

Are Interoperability and Privacy Compatible?

Anyone who has been the victim of identity theft is most likely very familiar with the Fair Credit Reporting Act (FCRA). First enacted in 1970 and amended at least 17 times since then, the FCRA codifies in federal law all the rights and privileges of consumers that impact their personal credit histories. In addition, it details the responsibilities of various parties when handling personal financial information. This includes everything from the amount of information that can be printed on an electronic credit card receipt (no more than five trailing digits) to the processes to be followed when credit information is requested by any organization or individual.

In addition, the FCRA, summarized in an 86-page document prepared by the Federal Trade Commission (FTC) and available on its Web site (www.ftc.gov), includes provisions for how credit information is shared among parties, as well as how inaccurate information stored by credit reporting agencies gets corrected. Although each credit agency follows its own internal processes when handling credit information, the FCRA outlines very specific rights belonging to the consumer that must be protected.

Identity Theft Common

Even with these protections written into federal statutes and additional protections afforded by state laws, identity theft and accuracy of credit information continues to be a major problem in the United States. In the latest report on identity theft published by the FTC in 2003, almost 13% of the adult population in the United States experienced some form of identity theft in the past 5 years, while 5% reported an identity theft in the past year (*FTC Identity Theft Survey Report, 2003*).

In 2005, the FTC received more than 255,000 complaints of identity theft, with credit card (32%) and phone/utilities

(20%) fraud forming the bulk of the complaint categories. Interestingly, about 2% of the complaints were focused on theft of identity information to commit medical fraud (*Fighting Back Against Identity Theft, 2005*). This type of fraud covers the use of stolen identity information to obtain medical care (Table 1).

With the progression to digital medical information, concern is mounting among consumers about the ability of trusted institutions to keep those records private. Reports in the past few years of privacy breaches of personal information (e.g., Department of Veteran Affairs, CheckPoint) only decrease the confidence of consumers. In the United Kingdom, civil libertarians are encouraging people to “opt out” of the National Health Service’s Spine, the single repository for each citizen’s most basic electronic medical information. Without high levels of participation, much of the \$24 billion being invested in healthcare IT and electronic medical records may be wasted.

HISPC Works on Privacy

To promote the development of electronic medical records for Americans, the federal government formed the American Health Information Community (AHIC). Recognizing that privacy would be a significant issue for consumers, AHIC helped organize the Health Information Security and Privacy

Collaboration (HISPC), a partnership consisting of multi-disciplinary team of experts and the National Governors’ Association. HISPC works to develop plans to address variations in business policies and state laws that impact privacy and security.

Also part of AHIC is the Certification Commission for Health Information Technology (CCHIT). CCHIT continues to evaluate and certify healthcare information technology products for the ambulatory and acute care environments. The Health Information Technology Standards Panel (HITSP) focuses on “harmonizing” health information technology standards to support interoperability among all software applications.

It is through these and other efforts that electronic medical records can become a reality in the United States. Unfortunately, the deployment of comprehensive electronic medical records may deliver the benefits of decreased medical errors and reductions in unnecessary testing as well as the risk of unintentional release and misuse of personal medical information.

Although a significant number of Americans fear that the unauthorized release of medical information may lead to discriminatory actions in the areas of employment or insurance, another area of concern exists: the distribution of inaccurate medical information.

Table 1. Fraudulent Use of Stolen Identity Information

Type of Fraud	Percentage
Credit Card	32%
Phone or Utilities	20%
Bank Fraud	17%
Employment-Related	11%
Government Documents or Benefits	8%
Loan	5%
Medical	2%

Source: Identity Theft Victim Complaint Data, Figures and Trends, Jan. 1 – Dec. 31, 2005, Federal Trade Commission, http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf

Interoperability Threatens Data Integrity

With the growth in interoperability, the problems of ensuring data integrity become exponentially larger. In single, stand-alone systems, data integrity and data reliability issues are rather straightforward. Standard quality assurance testing greatly reduces the potential for the production and storage of inaccurate information. In an environment of interoperability, the challenge to ensure data integrity and reliability becomes significantly larger.

With interoperability, reliability in the quality of the data is lowered to that of the least reliable system. In addition, interoperability introduces an environment where the systems are spread out geographically and encompass applications with varying levels of system integrity and network security. In such an environment, interoperability opens the way for inaccurate data to populate other systems and patient records that are far removed from the data source. This "remoteness" decreases the likelihood that errors will be discovered, and more importantly, corrected.

For example, an inaccurate positive test for HIV caused by a software "bug" in a laboratory system may populate not only the electronic medical record in the hospital in which the test was conducted, but potentially dozens of other records in a variety of patient care settings. Although it can be imagined that proper data correction procedures can be put in place within an institution to correct the mistake, it is much more difficult to imagine such standard data correction procedures being deployed across multiple geographic areas, institutions, and care settings.

Clearly, the planning to address privacy concerns must go beyond those outlined in HIPAA regulations. Even though sanctions exist for breach of privacy, they do not have the needed "teeth" to effect adequate protections.

Although there are flaws in the current protections outlined in the FCRA to protect consumers' credit information, it does provide both a call to action and framework on which such protec-

tions can be developed to protect electronic medical records. Without such protections, a comprehensive electronic medical record with nationwide access will never become a reality, and all the current work on a National Health Information Network and Regional Health Information Organizations will be for naught. **IPSQH**

Barry Chaiken has more than 20 years of experience in medical research, epidemiology, clinical information technology, and patient safety. As founder of his own company, he has worked on quality improvement studies and clinical investigations for the National Institutes of Health, Framingham Heart Study, and Boston University Medical School. Chaiken is board certified in general preventive medicine and public health and is a Fellow and Board Member of HIMSS. He is the associate chief medical officer of BearingPoint, Inc., adjunct assistant professor in the Department of Public Health and Family Medicine at Tufts University School of Medicine, and serves

on the Editorial Advisory Board for Patient Safety and Quality Healthcare. He may be contacted at bchaiken@docsnetwork.com.

REFERENCES

- American National Standards Institute. Healthcare Information Technology Standards Panel. http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3
- Certification Commission for Healthcare Information Technology. <http://www.cchit.org>
- Federal Trade Commission Identity Theft Survey Report, September, 2003. http://www.consumer.gov/idtheft/pdf/synovate_report.pdf
- Fighting Back Against Identity Theft. http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf
- Leigh, D. & Evans, R. (2006, November 1). Warning over privacy of 50m patient files. *Guardian Unlimited*. <http://society.guardian.co.uk/health/news/0,,1936403,00.html>
- RTI International. <http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0>
- The Fair Credit Reporting Act. <http://www.ftc.gov/os/statutes/031224fcra.pdf>

Customized Reprints

Has your company been featured in **Patient Safety and Quality Healthcare (PSQH)**? Maximize your exposure to the market and reinforce your professional credibility with customized reprints.

HOW CAN YOUR COMPANY USE REPRINTS?

- Sales presentations
- Include them with your proposal package
- Create a direct-mail piece
- Distribute at trade shows and events
- Education and training

WHAT KIND OF CUSTOMIZATION IS AVAILABLE?

- Add your company logo
- Include your company profile and contact information
- Use an extra page to showcase a product or include an ad
- Highlight key points in the article

All reprints are printed on 70-lb gloss stock and are available in full-color or black and white. The reprint will state the article was featured in **PSQH** and indicate the issue.

- 100 minimum order
- Delivery time 3-4 weeks (rush delivery available)

FOR REPRINTS CONTACT

Kelly Millwood
770.431.0867, ext. 215
Toll Free - 888.303.5639
E-mail:
kelly@lionhrtpub.com