of reliability, safety, security and confidentiality of information.

A NATIONAL SOLUTION: ENGLISH NATIONAL PROGRAMME FOR IT (NPFIT)

Today, BT sits at the heart of the biggest-ever IT programme for the National Health Service (NHS) - the NPfIT. Commencing in 2003 the project essentially puts England's health system 'on-line' and supports the drive to improve care by allowing authorised clinical and administrative staff, as well as patients, to have the right information, at the right place, at the right time. At £12.7 billion affecting 1.3 million healthcare workers and more than 50 million patients, the NPfIT is reported by Gartner to be the largest civil IT project in the world (Burke 2008).

The high level solution set provided by BT includes the following 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. It is pattern based, using both synchronous and asynchronous messaging patterns, facades and orchestrated patterns to deliver complex services to internal and external services.

RELIABLE: TRANSACTION MESSAGING SERVICES AND PATIENT IDENTIFICATION

Prior to the NPfIT, technology development and deployment in the NHS had been uncoordinated. The result was a multitude of systems of varying quality and capabilities, even including some old systems running on operating systems that were no longer formally supported.

At the centre of the NPfIT lies the 'Spine'. It gives authorised healthcare professionals faster, secure access to reliable information about patients, helping the NHS to operate more efficiently. The basis of the Spine is a gigantic Transaction Messaging Service (TMS) connecting over 20,000 system instances from more than 300 suppliers of hospital, GP and community systems. This central infrastructure is now processing 2 trillion messages a year. At the core of safely exchanging all this information is the ability to correctly identify the patient.

Before the NPfIT, there was no single source of patient information, which was dispersed between legacy systems with duplication and incomplete data held in multiple places. The Personal Demographics Service (PDS) is focussed on the creation of a master Patient

Demographic Database, the master patient list that contains non-clinical information critical to the process of identification before clinical care can be provided. It is not a single service but is comprised of many interrelated services that triangulate to mutually assure and improve data quality and accuracy and thereby safety. Some of these services are:

- PDS Manage Practice List Service centrally manages general practitioner practice lists
- PDS Records Tracking Services tracks and controls the paper and electronic records of patients between physical locations. Previously paper records were sent between GP practices by post, and not tracked, often not reaching their destinations
- PDS NHS Number Issuing Service (NIMS) controls the NHS numbers that are issued for new patient records centrally. This ensures no duplicate or incorrect numbers are issued or allowed into PDS. A unique identifier is issued to all patients to be used in all eHealth systems that are replacing legacy systems. This identifier is also sent to the legacy systems that will not be replaced to ensure forward and backward linking of new and legacy data
- The PDS Tracing Service allows end users to trace (search) against the PDS database. The integrity of address, gender and date of birth are critical in identifying patients These traces include the ability to identify babies, verify NHS unique identifier number, verify address, names and other more complex traces. These include an algorithmic advance trace which uses a Cartesian join algorithm and rates the results to identify those that closely fit the search criteria
- PDS Data Quality Service uses data from legacy systems and institutions such as the Royal Mail, in addition to business rules and work item tasks to improve the data quality of the PDS database. As more institutions join the NHS NPfIT, so more – but potentially incomplete, out of date or conflicting – information becomes available. With all the patients in a single database a lot of duplications and confusions can be resolved using merge, unmerge, confusion resolution and address update components
- The Data Migration Service is part of the PDS. Up to 70 million records are migrated and cleansed from each legacy system before loading into the master database

BT learned several lessons from its experience in these areas. If a single Patient Master Index (PMI) does not exist, early implementation of it is crucial. Data quality is critical and legacy data requires deep cleaning before it can be utilised with integrated services. 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 healthcare data input. Technical solutions need to be constructed in such a way that they mutually enforce data quality. Business continuity plans must be in place to address integrated solutions, not just local solutions. 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.

RELIABLE: SECONDARY USES

The NPfIT Secondary Uses Service (SUS) will be one of the largest clinical data warehouses in the world, providing anonymised patient-based data: a powerhouse for public health and medical research, development and business planning. NHS confidentiality policy now requires that pseudonymisation is used in all NHS based secondary use data handling however that information is garnered.

SECURE AND CONFIDENTIAL: ACCESS CONTROL FRAMEWORK

All data that passes within the NPfIT is subject to a stringent Access Control Framework (ACF). The ACF itself uses information within the PDS, care records service, identity management and SUS with all activity informing the audit service. ACF is not just about technology. Most importantly, it is about people and process. Intended users must first give evidence to a Registration Authority (RA) as to who they are, and along with sponsorship from their employer(s), what access they need so that they can undertake their role(s) within healthcare. Directory services are also needed to enable the validation of healthcare practitioners and organisations transmitting, receiving or accessing data.

Role Based Access Control (RBAC) is concerned with controlling which users can have access to which application functions, based on the roles(s) they perform, and consequently what kinds of data they can access. It forms a vital piece of the information security jigsaw along with legitimate relationships, patient consent, sealed envelopes for information, audits and the existing professional, legal and ethical controls supported by disciplinary procedures.

Many lessons were learned from this experience. The complexity and diversity of healthcare roles needs to be acknowledged, with the implications understood and communicated in terms of people and processes before the technical solution is tailored. Obtaining agreement of a set of "standard" user roles between regions is a lengthy process; time invested "up front" will be amply rewarded in later stages. There needs to be a balance between defining sufficient roles to accommodate the granularity of rights associated with these and a model that becomes untenable to maintain practically. Health organisations change over time through merging and other restructures. This has an impact on RBAC, identity management and access control generally. Such changes are often very complex to change in production systems if these are not designed to accommodate change from the outset.

Access Control Framework: Legitimate Relationships

A user must have a 'legitimate relationship' with a patient in order to gain access to the NHS Care Record Service clinical records of that patient.

The patient will be seeing, at different times, unexpected members of care teams, visiting specialists, community intervention teams and so on. This requires the ability to create new legitimate relationships at all times and is especially beneficial at times of crisis when emergency care is required by new care teams. Functionality exists to support the creation of a Self-Referral legitimate relationship allowing a user to select a patient for care. This also allows care professionals in the same workgroup to access the patient's appropriate clinical record. This self-declaration of course requires oversight to ensure there is a genuine legitimacy. However, if every relationship is reported to an information guardian, then the risk is that inappropriate access is lost in the white noise created.

BT has learned that data guardianship, mechanism, process and anticipated volumes need to be debated and made clear to all stakeholders. The patient's right of and mechanism for being informed over their data being accessed must be explicit early in any programme. Each jurisdiction will need to carefully plan the governance of information guardianship.

Access Control Framework: Consent

The evolution of healthcare has often resulted in sharing patient data without their explicit consent of the patient. With the transition to electronic records and changing privacy legislation, this aspect has had to be considered very carefully. Patients must give explicit contemporaneous consent before a clinician can open a shared record. BT has learned several lessons about the opt-in or opt-out choice offered to patients. Changing custom and practice is never easy, and the idea of a clinician or organisation being the sole owner of individual patient data has become questionable in most of the world. The concerns of professional groups must be addressed, and any change in practice and education of staff addressed. Clinical risk aspects of opt in and opt out models need to be understood by all. The impact of legislation must be assessed and a public debate held before healthcare IT solutions are integrated.

Access Control Framework: Audit

By far the largest amount of information held in the Spine is the audit log. For every piece of data sent, retrieved or viewed, there is a full audit trail of who did what, where and when and, in the case of Legitimate Relationships and referrals, also why. As a result, for every data item held about the patient, there is a related audit log of 4 to 5 times the volume.

Information governance structure, rules and processes must be in place prior to programme design and deployment. The implications of storing this volume of data and how it is to be accessed need to be fully understood by purchasers and providers of solutions.

SAFE

Connecting tens of thousands of local systems and facilitating clinical information flows between them needs governance over the sharing of clinical information to know not just who sent what to whom and when, but that the content of the message is consistently captured to assure no inadvertent technical event has altered the intended clinical message in any way.

The solution was to define a set of interoperability standards and services that have been implemented and integrated within the entire healthcare ecosystem. Open standards are used whenever possible to enable the interoperability that the NHS requires and the diversity to meet individual business needs.

However this multiplicity of standards, such as Health Level Seven (HL7) version 3, clinical document architecture (CDA) version 2, Systematised Nomenclature of Medicine (SNOMED) and Electronic Business XML (ebXML), have rarely been used together in integrating national and local systems. Compliance to standards is readily achieved by most products independently, but to work in an integrated way, the standards need to be constrained to ensure technical robustness and to maintain clinical and semantic integrity.

INTEGRATED NATIONAL SERVICES

BT learned many lessons about reliability, security, confidentiality and safety from this large project to provide integrated national services.

On *reliability*, creating inclusive technical boards from an early stage encourages negotiation and compromise between integrating parties. The non-functional requirements such as message volumes and performance targets are frequently more challenging than the functional integration requirements. Version control and ensuring compatibly with previous releases as the service evolves is challenging. Integrated solutions and shared clinical data are new ways of working. Governance structures need to reflect these changes, with new structures created where these are absent. A collaborative approach needs to be fostered with organisations newly adopting health IT standards, involving clinicians as much as possible. As much standardisation as possible needs to be enforced and local tailoring of systems needs to be limited.

On *security and confidentiality*, compliance, and accreditation of vendor solutions needs to include adherence to access control frameworks. Information sharing is always complex. Sharing protocols often reflects local service circumstances which will include electronic and other communication media requirements.

On *safety*, data quality is a key aspect of a health system and should be validated both at source and at point of update. Early clinical engagement to standardise clinical content to support semantic interoperability, messaging content and information exchange needs is essential. Technology is merely the enabler of change. Change management and clinical transformation is crucial in providing continuous services.

A REGIONAL SOLUTION: HUNGARY

BT developed a regional solution in Hungary under the umbrella of the European Union's IT Development in Healthcare in the Disadvantaged Regions (HEFOP 4.4.1 initiative). Called IKIR (Inter-Institutional Information System), this solution connects 38 healthcare institutions in Southern Transdanubia, Northern Hungary and Northern Plain, 15,000 medical practitioners. A population of 1.5 million benefits from the system.

The electronic health record (EHR) service is a central index service with federated clinical information in repositories requiring a different architecture to the UK. This model is similar to that used by other countries with state or regional autonomy of health services. The information is fully accessible between domains, but is not collated as a care summary. While this may be perceived as still leaving the clinician with the burden of having to collate information from several sources, it is a significant step forward in delivering safer and more effective care with no delay caused by a debate about who has the responsibility of providing a care summary. For countries where the GP is not the locus of ongoing patient responsibility, this model provides a fast and effective solution. Patients are also able to access the solution via a portal and can check data held, thus improving its accuracy.

RELIABLE

Just as in the UK, the core of the system is a message-transmitting engine which supports the secure transmission between healthcare institutions, with searching and downloading of 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 business flow is as follows. 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.

Two main lessons were learned from this experience. First, whilst the TMS needs contextualising to meet country-specific rules, the principles of adherence to standards and rigorous verification of conformance and compliance remain a fundamental requirement in every solution. Second, technical integration brings into focus the need for standardised understanding and representation of clinical information held. Standardisation of clinical content must be undertaken if semantic integration is to be achieved.

SECURE AND CONFIDENTIAL

The most significant difference between the solution sets in the UK and Hungary is that in Hungary, while most clinicians use their own hospital information systems for patient information, the solution does allow them to search and access healthcare documents held by others using a secured web connection via a portal. It also allows patients to consent or not to sharing and for all to apply the data protection law which demands that no patient data be stored centrally, including their unique patient identifier. Healthcare data can only be stored by specific organisations such as hospitals, clinics, GP surgeries and the National Health Insurance Fund.

Under the constitution, Hungarians have three unique IDs. Healthcare is one of these. It is this number that the healthcare providers use as a unique ID, whereas the patient portal access uses the citizen ID as the unique identifier. The cross-validation between the two government bodies is part of the IKIR service. As in many countries, data protection law had not been tested in earnest and there are multiple opinions on its interpretation. The current business

solution has been to create and utilise another identifier number derived from the unique healthcare ID. This is held in the IKIR service which is not categorised in existing law.

Two main lessons were also learned from this experience. 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.

SAFE

Significant improvements in care have been made possible by allowing documents and other information to be requested and retrieved from other systems using a central index. The lesson from this experience was that mandating and adoption of international and national standards is imperative for safe transference and retrieval of data, including the context and semantic intent.

CONCLUSION

Interoperability between diverse constituents in a health ecosystem, enabled by a set of standard interfaces, is achievable. BT's has succeeded by developing and understanding the interrelationships of these standards, and learning that all solutions must be based within the local context, reinforced and supported by local governance and decision making structures.

REFERENCES

Burke, Brian. 2008. Case Study: Architecting an Emergent Business Ecosystem at the U.K. National Health Service. Gartner, Stamford, Connecticut (19 May).

NEHTA. 2008. 'Stakeholders give a clear message of support for approach to privacy', Media Release, 7 November 2008. Accessed 3 August 2011. Available from: http://www.nehta.gov.au/media-centre/nehta-news/447-stakeholders-give-a-clear-message-of-support-for-approach-to-privacy.

Sprivulis P et al. 2007. 'The economic benefits of health information exchange interoperability for Australia'. *Australian Health Review* 31 (4) (November): 531-539.

Cite this article as: Bennett, Janette. 2011. 'Person-centric integrated eHealth records: Reliable, secure, confidential and safe'. *Telecommunications Journal of Australia* 61 (3): 47.1-47.7. Available from: http://tja.org.au.