HealthManagement
Promoting Management and Leadership

Volume 3 / Issue 5 / 2008 - Features

EHR :Privacy vs.Interoperability

Openness/Interoperability Versus Privacy/Security

Author

Tosh Sheshabalaya,

Both philosophically and technologically, the margins of the debate about electronic health records (EHRs) have been set by the long-running trade-off between openness and interoperability on the one hand, and privacy and security/confidentiality on the other.

From Telephones to Satellites and DNA Screening a Longstanding Debate

Such a debate stretches back several decades, marked in the first instance by the invention of the telephone and radio. In 1928, US Supreme Court Justice Louis Brandeis noted that technology had made it possible for governments, "by means far more effective than stretching upon the rack to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."

The 1950s saw the issue of technology assaulting privacy attain a fever pitch. The infamous campaigns by Senator McCarthy against trade-unions and everyone showing the slightest Communist 'sympathies' – real or imagined – were followed in the 1960s by the personal crusades of Federal Bureau of Investigation Director J. Edgar Hoover to wiretap a wide range of people, from civil rights campaigner Martin Luther King to Mafia bosses.

The decades since then have seen a variety of other technological developments intensifying this longstanding debate. Spy satellites were less eagerly embraced by the public than the evident utility of mobile phones, the Internet and GPS navigation systems. Only recently have some critics pointed out that the latter can provide authorities far more private data than any spy satellite possibly could.

The greatest recent concern about privacy is DNA screening and monitoring, biometrics and sophisticated face recognition systems.

The Katz Decision – Reality Check or Submission?

Meanwhile, the legal establishment has sought to stop a Sisyphean battle against the march of technology. In 1967, about 40 years after the libertarian observation by Justice Brandeis, the US Supreme Court ruled in its so-called 'Katz decision' that privacy was only protected when it could be reasonably expected.

The Debate on EHRs in the US

The current debate about EHRs (as well as their cousins electronic medical records/EMRs and electronic patient records / EPRs) have to be set against this backdrop.

So far, the signals are mixed and volatile, both in Europe and the far-more litigious environment of the US.

In November 2007, a survey by Harris Interactive and the Wall Street Journal concluded that a three-fourths majority of Americans believed that the benefits of EMRs outweigh privacy risks. 63% felt such technologies could cut medical errors, while 55% believed they would cut healthcare costs (against 15% who disagreed, with the rest unsure).

The issue of building up a critical mass of users – to provide buy-in – was also clearly demonstrated by the survey. Half of patients whose physicians had their records in electronic form said they trusted their provider to see their entire clinical history and status. The figure for those whose providers did not use electronic records was only 27%.

Up and Down

More recently, the outlook seemed to have reversed in some key respects. In October 2008, a survey by the Employee Benefit Research Institute found that although most Americans found the idea of having electronic medical records likeable, they were concerned that their privacy would not be protected. Indeed, only a little more than half (55%) of respondents to the survey said it was ‘extremely’ or ‘very important’ for health care providers to use electronic records. 43% of respondents said they would be ‘extremely’ or ‘very likely’ to access their health records online, while half this number (21%) reported that they were not likely to do so.

However, the survey reported that 62% lacked confidence about their EMRs remaining private, over 5 times higher than the 12% of respondents who were confident or extremely confident about it.

From Legal Definitions to Technology Standards

Also in October, US media reports again raised the issue of legal risks with EMRs. The key concern is about the Federal Rules of Civil Procedure, which the Supreme Court approved at the end of 2006. This makes any electronically-stored data discoverable in a trial. One example cited was a nurse recording erroneous information under a doctor’s login and password, which would make the doctor liable for any misinformation. In addition, physicians were warned about problems if the EMR time stamp (access or data entry) conflicted with their version of events. The final word of caution ran close to the tighter rules-based world of technology standards.

Some experts have warned that the legal status of an EMR is still not clear, nor is it certain if all EMRs meet the legal definition of medical records. Such concerns could come to the fore in legal disputes over patient care.

European Perspectives

Perspectives in Europe are also mixed. In France, media critics have launched concerted attacks on its perceived technical limitations. Underlining its perceived risks to privacy, the newspaper ‘Liberation’ has darkly alleged that the EHR carried the risk of making ‘Big Doctor’ into an Orwellian ‘Big Brother’. Similar concerns have been voiced from Scandinavia and Germany to Italy and Spain.

In Britain, some observers state that EHR is a war, pitting a powerful Anglo-American alliance against the rest of Europe and the world. In early 2007, the influential Royal College of Nursing attacked a core plank of the EHR project – to make national healthcare databases accessible across all European Union Member States – saying this could compromise patient care and safety.

The EU Response

Such concerns have been voiced since the early 2000s. However, many of them reflected national cultures as well as vested interests, and priorities.

In 2007, the European Union’s Working Party of European Data Protection Commissioners finally published a paper on the privacy of medical data within an EHR system.

Endorsing the primacy of patient privacy rights, the conclusions of the document are straightforward: unless there is a substantial public interest to the contrary, a patient’s wish on the processing of his or her medical data held in an EHR system should prevail.

Differences in the EU Approach Versus the UK/US

Centralization

One of the Working Party’s key observations was the need to avoid too much centralization. It pointed explicitly to the English NHS model, which “assumes there will be a single controller for the whole system separate from the healthcare professionals/ institutions”.

This, it said, would erode the trust of patients and the public. In contrast, it went on, such a credibility gap would not arise in a decentralized EHR system, where responsibility for personal records rests with healthcare professionals and institutions.

Information and Informed Consent, Medical Research and Public Interest

Further evidence of such a difference between the UK (along with the US) and the EU is also apparent in the European Data Protection Commissioners report, which asserts that all EHR information – including administrative data – is personal data (simply by virtue of their inclusion “in a medical file”). In the UK, healthcare administrative data is treated separately from personal medical data.

The EU report calls for major efforts to strike a balance between the privacy of medical data and the public interest. It limits the legitimacy of the use of such data to healthcare professionals for healthcare delivery – but explicitly makes two exclusions, limiting access to an EHR only by professionals “presently” providing a patient with medical care, and excluding medical research as part of the latter.

While underscoring that patients should retain residual rights to prevent access to their data, the European Data Protection Commissioners also voice major concern about patient consent - as a means to legitimize the use of protected personal medical data by actors outside the healthcare delivery area (so-called ‘secondary use’).

The report highlights the need for “genuine” free choice and the provision of full information to patients; otherwise, it warns, both the substance of medical data confidentiality and patient rights to withdraw consent are misleading.

Again, this contrasts with UK policy, which holds that substantial public interest for secondary use over-rides the need to consider issues of self-determination.

The Challenge for Technology Companies

In the final analysis, it is up to the healthcare IT industry to satisfactorily reconcile the conflict between openness and

interoperability (crucial to any meaningful EHR) and concerns by the general public and policy makers on privacy and security. This will be crucial to ensure its adoption.

In the US, as reported in this edition of Healthcare IT Management (see ‘Doing the Right Thing for the Wrong Reasons’), President Bush has called for setting up a National Health Information Network (NHIN) by 2014. On its part, as reported in our previous issue, the EU has recommended implementation of a pan-European EHR system by 2015.

For now, however, this question remains open. In 2007, the New York Times cited the US Government Accountability Office finding a “jumble of studies and vague policy statements but no overall strategy to ensure that privacy protections would be built into (EHR) networks.” Such a picture still has many elements of truth, both in the US and Europe.

Published on : Sat, 3 May 2008