Background – Data use in healthcare

The traditional view of healthcare, with a single set of patient notes, written by the clinician, and physically present at every consultation, seems a long way behind us. Although this model worked well for the ‘single patient, single physician’ model of patient care, there are very few situations where this model holds true in the 21st century. With increasingly complex treatments, sub-specialisation of clinicians and use of a range of diagnostic services, information on each patient is gathered from a huge variety of sources. The use of technology to streamline the process to ensure information is accurately recorded in a timely manner seems highly desirable and increasingly healthcare providers of all sizes are turning to electronic systems.

One result of this is that truly unimaginable volumes of patient data are being stored. Data from the U.S. healthcare system alone in 2011 reached 150 exabytes. To try and put this into a little bit of context, 5 exabyte would be enough data to contain all the words ever spoken by human beings on earth. Of course, medical data is so huge because it contains not only words, but also images, and occasionally videos. [1]

Capturing and storing so much data is a complex undertaking. Storing it an accessible way and keeping it safe presents huge challenges. However, when this is achieved, the benefits to efficiency for the medical team, and improved care for the patient can be huge. The current trend has healthcare providers moving towards storing information in a variety of “Cloud” solutions; these are public, private, or hybrid off-site data centres, sometimes shared between multiple tenants, that allow authorized users access to relevant data from virtually any device with an internet connection.
Potential benefits of electronic healthcare systems

The potential benefits of electronic data capture and storage are immense. An ideal system would involve the ability for different clinicians to enter information from different sites, at different times; and all for that information to be immediately available to anyone caring for the patient – wherever they are (and wherever the patient is). This means that delays are prevented, all new information from test results to expert opinions is immediately available. Changes in a patient’s condition can be treated in the best possible way and efficiency is maximised for both clinician and patient.

From the perspective of healthcare workers, the best electronic systems should help improve the quality of their work in an increasingly pressured environment. Synoptic-style reporting systems facilitate complete reporting, whilst electronic data storage permits easy access for analysis for audit or research purposes, facilitating benchmarking and outcomes monitoring.

Pitfalls of the new technology

Of course, electronic patient data also carries potential pitfalls. Capital outlay and the need for ongoing technical support may deter some – although the costs are often rapidly offset by savings and improved efficiency.

The biggest challenge probably lies in data security, we have all heard of high profile cases where insufficiently protected medical data has been inappropriately accessed, leading to embarrassing and expensive lawsuits. A recent study estimates that data breaches cost the healthcare industry about $5.6 billion annually. As well as the financial cost, the loss or sharing of personal medical information can have significant implications for patients. In 2015 the US Office for Civil Rights (OCR) identified 253 breaches which affected 500

From the perspective of healthcare workers, the best electronic systems should help improve the quality of their work in an increasingly pressured environment.
individuals or more – affecting in total around 112 million records. To put it another way they estimate that around 1 in 3 healthcare users will experience a data breach [2,3].

Data security is obviously hugely important, and legislation exists which is designed to try and help medical data is kept safe. In the US, the most relevant legislation comes under the Health Insurance Portability and Accountability Act (HIPAA) from 1996. Similar legislation exists in the European Union, with new regulations coming into place in 2018.

Another potential area of concern is ensuring the reliability of data access. System upgrades, viruses and even natural disasters can all prevent electronic data access, and potentially lead to delays in patient-care.

With the right system in place, all these problems can be avoided – understanding the basics of the technology, and the questions to ask of a data management company is crucial to ensure your organisation, and your patient’s data, is protected.

**Key things you need to know and important questions you need to ask**

**LANs**

Small volumes of data can be physically stored on individual computers or ‘local area networks’ (LANs). LANs may be suitable for small medical facilities where a very limited number of people need to access patient data – usually only on a single site. A local area network stores data on a central ‘server’ which is located on-site, and allows authorised users to access centrally held data. This prevents individual computers becoming overloaded with data, and improves performance while allowing access to data. However, LANs require investment in hardware and often need on-site IT support.
Cloud computing

Cloud computing has become commonplace in recent years, thanks largely in part to the many advantages it offers over other traditional means of computing. At its core, cloud computing is about using large, third-party data centers or server farms to store data for easy access from other locations via the internet. Unlike LANs, which require hardware investments and IT support, Cloud service providers essentially lease portions of their data centers to clients for a monthly subscription fee. This allows the organization to focus on delivering their core services without having to purchase or maintain expensive hardware and extensive IT support teams.

There are several different types of clouds, and different models will be appropriate for different institutions with varying amounts of data to store or complexity of operation. The right solution may also depend on the amount of in-house expertise that an organisation has.

Data Security and HIPAA compliance

No data storage system is inherently more or less secure than another. Data security relies on how well designed the system is, and may be enhanced by best-practice techniques such as regular passwords updates.

In addition to conforming to the regulations laid down by HIPAA, PIPEDA or the EU data management rules, there are several best-practice techniques which enhance data security.

- Geographical redundancy

This describes a system where data is stored in several different physical locations. In this way data can be protected against power outages, fire and natural disasters. There are many examples of when natural disasters have
prevented access to patient data, and examples of how geographical redundancy can prevent this.

One example comes from the US in 2012, when Hurricane Sandy hit the eastern cost of America. Long Beach Medical Center (New York) were able to access the electronic health records of their patients despite the hospital itself being flooded by 10 feet of water. In fact, during this emergency, there was only one report from New York of patient data being lost where electronic patient records were being used; in contrast many paper records were lost [4].

This natural disaster clearly illustrates how electronic data storage with geographical redundancy can ensure patient records are much more secure and robust than a traditional set of paper notes.

- **Encryption**

  Encryption is the process which makes data unreadable to all except authorised users. The best systems will encrypt data during use, storage and while it is being sent. Although data encryption is not mandated by most legislation, failure to encrypt data was at the heart of the 2014 Anthem HIPAA data breach which affected up to 80 million Americans.

- **Data destruction**

  Effective data destruction involves more than simply dragging a document into the computer’s recycle bin. Understanding the difference between clearing, purging, and destroying (or at least ensuring your cloud provider does) is essential to ensure regulations are met.

- **Additional considerations**

  In addition to cloud security best practices such as encryption and geographic redundancy, legislation like HIPAA requires healthcare providers and their business associates to develop contingency plans for emergency situations. Before choosing a cloud service provider, it’s important to ask what
procedures they have in place to ensure that both your healthcare applications and your patients’ protected health information are still accessible in the event of an emergency.

We often assume that data is safer when locally stored – it feels more under our control, and for many of us we feel more comfortable with our understanding of where the data is and who can access it. However, no data system is inherently more secure than any other. Each relies on the design of the system, and the security processes in place to keep information safe. Locally administered systems can often fall short in some of these areas. Locally employed IT staff may not be security experts, software security updates may not be regularly installed, access to the server may be inadequately regulated. Any of these can lead to system weaknesses which employing a reputable cloud storage system will usually avoid. When human imperfections are added to this, locally administered systems can fail – sometimes with significant consequences.

Data regulators will sanction and fine organisations for such data breaches, so care needs to be taken at every level. Updating ‘tired’ hardware is a regular necessity for a local network, and usually seen as a good thing. Unfortunately, this wasn’t the way it turned out for Brighton Hospital in 2010. They received a large fine from the Information Commissioner’s Office when data of thousands of patients was discovered on hard drives being sold on eBay. The hard drives were due to have been destroyed, however an

Before choosing a cloud service provider, it’s important to ask what procedures they have in place to ensure that both your healthcare applications and your patients’ protected health information are still accessible in the event of an emergency.
unscrupulous individual was able to remove 252 drives, some of which were eventually purchased by a data recovery expert. The lost data included patient names, diagnoses, and other personal information. Undoubtedly a huge failing, this clearly illustrates the potential problems encountered when using local data storage. Other problems can result from simple human error. A prominent sexual health clinic in the UK discovered this to their cost. In 2015, a letter was emailed to 781 patients, many of whom were HIV positive. Sadly, the letter was incorrectly sent as a group email, rather than other recipients being blind-copied in. This, of course, meant that recipients could see the email address, and, in 730 cases, the full name of the intended recipients. This significant and embarrassing data breach was a simple mistake, but led to a hefty fine for the hospital. Cloud-based data security systems should have the capability to detect, warn and prevent users from making such simple errors.

Types of cloud

Public

Although these are the clouds that most of us will use most of the time, they are rarely suitable for healthcare data. A public cloud doesn’t mean that just anyone has access to your data, but it does mean that all data is stored in the same server. This works well for services like Dropbox, but their relative vulnerability to attack and lack of configurability makes them unsuitable for most healthcare needs.

Purely Private

Purely private clouds are dedicated to just one organisation (or even one department). While this can offer outstanding flexibility and may be the best option for organizations with extremely high data storage, they often require dedicated IT staff, and the transition may be hard to justify for many healthcare users.
Hybrid
A cloud is considered a public-private hybrid when your data is hosted on the same servers as the data of other organizations. Users of the server are called ‘tenants’, so the cloud is called a ‘multi-tenancy’ cloud. In reality, most clouds are multi-tenant. Differences in the construction or architecture of the cloud can have significant effects on their performance, and data security.

Multi-tenant cloud with a Shared Database
Although it may be possible for this type of cloud to comply with regulations, a major drawback of sharing databases with other clients is that the overall data load can slow down the cloud’s performance. In addition, updating or restoring data for one tenant often leads to service interruptions for other clients as well, in the worst-case scenario, if someone gains unauthorised access to another tenant’s data, they might also have access to yours.

Multi-tenant Cloud with a Unique Database
The advantages of a unique database within a multi-tenant cloud is that it isolates your data from the effects of other tenants’ data loads, security breaches or service interruptions. It is also easier to audit the activities of your authorized users.
Types of cloud service; which is right for my data?

Clouds are normally divided into three categories, depending on what they provide ‘as a service’ (aaS): software (SaaS), platform (PaaS) or infrastructure (IaaS). Many factors will influence your choice of service such as the level of in-house expertise or the extent to which you plan to contract IT professionals to set up customized operating procedures.

*Software as a Service – SaaS*

Software as a Service use the cloud to provide and update software – meaning software no longer needs to be installed or updated locally. Software such as Office 365 and Google Apps are examples of SaaS, but there are also many cloud applications designed specifically for business and healthcare. SaaS cloud services can be used by teams with no IT staff for regular tasks such as appointment scheduling, payroll, or operative reporting.

*Platform as a Service - PaaS*

PaaS allows a user to essentially rent hardware and network capacity. It can be especially useful when running several customized applications, but usually requires a higher level of IT skill for set-up and maintenance.

*Infrastructure as a Service - IaaS*

IaaS offers the greatest customization and scalability, but also requires the highest level of IT skill. Whilst IaaS may be necessary, and the best option for a large hospital, it may also be an unreasonable burden for a small clinic.
What is encryption and does my data require it?

Encryption refers to the process of scrambling data so that it is unreadable to unauthorized viewers. When a user has the proper authorization (also called an encryption key) they can view and use the data. Best practice security involves encrypting even the encryption key – using a different encryption method from that used to scramble the data itself.

In the US, the HIPAA regulations do not strictly require data to be protected by encryption. If you decide not to encrypt your data, they do require you to document your justification for this, and continually re-assess this choice as your data needs evolve. Furthermore, as encryption is recognised as IT best-practice, HIPAA considers encrypted health information to be in 'safe harbor' in cases that might otherwise be considered breaches. Many data breaches involve the theft of devices storing unencrypted data – when devices are properly encrypted the theft is not an HIPAA breach as the data remains unreadable.

Key questions to ask your cloud provider?

- Is my database separate from those of other tenants?
- If I need to use my backup data, how quickly can it be brought online?
- How geographically dispersed are your data centers?
- If one of your data centers goes offline, will it affect the performance of my cloud?
- Why do you use the kinds of encryption that you do?
- How do you protect encryption keys?
- What tech support services do you offer?
What if something goes wrong? Will my patients be affected?

- Do you offer support during urgent situations?
- When was the last time you tested your emergency preparedness?
- What crisis situations have you handled in the past?
- Did cloud tenants experience any service outages, and if so, for how long?
- How have your emergency preparedness procedures improved over time?

Potential for the future

Technology advances extremely rapidly. Investing in an electronic patient data management system is a huge undertaking. It makes sense therefore, that some thought should be given to whether the system is ‘fit for the future’, or able to adapt and expand to new advances, and the ever-burgeoning volume of data we need to store.

One area which is currently attracting interest and research is the regular acquisition of physiological data using devices worn by the patient such as ‘fit-bits’ or ‘apple watches’. The potential to monitor patient parameters on a daily (or perhaps even hourly) basis is fascinating. In some areas, the acquisition of
this type of regular (or even continuous) data is reaping benefits for patients. For example, in neonatal intensive care, gathering and analysing data on huge numbers of newborns has allowed the recognition of patterns which reduce antibiotic use and enable the earlier detection of potentially fatal infections in these vulnerable patients [5,6,7].

Who knows what innovations in care could be made if similar information were interrogated on people going about their daily lives? Some early progress is being made in this field, with personal monitoring devices able to transmit information such as daily blood pressure or weight to help predict the onset of heart failure [8]. Whilst this is technically possible, the vast volumes of data such approaches generate need to be collected, stored, and of course analysed before the techniques can become a reality. Along with cost, this represents a huge challenge for data storage and security in the years to come.

Ensuring data management systems have sufficient ‘scalability’ to cope with innovation is key to ensuring patients can benefit.
References:


http://c4fd63cb482ce6861463-bc6183f1c18e748a49b87a25911a0555.r93.cf2.rackcdn.com/iHT2_BigData_2013.pdf


https://doi.org/10.5210/ojphi.v5i3.4826


