



# Electronic health records, information misuse, and ID abuse: Uneasy perspectives

Dr Gordon Atherley

*Dr Gordon Atherley is the Principal of Greyhead Associates*

Deloitte's November 2006 performance review of Ontario's Smart Systems for Health Agency<sup>1</sup> confirmed the Toronto Star's front-page criticisms of a year earlier<sup>2</sup>. Both critiques focused on the Agency's failures—client dissatisfaction, undemonstrated value proposition, and inadequacy of financial management.

Deloitte reproached the Agency's board and senior management, and Ontario's health ministry. But it didn't take or wasn't given the opportunity to examine the contribution of systemic problems of information and its technology—a surprising omission, given the rapidly increasing experience of modern information technology's shortcomings in preventing information from flowing into the wrong hands through ID abuse and in protecting against the harmful consequences of misuse of information.

Harmful consequences widely known to the public include mortgage and title fraud, and drivers' licence and health card counterfeiting, which supports bank account fraud through ID abuse.

From 1985 to 2005, fraudulent use of VISA and Master Card increased 994 percent; from 2004 to 2005 alone, 30 percent. In 2005, the number of such frauds comprised 21 percent of merchant outlets<sup>3</sup>.

The public sees media reports of physician, pharmacist and nurse fraud, health ministry employee malfeasance with health cards, and defrauding or deceit of the healthcare system by ineligible persons. All of these abuses of ID and misuses of information possess the potential to corrupt individual patients' health data held in electronic health records.

Ontario's Provincial Auditor General warns that, as healthcare increasingly shares electronic records, the risk "increases that a patient could be misdiagnosed or mistreated if his or her health records have been compromised by those of another individual using the same health-card number"<sup>4</sup>.

The Globe and Mail's January 29, 2007 editorial page's cartoon caught the public's sense of danger in information misuse mediated by technology. It pictured Little Red Riding Hood using her mobile phone to order cookies for Grandma. She's on the point of giving her credit-card number. All around her, behind the trees, lurk wolves with open laptops and cocked ears. On February 3, the Globe, among other newspapers, carried a full-page advertisement by the TJX group of companies acknowledging the "recently announced unauthorized intrusions into our computer systems" and associated compromise of credit-card information.

The harmful consequences for healthcare organizations of information misuse asserted themselves in the controversy over the morning-after pill, Plan B. In March, 2005, an

editorial in the Canadian Medical Association Journal commented critically on the then emerging practice of Ontario pharmacists in asking women for their names, address, and sexual history before selling them Plan B, an over-the-counter, non-prescription pill<sup>5</sup>.

In November 2005, The Journal's writers asked the Canadian Pharmacists Association for comment on their research into pharmacists' Plan B activities. The Canadian Pharmacists Association complained to the CMA, which agreed with the pharmacists. The CMA asked the Journal's publisher for changes, which the editors reluctantly agreed to. In December, the Editor wrote an editorial critical of the CMA's interference.

In February 2006, the CMA board dismissed the Editor and Senior Deputy Editor (full disclosure: I was a reviewer for the Journal at the time). The dismissals provoked an outcry about editorial freedom from the international medical-scientific community. Despite extensive policy-enhancing activities, it's still unclear if the CMA's reputation is fully recovered.

Ontario's Information and Privacy Commissioner decisively intervened on the pharmacists' need to know: "Controversial morning-after pill screening form scrapped in Ontario: Women's health information protected", said the IPC's December 7, 2005 news release. With Plan B, a professions' need to know was judged misuse of information pertaining to women's health.

As a whole, the events of Plan B appear consistent with Malcolm Gladwell's tipping-point theory<sup>6</sup>, which holds that small numbers of people and events provoke major changes, as governments are well aware.

Relative to electronic health records, a tipping point was certainly reached in the UK late in 2006 over the right of patients to opt out of the government's project for 50 million electronic health records with access by 250,000 healthcare staff<sup>7</sup>. After months of adverse media, November 2006 saw a report of a poll which found that 53 percent of patients opposed on privacy grounds having their data in the government system and that 52 percent of family doctors would refuse to upload data without the patient's specific consent<sup>8</sup>. Late December, in an abrupt U-turn, the government granted patients a right to opt out, albeit limited. Immediately afterwards, the junior health minister responsible for the electronic health record project, Lord Warner, resigned.

Early in January 2007, German doctors threatened to boycott Germany's largest healthcare information technology project. An expert report on the costs of the project provoked fears among doctors that they would have to pay far more for new computer software and hardware than the estimated

1500 Euro for each practice. The health ministry had said that it would cost about 1.6bn overall. But a report from the technology consulting firm Booz Allen Hamilton, published by German hackers Chaos Computer Club, estimated costs of at least several billion euros<sup>9</sup>.

On January 29, 2007, Meyer<sup>10</sup> reported that the European Commission was about to call for proposals on how patients' medical details would be shared between its member states, with the UK almost certain to be included in the scheme. One requirement would be interoperability between member states' healthcare IT systems.

Commenting on the uncertainties about the level of security that would be required, and the existing disquiet in the UK about the security implications of a centralized national health database, Meyer noted that the idea of patients' health details becoming available in other countries "under those countries' home-grown security restrictions...seems sure to cause further concerns".

In November 2006, The New York Times had identified "acute public concern about security breaches and identity theft" as the toughest challenge the US federal government faces with the increasingly politicised issue of electronic health records<sup>11</sup>.

On Feb 1, 2007, the US Government Accountability Office (GAO) published its conclusions from its task of describing the effort of the Department of Health and Human Services (HHS) to ensure privacy as part of its national strategy and to identify challenges associated with protecting electronic personal health information<sup>12</sup>.

GAO recommended that HHS should define and implement an overall privacy approach to ensure that key privacy principles are fully addressed, along with "challenges associated with the nationwide exchange of health information". "HHS disagreed and stated that it has established a comprehensive privacy approach", wrote GAO, believing instead that "an overall approach for integrating HHS's initiatives has not been fully defined and implemented".

Because surprisingly little is published in Canada about the unfolding international story of the safety, privacy and security challenges of electronic health records, the author's website provides references indicative of the uneasy international perspectives<sup>13</sup>.

In Canada, strategic questions for electronic health records systems include:

1. whether the public is well enough informed to judge claims—implicit or explicit—that healthcare's IT is demonstrably safer than that used in the financial, commercial and government sectors, and whether Canada needs something comparable to the US GAO to provide critical overviews of government initiatives for interoperable electronic health record at their early stages;
2. whether 'need to know' provides a practicable and reliable basis for deciding who, among perhaps 160,000 healthcare personnel and others, can and cannot see all or part of a patient's personal interoperable electronic health record;
3. whether consent-based privacy laws are adequate against information misuse and ID abuse, and whether Canadians should have a right to opt out and not be restricted to the limited protection of lockboxes;

4. Whether the costs are too great for a healthcare system under mounting financial pressures given the significant but unpredictable costs of achieving and maintaining healthcare IT safety, security and privacy at a level that satisfies public, patient and provider trust, current and future.

Safety of IT generally is a strategic challenge for governments as part of their fundamental responsibilities to protect citizens against risks over which the individual has little or no control. Surely the time has arrived for governments to focus on protection against ID abuse and information misuse, which also are the systemic challenges of electronic health records, even if this means reconfiguring legislation, redefining the roles of their agencies and revisiting their own e-health ambitions? ●

## References

- <sup>1</sup>Smart Systems for Health Agency (2007) [www.ssha.on.ca/operationalreview](http://www.ssha.on.ca/operationalreview)
- <sup>2</sup>Hamilton, Tyler (2005) "Digital health slow to boot up; Ontario's push to get patient records online is plagued with bugs; Provincial move to electronic records running year behind; Few benefits to show for millions spent, critics complain" Toronto Star, 21 November 2005
- <sup>3</sup>Canadian Bankers Association, 2006 <http://www.cba.ca/en/content/stats/DB038%20-%20Visa%20%20MCI%20Stats%20-%20Updated%20for%202005.pdf>
- <sup>4</sup>Office of the Auditor General of Ontario (2006) Annual Report 2006 at p185
- <sup>5</sup>Editorial: "Emergency contraception moves behind the counter" CMAJ, MAR. 29, 2005; 172 (7)
- <sup>6</sup>Gladwell, Malcolm (2002) "The tipping point: how little things can make a big difference" New York: Black Bay Books
- <sup>7</sup>The Guardian (2006) "Warning over privacy of 50m patient files" <http://www.guardian.co.uk/frontpage/story/0,,1936404,00.html>
- <sup>8</sup>Dyer, Owen (2006) 'Patients can't stop their data being put onto NHS "spine," department says' BMJ 2006;333:1188 (9 December), doi:10.1136/bmj.39056.373935.DB
- <sup>9</sup>Tuffs, Annette (2007) "German doctors threaten to boycott patient record project" BMJ 2007;334:63 (13 January), doi:10.1136/bmj.39090.604248.DB
- <sup>10</sup>Meyer, David (2007) <http://www.zdnetasia.com/news/business/0,39044229,61985335,00.htm>
- <sup>11</sup>New York Times, 2006 "Health Hazard: Computers Spilling Your History" December 3, 2006 <http://www.nytimes.com/2006/12/03/business/yourmoney/03health.html?ex=1170478800&en=2e14b16c31091f18&ei=5070>
- <sup>12</sup>US Government Accountability Office (2007) "Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy" <http://www.gao.gov/highlights/d07238high.pdf>
- <sup>13</sup>eHealth, International Perspectives <http://www.taxonmer.com/PublishTxgd001/eHealth,%20International%20Perspectives/index.htm>

Gordon Atherley holds the British equivalent of the Canadian PhD and MD degrees, and the LLD, Honoris Causa, from Canada's Simon Fraser University. He was first President and CEO of the Canadian Centre for Occupational Health and Safety, a federal corporation that has grown to supply knowledge service to 40 countries.