



Neil Stuart

Identity Fraud in Health Care: How big is the threat and are we doing enough?

Neil Stuart, Paul K. Wing and Nigel Brown

Neil Stuart is a Partner, Health Care Consulting Practice, IBM Global Business Services; Paul Wing is an Executive Consultant Security, Information Risk and Privacy Services and Nigel Brown is the Managing Consultant of the Security, Identity and Privacy Practice of IBM Global Technology Services.



Paul K. Wing

We hear much about identity theft and the potential impact on individuals' personal finances, but what about the loss of medical identity? In the last year, there was the story of hackers exposing customer information from TJX Cos. the parent firm of the Canadian retailer Winners and the concern that the credit card numbers and accounts of as many as two million Canadians might have been disclosed and misused. In November 2007, another story broke about the U.K. government losing disks that contained sensitive personal information on over

25 million Britons. In Canada in December 2007, there was the reported disclosure of personal information for an unknown number of on-line Canadian Passport applicants. In this case on-line users of the service could see the on-line applications of other applicants. Could we see similar stories start to emerge involving personal health information?

We are investing billions of dollars in getting the health information of Canadians into electronic health records (EHRs), building systems that will allow for the sharing of personal health information among health care providers and enabling patient self-service through health care portals and on-line access. Should we be paying more attention to the risks that will come with these changes? This article explores the nature of risks around medical information and the EHR and reviews how we are addressing these risks.

Health information risks and the threat of medical identity fraud

There are several kinds of risk that arise when managing health information, risks that potentially assume greater significance when the information is shared electronically among members of the health care team and increasingly with patients themselves. They include:

- **Privacy** - the inappropriate use or disclosure of personal health information
- **Authentication and authorization** - invalid identification of patients or health providers who seek to use health information systems and the related risks around controlling access to individuals' personal and health information within those systems
- **Integrity** - errors or inaccuracies that could give rise to patient safety issues, or to unfounded typecasting or embarrassment of patients
- **Fraud** - intentional misuse of health information by a provider or external party

'Identity fraud' describes instances where parties masquerade as:

- an eligible patient
- an authorized care provider
- a family member or an informal caregiver of a patient.

In health care, identity fraud could entail situations such as:

- Individuals masquerading as others to get access to 'covered care'
- Individuals masquerading as others to avoid stigmatizing diagnoses or interventions appearing in their records - potentially resulting in incorrect attribution to others of diagnoses or treatments
- Providers using invalid identities to submit fraudulent claims
- Unqualified individuals masquerading as providers to practice illegally or make illegal orders/prescriptions

Identity fraud can lead to inaccuracies in individuals' health records and this in turn can result in significant patient safety risks. An example of this could be if a person was using someone else's medical identity and the two individuals had different blood types or different drug allergies. It could also lead to other

personal impacts such as denial of employment, insurance etc. Furthermore, the collateral effects of stolen or lost personal health information being available on the online information "black market" that has emerged primarily for personal financial information could lead to other personal impacts such as embarrassment, reputational damage and even extortion.

In the business sector, identity fraud is viewed as one of many potential threats. Financial institutions have realized that it is difficult to anticipate every form that fraud and masquerading might take. This realization has been reinforced with the increasingly rapid rates of innovation in the use of information technology. The authors believe that this view is equally applicable in health care.

Addressing risks

The authors of this article also argue that we should not develop an architecture and policy framework just to deal with identity fraud alone. Rather, we should deal with the threat of medical identity fraud in the context of a broader privacy and security architecture. And such a response needs to be built around key principles that address the full spectrum of risks. The authors also caution against taking the discussion on this issue as it is unfolding in the U.S. and transplanting it directly to

Canada. With public coverage of health care in Canada, the issue of identity fraud for financial gain is less of a concern here than in the U.S. Though there are some that would argue we need to be on the lookout for people who are not Canadian residents using false Canadian identities to gain access to "free" health care in Canada.

Medical identity fraud is not a threat unique to electronic health records. EHRs actually hold the potential to better manage health care information, and thus better control identity fraud through:

- Improved opportunities for more robust and reliable authentication of users and their associated health record
- Better opportunities to track unusual or spikes in individual use, as is done with bankcard use
- Easier or automated consistency checks and controls
- Opportunities to mask or anonymize information that are not available with paper records
- Bringing together disparate "islands" of health records from service providers/organizations across the health system and treating them as an integrated electronic health record

EHRs also provide unique opportunities to identify providers who abuse their access to personal health

North America's Leading Provider of Electronic Medical Records

Trusted • Proven • Reliable



in Canada
1-800-563-0579
clinicare.com



in USA
1-800-438-1277
chartcare.com

Visit us at HIMSS 2008 Booth #7948

information by accessing information that is not directly related to their care-giving responsibilities.

Health information risks, and particularly the threat of identity fraud, can be significantly reduced by giving the individual health care user greater access and recourse:

- Giving individuals access to their health records
- Enabling them to seek timely correction of any inaccuracies in their health information

addictions, sexually transmitted diseases, terminated pregnancies, genetic information) are more likely to lead to personal and reputation-related harm than financial harm. Also, in health care there is potentially a wide range of users with access to health information - - provincial ministries, regional health organizations, hospitals, clinics, independent labs, physician offices, retail pharmacists, insurers, health call centres, and more. They can span public and private sectors and can be covered by different privacy legislation. And

“EHR initiatives are still a ‘work in progress’, and will continue to evolve and become more sophisticated and comprehensive in the years ahead, with increasing degrees of patient and caregiver access to the records. Thus the risks will also evolve and likely become more complex.”

- Giving them access to the trail of who has accessed their health records
- Providing electronic alerts to individual users to let them know of additions to their record, (e.g. that a lab test result has just been reported) similar to Credit Reporting Bureau alert reporting. In this way, individuals can become their own watchdogs as to whether activity related to their record is expected or suspicious.

Connecting the individual to their health information and informing them as to who has had access to it should help to reduce anxiety about the management of their health information. It makes the information transparent to the patient, allows for validation of the information and builds trust. These patient-level controls have been built into electronic health records in several European jurisdictions, for example in the EHR implemented in Andalusia, Spain. The concept of a visible audit trail also allows health care providers accessing a record to question any apparently inappropriate access by other providers.

Misuse of personal health information can also be reduced with systems of internal controls. Experience in the financial services sector shows you do not have to foresee all the specific threats to identify controls that will minimize threats like “phishing” or web site “spoofing”. Having a comprehensive security and privacy architecture helps to identify the controls that will protect against the intentions of such attacks even if the methods of the attacks is new.

Health care is different

While the authors have argued that there are important lessons to be learned from other business sectors, we also observe that health care presents a number of distinctive information risks.

The risks of inappropriate disclosure of sensitive personal health information (e.g. mental health conditions,

the scale is not the same in all health care settings. A regional health organization covering a million people approaches privacy and security differently from a physician’s office. And within health care organizations there can be a range of players accessing the information - - clinicians, unit clerks, care coordinators, health records staff, planners, researchers, etc. There are also unique complexities around managing and authenticating access to health information - - it needs to be context specific. There is the question of the capacity in which an information user is accessing and/or sharing information? And there are further complexities with access authorization by non-medical individuals other than the patient, e.g. relatives and other people acting as caregivers. There are unique information access issues with children both before they reach the age of majority and once they reach that age, and questions of parental consent.

These considerations which give a unique character to privacy and security risks in health care settings will become even more marked as our health care system evolves:

- Health care is increasingly networked and team-based, and is more frequently delivered beyond just one facility. This results in a significant increase in the sharing of personal health information, whether it is done electronically or not.
- New channels of health care delivery are being introduced - - e.g. telehealth, health call centres, patient portals, retail health care, web services, remote monitoring, etc.
- There is a shift in emphasis from short-term, episodic acute care to ongoing management of chronic conditions and chronic diseases, life-long care; this adds emphasis to maintaining and continuously sharing health information. Unlike other business sectors, personal information in health care will often

remain on individuals' records for their entire life – and even beyond!

EHR initiatives are still a 'work in progress', and will continue to evolve and become more sophisticated and comprehensive in the years ahead, with increasing degrees of patient and caregiver access to the records. Thus the risks will also evolve and likely become more complex.

All this means that dealing with privacy and security risks in health care is not a one-shot deal, but will require ongoing attention. It calls for ongoing assessment and understanding of current risks, threats and the architected responses to them.

Surveys show that privacy and security are increasingly critical issues in determining the acceptance and success of technology initiatives leveraging personal health information such as EHR's – from the perspective of health care providers and individuals. It is also a significant consideration in government policy making and investment decisions on e-health. The inescapable conclusion is that good privacy and security must be designed into such initiatives from the start and not added on as an afterthought.

The role of technology firms

There is a valuable role that technology firms can play in assisting health care organizations develop and

adopt effective solutions for assessing and managing risk, protecting privacy and minimizing security threats. These firms offer a range of solutions and services that help to protect sensitive data and help health care organizations manage health information more appropriately. Areas where technology firms can assist include:

- Consulting services to help: identify and implement best practices; analyze risks and develop risk management practices; design and implement structures, policies and governance for effective privacy and security; create awareness and adoption of appropriate behaviours/processes; conduct compliance assessments
- Architecting, designing, engineering, implementing and in some instances even operating systems to facilitate privacy and security, e.g. identity and authentication management, access control, encryption, etc. And designing work processes and checks and balances for better health information management

When we look at the different forms identity fraud can take, indeed when we look at broader health information risks, they can be rooted in either:

- The actual technology and weaknesses in its design, or
- The way the technology is used

The Next Generation of Healthcare Workload Management Software



Better Care.
Better Efficiency.
More Happiness.

With the latest generation of workload acuity software from GRASP Systems, intelligent staff management has never been simpler. The GRASP Methodology is the proven gold standard for nursing and allied health workload management, case costing and decision support. With GRASP staff can quickly and accurately review delivery requirements, record activity, and communicate across services. GRASP's on-demand resource allocation and trend analysis planning tools help you increase your facility's efficiency, improve care, and support staff satisfaction and happiness.

Contact us at www.graspinc.com or 905-508-1134

GRASP Systems International, Inc. • 9555 Yonge Street, Suite 310 • Richmond Hill, Ontario L4C 9M5



In the health care sector, the complexity of how services are delivered and the complex nature of health information itself make the latter category of risk a particular concern.

Health care organizations usually have an expert grasp of clinical risk. They have much less experience of how IT introduces additional risks. And this is where technology firms can bring in their experience and expertise, address the relationships between business processes and technology, share best practices, and draw on other industry sectors. Given health care's relatively recent entry into the "e-world", there are opportunities to leapfrog other sectors, for example taking advantage of biometrics and proximity devices for authentication.

The leading technology firms will also take a holistic view of the issue, not just advocating point technical solutions. They will assume a data-centric security perspective rather than an enterprise-centric perspective - - in other words they will address the security of the 'content' as well as the 'container'. This is particularly important in health care where all the data generally does not belong to a single enterprise. The initial response to managing information privacy and security risks is often to create a strong barrier around the information that prevents unauthorized penetration. However, given the federated nature of so much health information and the emphasis on sharing this information among health care providers it is also important to look at the fundamental questions as to what information is collected and the associated accountability for its accuracy, access and use. In a sense, personal health information must be "self-defending" and must carry with it the rules regarding who is allowed to use it and under what circumstances.

Conclusion

There is a paradox in that on the one hand we see huge benefits to introducing EHRs, even the potential to fundamentally transform how health care is delivered. On the other hand there is anxiety about our capacity to manage the associated information security and personal privacy risks. Our health care leadership, political decision makers and even the media push for more e-health, and say they cannot get it fast enough. They cite the benefits of greater patient safety, elimination of redundancy, improved service and access, improving care processes, integrating services, giving patients more control, the opportunity for more self-service and a better patient experience. According to the Ontario Health Quality Council, for example, 32,000 Ontario patients are made worse each year because of errors caused by the lack of electronic health records. Patient safety and privacy are among the goals of e-health, but they also rank among the risks of e-health.

'Interoperability,' or the ability to share more timely and accurate health information among providers,

is a goal of many e-health initiatives. Integrated health care delivery, team-based care and patient engagement are three of the highest priorities on the health care agenda. And they all call for more sharing of individuals' health information. And yet it is this very goal of interoperability that raises so many of the concerns about risks! As we explore measures to reduce these risks, we need also to recognize the consequences of constraining interoperability. If providers cannot share data electronically, work-arounds will proliferate, for example paper copies, screen prints, and CDs being made and shared, and the greater use of faxes. These work-arounds will generally carry much greater risk and be harder to monitor and control.

In conclusion, the challenge is to understand, embrace and manage risks, to minimize their impact, while also maximizing the benefits of information technology. This is a challenge faced with most significant innovation - - new forms of commerce, new forms of transportation, new energy sources, new therapies, new channels of service delivery and new forms of service access. EHRs are a dynamic, evolving field. New forms of health service delivery are continually being introduced. We must continue to analyze emerging risks and address them on an ongoing basis. This should be done in conjunction with existing enterprise risk management and governance processes. We have to continue to educate stakeholders of the evolving risks. And we must also ensure the flexibility to refine and develop new approaches to managing risk as our understanding of the new technologies and emerging threats evolves.

This is new ground and we will not be able to foresee the nature and significance of every risk - - above all we have to be able to learn and adapt. We do need common, accepted definitions of health information and information technology risks and clarification of standard risk management objectives and protection principles. We also have to make sure that people on the front line, who ultimately have to make the EHR work, have tools and practices they can use. We must not paralyze them with a morass of controls. We must not preclude the opportunities to take advantage of new information technologies.

So, let us return to the question posed in the title of this paper "Identity fraud in health care: how big is the threat and are we doing enough?" The authors conclude that identity fraud, or more broadly, security and privacy issues, are a real threat to the success of the EHR and related initiatives. We are probably not collectively doing as much as we should to address this threat but the path forward is clear and involves holistic data-centric and risk-based approaches to privacy and security. ●