

# Usability Failures and Healthcare Data Hemorrhages

In healthcare, data leaks risk patients' health as well as their identity. The authors conducted interviews and field research to determine how system usability failures can lead to such data hemorrhages.

M. ERIC  
JOHNSON AND  
NICHOLAS D.  
WILLEY  
*Dartmouth  
College*

Usability failures—of both systems and embedded security—lead to user workarounds and security failures. In many areas of healthcare, workarounds are epidemic.<sup>1</sup> Struggling to cost-effectively meet patients' needs while balancing regulatory demands and ever-changing technology, nurses might improvise to circumvent failed processes.<sup>2</sup> Likewise, healthcare marketing and finance managers, shackled by poorly integrated systems, might be tempted to work around security by moving data into user-friendly spreadsheets. Such workarounds, whether clinical or back office, create new information risks and patient data hemorrhages.

To gain insight into healthcare usability problems, we studied data leaks in peer-to-peer (P2P) file-sharing networks. The leaks are symptomatic of the underlying problem and show how workarounds lead to security failures. P2P networks provide a window into the leakage problem and let us examine the data types that seep out of the healthcare supply chain.

### **Breach Consequences**

Breaches of private customer information have occurred in every industry, from retail to education. Data losses can generate alarm and outrage and also lead to fraud and identity theft. Although hackers regularly penetrate poorly secured networks, many recent security breaches weren't break-ins, but rather inadvertent data leaks. For example, lost corporate laptops have exposed sensitive information on millions of individuals. From poorly disposed computers to misdirected emails and lost flash drives, nearly every organization has mis-

takenly leaked sensitive customer information at some point.

The healthcare sector suffers such data hemorrhages with multiple consequences. Data losses can translate to privacy violations, embarrassment, and social stigma as well as lead to fraud and medical identity theft. Protected health information (PHI), including identifying information such as social security numbers (SSNs) and insurance policy information, can be used fraudulently for financial gain at the expense of public funds, firms, and individuals. Stolen medical identities can also result in life-threatening changes to medical records. Any consequential changes in patient information, such as allergies or blood type, can jeopardize patient health. Because of the US healthcare system's fragmented nature, data hemorrhages come from many different sources—ambulatory healthcare providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back offices, and outsourced service providers, such as billing, collection, and transcription firms.

In earlier work, we showed that inadvertent disclosures of medical information collected in 2008 made PHI readily available on P2P file-sharing networks.<sup>3</sup> We found leaks throughout the healthcare chain, including care providers, laboratories, and financial partners. In one case involving an AIDS clinic in Chicago, a patient data leak resulted in myriad consequences, including identity theft. Impacted individuals who experienced fraud and social stigma filed a

class action lawsuit against the clinic (*John Doe et al. vs. Open Door Clinic of Greater Elgin, an Illinois Corporation*, 2010). Recently, Khaled El Emam and colleagues estimated that of all the US IP addresses exposing files on P2P networks, 0.5 percent leaked PHI.<sup>4</sup> With tens of millions of simultaneous P2P users, the exposed PHI at any given point of time is substantial.

### Recent Healthcare Data Losses

Awareness of healthcare data losses is growing. Between 2005 and 2009, the Open Security Foundation documented 166 incidents of medical data breaches impacting nearly 6 million individuals (<http://datalossdb.org>). Many of the largest breaches have come to light in the past two years. For example, in November 2009, insurance provider Health Net lost a single hard drive containing the personal information and medical records of 1.5 million members. The information on the hard drive dated as far back as 2002. Health Net offered members two years of identity protection,<sup>5</sup> at an estimated cost of US\$360 million.

The majority of breaches reported to the Open Security Foundation are the result of lost or stolen laptops, computers, disks, media, hard drives, and tapes. Many of these incidents represent inadvertent disclosures rather than technical hacks. Laptops are often stolen for the laptop itself—not the data. Nevertheless, the data is inadvertently disclosed.

Whereas physical losses represent the largest component of reported data breaches, significant losses have occurred over the Internet. In many cases, Web-related breaches have been caused by employee errors that resulted in inadvertent disclosures. For example, in April 2008, two improperly configured servers holding Wellpoint data exposed the personal and medical information of nearly 130,000 individuals over the Internet.<sup>6</sup> On one server, 1,320 enrollees' data was so freely available that it had been indexed by search engines. In the case of the second server, a form of data protection was in place, but the protected files were available for download for more than a year.

Viruses such as Coreflood have also resulted in breaches. In other cases, employees themselves have inadvertently disclosed private information by sharing data directly over email. For example, in October 2009, an employee at Baptist Hospital East in Kentucky accidentally sent out a list of 350 employees' SSNs to a large mailing list.<sup>7</sup> Employee fraud is also a significant source of data loss. In April 2009, Johns Hopkins reported that a patient registration secretary was suspected of participating in an identity theft scheme that had affected as many as 47 people. During her employment at Johns Hopkins, she had accessed the personal information of more than 10,000 people. This information, including addresses, SSNs, parents' names,

dates of birth (DOBs), places of birth, and medical insurance information, was more than enough to perpetrate fraud. Such incidents—from lost laptops and misdirected email to technical hacks—now receive increased visibility thanks to new legislation.

### The HITECH Challenge

The US Health Insurance Portability and Accountability Act (HIPAA) includes privacy and security rules that became effective more than five years ago. Nevertheless, healthcare information security remains a significant concern as organizations migrate to electronic health records (EHRs). The Health Information Technology for Economic and Clinical Health (HITECH) legislation, which passed in February 2009, aims to accelerate this migration. It contains mandates for greater security, including the addition of new requirements on reporting breaches. The legislation was enacted as part of the 2009 American Recovery and Reinvestment Act to spur EHR adoption. With US\$20 billion for investment in health IT, HITECH is driving tremendous change in the industry, providing powerful incentives to encourage doctors and hospitals to rapidly migrate to EHRs.

Beginning in 2011, private physicians can receive as much as US\$15,000 annually for IT investments up to US\$65,000. These incentive payments will decrease over time as the program is phased out over a maximum of five years of eligibility.<sup>8</sup> Similarly, hospitals receive incentive payments for implementing and demonstrating meaningful use of EHRs, starting at US\$2 million for the initial year. This amount increases for hospitals discharging more than 1,150 patients per year (US\$200 per patient). Like the physicians' payments, these incentives will be phased out over a five-year period, pushing institutions to make investments sooner rather than later.

Recently, there has been significant discussion concerning the financial incentives to implement new systems and the meaning of the phrase “meaningful use.” In 2010, US Health and Human Services (HHS) finalized rules related to meaningful use of certified EHRs, which included a three-stage definition along with other requirements for qualifying for incentive payments.<sup>9,10</sup>

In addition to HITECH investment incentives, the legislation created the National Coordinator for Health Information Technology to facilitate the transition to EHRs and ensure patient privacy. HITECH also buttressed the HIPAA legislation, outlining plans for required privacy and security controls. To address security concerns, the initiative establishes protocols and certifications for health information technology products. The National Institute of Standards and Technology handles certification, which is necessary to qualify for the incentives.

Furthermore, the legislation established a new breach-reporting protocol for PHI leaks. HHS outlined a breach notification process with varying response levels depending on the breach's severity ([www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/hitechrfi.pdf](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/hitechrfi.pdf)). The response makes a distinction between unsecured and secured PHI. HHS defines *unsecured* as information that isn't secured with technology rendering PHI "unusable, unreadable, or indecipherable" to unauthorized individuals. In most cases, this means that data must be encrypted and health practitioners must destroy unencrypted copies of health information after use. Medical data used for research must be limited to the information relevant to the study and adequately obscure patient identity. HITECH also extended these requirements beyond parties covered under HIPAA to include business associates.

On 24 August 2009, HHS published final guidance on HITECH notification rules for PHI breaches occurring on or after 23 September 2009.<sup>11</sup> The rules specify that organizations must notify affected individuals within 60 days of breach discovery. If contact information is unavailable, then the organization must post an announcement of the breach on its website or through the appropriate media (for example, newspapers). Breaches involving more than 500 people also require state media and government notifications. Although these requirements went into effect in September 2009, HHS provided relief from full enforcement until 22 February 2010 to allow the industry time to adapt to the new rules. On 23 February 2010, HHS's Office of Civil Rights posted a list on its website of more than 60 organizations that reported PHI breaches occurring between September and February involving more than 500 individuals ([www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html)). One year after the effective date, the site had more than 100 breach announcements for the first nine months of enforcement (September 2009 to June 2010).

In addition to the notification process, HITECH increased HIPAA violation fines for both inadvertent and willful disclosure of unsecured PHI. The new penalties escalate with the violation's severity, ranging from US\$100 to US\$1.5 million.<sup>12</sup>

In the end, HITECH's success will be judged by the adoption of usable, secure systems that increase quality and reduce cost. However, many insiders agree that familiar paper-based processes supported by ad hoc systems such as Excel spreadsheets will be difficult to dislodge.

### Analyzing Healthcare Data Hemorrhages

To examine the usability issues that result in sensitive PHI leaks, we analyzed files we found as a result

of inadvertent disclosure, both before and after HITECH's new breach-reporting rules' effective date.<sup>13</sup> In our first study, we focused on *Fortune* magazine's list of the top 10 publicly traded healthcare firms.<sup>3</sup> To gather relevant files, we developed *digital footprints* for target healthcare institutions—key terms related to the firms, for example, important brands and affiliated hospital, clinic, and lab names. Using those terms in search engines such as Google or P2P networks will often result in material related to those institutions.

With the help of Tiversa—a company that monitors global P2P networks in real time—we searched networks, gathering a sample of shared files related to our digital footprints. Tiversa's technology let us search the four most popular networks, each supporting popular clients—Gnutella (for example, FrostWire, LimeWire, and BearShare), FastTrack (for example, Kazaa and Grokster), Aries (Aries Galaxy), and eDonkey (for example, eMule and eDonkey2000). We captured files containing any term or a combination of terms from our digital footprint, focusing on files from the Microsoft Office Suite (Word, PowerPoint, Excel, and Access) and Adobe (.pdf files).

Our goal was to gather a significant sample of files to provide insight into the types of data hemorrhages and to better understand the leaks' root causes. P2P networks change constantly as users join to find and share media, then depart. Therefore, the files that can be found at any point in time also change. In 2008, we randomly sampled P2P networks over a 14-day period in January, collecting 3,328 files for further manual analysis. Given our approach, we often captured files that weren't relevant to our search (in this case, having nothing to do with healthcare) as well as duplicates. Our sample yielded 389 unique, relevant files. The files found in this initial study and related follow-up showed many significant leaks involving thousands of patients' data.

After HITECH's passage in February 2009, we again collected samples of leaked files—this time using a large digital footprint of searchable healthcare terms we created based on the top 25 research institutions, as reported by the National Institutes of Health. For each institution, we developed a set of terms and phrases (average of 52) related to that institution and its medical specialties. These included hospital, lab, clinic, and research center names and specialties (more than 1,250 in total). We used these terms along with many generic healthcare terms ("medical," "hospital," "health," and so forth) to search for files in the major P2P networks. We conducted a search with these terms over a two-week period in July 2009, again focusing on text files from the Microsoft Office Suite and Adobe. Over a 14-day period, we collected 7,911 files, which yielded 2,966 unique, relevant files.

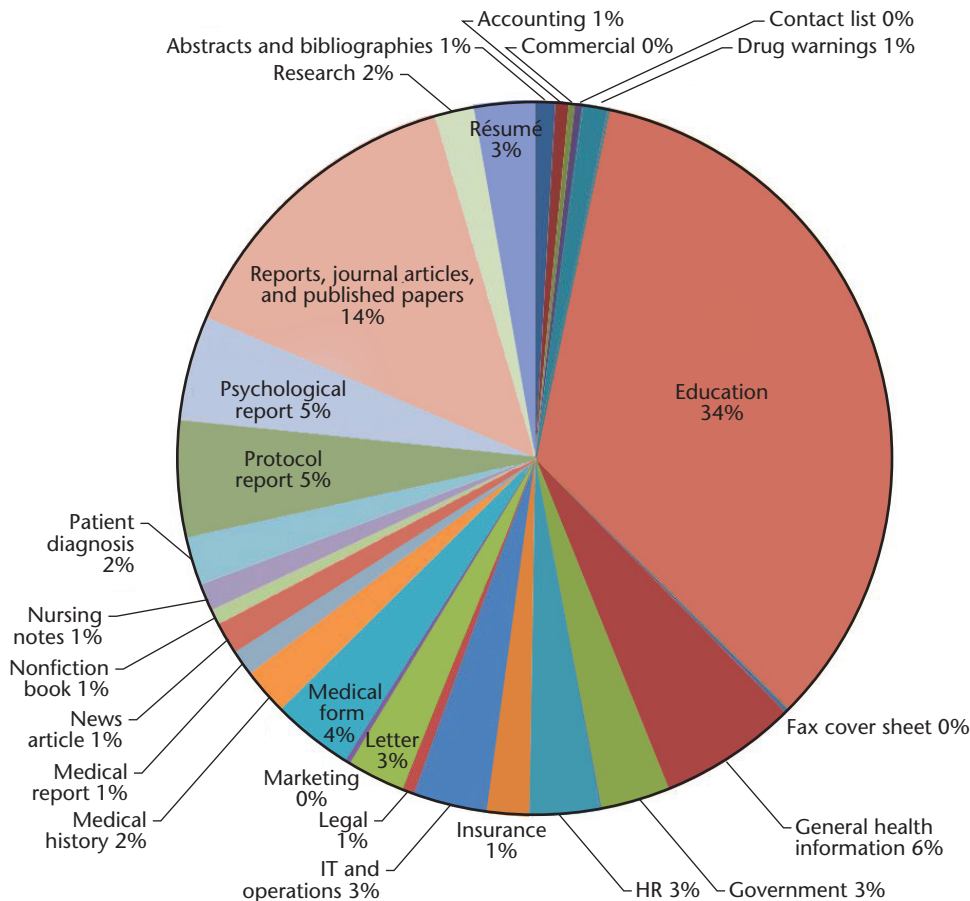


Figure 1. Categorization of files. We found a wide range of file types, from educational materials to operating documents. Categories such as nursing notes and patient diagnosis often contained sensitive protected health information.

Many of the files didn't disclose patient data. In fact, the majority of medical-related files available on P2P networks fell in the educational category—publicly available health-education materials, along with reports and journal articles. This finding was consistent with our earlier results and the fact that many P2P users are students. However, we did find a range of sensitive files related to organizational operation such as billings, insurance claims, marketing documents, and legal forms. Many of these included patient data. We also found human resources documents including job listings, cover letters, and résumés, some of which disclosed employees' sensitive personal information. To better understand the leaked data types and find clues on the usability failures that led to their disclosure, we manually assessed each file, then categorized the files by type and sensitivity (see Figure 1).

We rated all the files on a simple three-point scale, with 0 representing no risk, 1 for low risk, and 2 for high risk (that is, containing identifying information such as name, address, DOB, SSN, insurance number,

and health-related information). After categorizing the files, we found that approximately 15 percent of the relevant files posed some risk (a 1 or 2 on our scale) and 8 percent had significant PHI (a 2 on our scale). The files we found illustrate that PHI is often electronically stored outside enterprise-class EHRs in ad hoc file formats such as documents and spreadsheets that are vulnerable to inadvertent disclosure.

We also sought to assess the threat to these files by collecting samples of user-issued searches related to our digital footprints. These were search terms issued by users in these file-sharing networks. In 2009, we collected nearly 125,000 user-issued searches related to medicine and healthcare. We evaluated and rated these search terms on a simple three-point scale. In many cases, the search's intent was unclear. For example, we captured 17,993 searches on the term "medical," 12,983 on "DNA," and 8,329 on "medicine." Although these searches could be related to medical data, many were likely benign. For example, "medicine" could be a search for the film *Medicine Man*, the TV

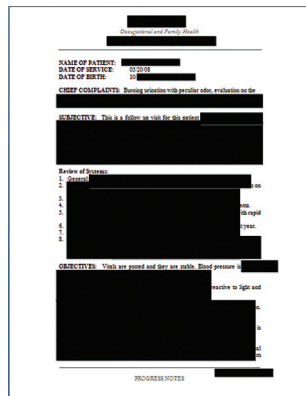


Figure 2. Redacted example of a born-vulnerable document with protected health information. Data collected in documents or spreadsheets might later be manually entered into an enterprise system.

show *Dr. Quinn, Medicine Woman*, the Bon Jovi song “Bad Medicine,” or the punk rock band Medicine.

However, other searches appeared to be more malicious and likely to be directed at recovering sensitive documents—for example, “University Research Park,” “HIV center,” “Broad Institute,” and “Columbia Center for Aids Research.” Remember, these aren’t Google searches, but rather searches in P2P file-sharing networks typically used for sharing music and videos. We assigned searches that were clearly intended to recover confidential research documents and other sensitive files the highest threat rating. For example, searches such as “public health passwords,” “HIV diagnosis,” “Breen Lab,” “Roche Labs,” and “Pittsburgh Cancer Institute files,” appear to focus on gaining access to either patient data or other confidential information. These specific searches indicate that P2P users are likely looking for more than patient information and might also be actively seeking out confidential research information. Overall, in our 2009 sample, nearly 18 percent appeared to have some level of threat, with about 1 percent representing highly focused searches. Given the sensitivity of files we collected, we conclude that malicious users are not only searching for sensitive files, but also finding them.

Finally, we collected another sample over a two-week period beginning on HITECH’s breach notification rules’ effective date (23 September 2009), using the same search terms. Given our interest in usability and the movement of data into unsecure formats, this time we focused exclusively on Excel spreadsheets (.xls) that might contain significant PHI. We collected 3,766 spreadsheets, of which 788 were unique, relevant files. Of those relevant files, 45 percent contained

information that held some risk for organizations or individuals, and 2.5 percent represented significant risk. For example, we found spreadsheets showing medical settlements that included names, addresses, DOBs, SSNs, phone numbers, employers, insurance information, and the financial settlement amounts. Others included medical forms and reports with PHI or healthcare employee information. Five qualified as major breaches under the new HITECH rules—that is, they contained significant PHI for more than 500 individuals. For example, we found one with detailed monthly case logs on several hundred mental health patients over a two-year period. Another contained insurance information for more than 7,000 individuals, including personally identifying information, their physicians, and dates of service. Yet another, more extensive spreadsheet included similar information on more than 16,000 patients, as well as employer information and diagnosis codes for each patient. Together, the five files contained sensitive PHI on more than 28,000 individuals.

Our research has shown that significant PHI is available on P2P networks. Much could be said about the flow of such data onto P2P networks, but the bigger issue is how and why this data ends up in unsecure, portable file formats. We argue that often this is a usability issue.

### Link between Usability and Leaks

To better understand the link between leaks and usability, we further examined the files and conducted interviews and field research with six healthcare organizations. This provided important clues into the usability problem.

First, we found that the sensitive files we collected could be broadly broken into two groups: those that were *born vulnerable* and those that were *moved vulnerable*. Born-vulnerable data includes files that were created directly from patient interactions. Figure 2 shows an example of a born-vulnerable document—in this case, patient notes. Often, these notes are created in a Microsoft Word file or spreadsheet, either by the provider or through a transcription service. As Figure 1 shows, we found many such files, including nursing notes, psychiatric evaluations, case-worker reports, medical histories, and patient correspondence. In many cases, they arise because healthcare organizations are small or technologically unsophisticated—they’ve moved toward EHRs, but their records are ad hoc file systems rather than enterprise systems. In other cases, employees create such documents because the enterprise system’s user interface is cumbersome, unusable, or not easily used in the patient’s presence (for example, a doctor taking digital notes during an examination). Such data collected in documents or

	A	B	C	D	E	F	H	I	J	K	L	M	N	O
1	txtReportCriteria	Carrier	Phone	Chart	Patient	Ins ID Nbr	DOB	Status	Aging	Total	Provider	CPT	Svc Mth	DOS
2	DOCT	MEDICARE PART B - (MC)	(866) 44				5/31/1937		5/18/2007	\$34.44				9/15/20
3	DOCT	MEDICARE PART B - (MC)	(866) 44				5/31/1937		5/18/2007	\$34.44				9/15/20
4	DOCT	AMERIGROUP OF FL MCD - (A	(800) 6				5/30/1946	DISABLED	6/20/2007	\$662.70				10/6/20
5	DOCT	MEDICAID - (MD)	(800) 2				3/24/1962		8/1/2007	\$102.92				10/18/20
6	DOCT	MEDICAID - (MD)	(800) 2				3/24/1962		8/1/2007	\$102.92				10/18/20
7	DOCT	UNITED HEALTH PPO - (UHPP	(888) 6				7/22/1933		3/22/2007	\$32.86				10/19/20
8	DOCT	MEDICARE PART B - (MC)	(866) 44				7/28/1963	DISABLED	6/20/2007	\$196.17				10/20/20
9	DOCT	MEDICAID - (MD)	(800) 2				4/6/1958	UNEMPLOY	5/1/2007	\$531.81				10/30/20
10	DOCT	MEDICAID - (MD)	(800) 2				1/23/1953	UNEMPLOY	10/28/2007	\$353.04				11/21/20
11	DOCT	MEDICAID - (MD)	(800) 2				4/6/1958	UNEMPLOY	10/23/2007	\$531.81				11/24/20
12	DOCT								11/11/2007	\$486.00				11/27/20
13	DOCT	MEDICARE PART B - (MC)	(866) 44				11/19/1934		8/15/2007	\$531.81				11/29/20
14	DOCT	MEDICARE PART B - (MC)	(866) 44				9/7/1936	RETIRED	6/12/2007	\$32.86				12/1/20
15	DOCT	MEDICAID - (MD)	(800) 2				1/21/1936		4/17/2007	\$34.80				12/2/20

Figure 3. Redacted example of a moved-vulnerable spreadsheet with protected health information. Often, employees create these files because enterprise systems aren't usable in that they either don't easily provide the desired functionality or the security and functionality make the application difficult to use in practice.

spreadsheets might later be manually entered into an enterprise system.

The second category of data, moved vulnerable, includes files generated from data residing in enterprise systems (see Figure 3). Often, employees create these files because enterprise systems aren't usable in that they either don't easily provide the desired functionality or the security and functionality make the application difficult to use in practice.

We observed several different categories of moved-vulnerable data in our collection of leaked files. In interviews, hospitals' chief information security officers (CISOs) described these same categories as "problem areas." Four of the most common categories were

- human resource—spreadsheets of employee data,
- operational—tools that help in daily operations such as scheduling,
- financial—spreadsheets for billing and collection, and
- research and analysis—data moved into spreadsheets to facilitate research and analysis.

Employees sometimes create these spreadsheets to supplement enterprise system capability; in other cases, they function as a workaround because of usability issues. For example, one CISO noted that physicians working at home could use a virtual private network (VPN) to gain access to hospital systems, but sometimes found it slow or cumbersome and chose to download data to their remote laptops. Likewise, researchers often move patient data used in research out of enterprise systems to perform statistical analyses not supported by the system. These tasks are typically episodic and can be done more safely using appropriate truncation, tokenization, and encryption; however, they're often quick workarounds created without the appropriate controls. For example, we found spreadsheets of HR data supporting tasks such as new employee training and benefits administration.

Operational tools are commonly used to supplement or replace poor enterprise systems. Through our field research, we observed many spreadsheets including those that facilitated scheduling of everything from surgery rooms to infusion suites. Likewise, clinic employees in larger hospitals who didn't like the patient appointment functionality developed spreadsheets or implemented their scheduling in Google Calendar. In all these cases, we found PHI. Possibly the most common operational tools we found were different versions of bed boards that kept track of patients, rooms, and beds. Spreadsheets keeping track of beds are common because of their flexibility and ease of use.

Our interviews indicated that financial systems are one of the biggest vulnerabilities. One hospital system CISO estimated that more than 60 percent of compliance issues came from billing. Given the US payment system's complexity and the importance of financial flows to healthcare organizations, it's little wonder this area faces challenges. One health executive in an imaging business noted that billing was his business's "core competency"—not image capture, processing, and reading. Simply ensuring timely payment for each image at the appropriate rate had become the most important part of the business.

From our collection of files, we observed some of the largest leaks stemming from billing and collection. Figure 3 represents such a spreadsheet, used internally to track payment; Figure 4 further illustrates this leak source. In this case, we found that a large hospital system had outsourced a collection of overdue payments. The figure shows part of a spreadsheet containing data the hospital shared with the collection agency. Rather than provide the agency with secure access into the organization's patient record system, hospital employees dumped the data into a large spreadsheet and sent it to the agency, without even Excel password protection. The collection agency later leaked the spreadsheet onto a P2P network. Evidently, a collection agency employee was using a P2P client on a work machine that also

	A	B	C	D	E	F	BV
1	providerName	providerFederalTaxId	patientFirstName	patientMiddleInitial	patientLastName	patientSSN	primaryDiagnosisCode
13804							413.9
13814							719.46
14082							719.41
14183							428
14379							584.9
14493							873
14518							786.52
14663							721.3
14784							788.2
14803							348.2
14882							682.6
15066							305
15136							
15174							790.5

Figure 4. Redacted example of a spreadsheet of more than 20,000 patients that contained extensive PHI including International Classification of Diseases diagnosis codes. Besides the possibility of fraud, such disclosure of diagnostic information can lead to embarrassment and social stigma.

held the spreadsheet. The spreadsheet contained vast PHI on more than 20,000 patients, including patient identification (address, phone number, SSN, DOB, and insurance carrier), employer information, attending physician name, and even diagnostic information.

### Discussion

Our analysis shows that substantial data hemorrhages have occurred and continued to occur even after HITECH disclosure rules became effective. However, this doesn't simply point to a HITECH failure—we didn't expect that HITECH would result in immediate elimination of PHI leaks. In fact, leaked files often circulate on P2P networks long after the original leak source is closed. However, our results show the challenges of reducing leaks in the healthcare supply chain. Eliminating P2P leaks isn't the answer. The files we found in P2P networks are the same ones that would be disclosed with a lost laptop, CD, or flash memory; P2P networks simply reflect the data types that can easily be disclosed.

Healthcare providers should consider many measures to protect against leaks. Too often the initial reaction is simply to block P2P networks or implement data loss prevention technologies that block files from migrating to unsecure machines (such as those that might participate in P2P). However, just as putting a collection of small bandages on a gaping wound won't stop the bleeding, plugging individual leaks can slow the data hemorrhage, but it won't solve the underlying problem. A more comprehensive strategy that includes P2P monitoring, disk-level encryption, tokenization, and data truncation will be more effective against many types of leaks. However, none of those solutions addresses the root cause. A long-term solution is to develop usable systems, with correspondingly usable security, to successfully eliminate risky

workarounds that move sensitive data out of protected enterprise systems and into portable user-stored files. Moving sensitive information out of ad hoc databases, such as spreadsheets and documents, and into secure enterprise-class software will eliminate most types of the inadvertent disclosure we observed.

A recent survey found that 60 percent of health organizations had experienced a breach in the past two years, costing the industry an estimated US\$6 billion annually.<sup>14</sup> Certainly, stiffer breach-reporting rules will create further financial incentives for firms to invest in new systems with better security. More important, incentives that facilitate the migration from legacy systems to new, more usable applications will reduce leaks. More research on usability in healthcare IT is necessary, both for large and small healthcare organizations. The industry needs usable systems that support everything from sole-practice offices to major healthcare organizations. Usable applications that keep the data stored in more secure systems and stop the flow of sensitive PHI into unprotected, ad hoc files will slow patient data hemorrhages. □

### Acknowledgments

This research was partially supported by the US National Science Foundation, grant award CNS-0910842, under the auspices of the Institute for Security, Technology, and Society.

### References

1. J.R.B. Halbesleben, D.S. Wakefield, and B.J. Wakefield "Work-Arounds in Health Care Settings: Literature Review and Research Agenda," *Health Care Management Rev.*, vol. 33, no. 1, 2008, pp. 2–12.
2. A.L. Tucker and A.C. Edmondson, "Why Hospitals Don't Learn from Failures: Organizational and Psycho-

- logical Dynamics that Inhibit System Change,” *California Management Rev.*, vol. 45, no. 2, 2003, pp. 55–72.
3. M.E. Johnson, “Data Hemorrhages in the Health-Care Sector,” *Lecture Notes in Computer Science*, R. Dingle-dine and P. Golle, eds., LNCS 5628, Springer-Verlag, 2009, pp. 71–89.
  4. K. El Emam et al., “The Inadvertent Disclosure of Personal Health Information through Peer-to-Peer File Sharing Programs,” *J. American Medical Informatics Assoc.*, vol. 17, no. 2, 2010, pp. 148–158.
  5. M. Sturdevant, “1.5 Million Medical Records at Risk in Data Breach,” *The Hartford Courant*, 19 November 2009; [www.courant.com/health/hc-healthbreach1119.artnov19,0,1798384.story](http://www.courant.com/health/hc-healthbreach1119.artnov19,0,1798384.story).
  6. T. Murphy, “Wellpoint Customer Information Exposed,” Associated Press, 8 Apr. 2008; <http://attrition.org/dataloss/2008/04/wellpoint01.html>.
  7. R. Nix, “Email Leaks 350 Baptist East Employee Social Security Numbers,” WHAS11 television station, 26 Oct. 2009; [www.whas11.com/news/consumer/Email-leaks-350-Baptist-East-employee-Social-Security-numbers-66250142.html](http://www.whas11.com/news/consumer/Email-leaks-350-Baptist-East-employee-Social-Security-numbers-66250142.html).
  8. *Title IV Health Information Technology for Economic and Clinical Health*, Majority Staff of the Committees on Energy and Commerce, Ways and Means, and Science and Technology, 16 Jan. 2009; <http://enpointeblog.com/wp-content/uploads/2010/10/HITECH-Act1.pdf>.
  9. “Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Proposed Rule,” *Federal Register*, vol. 75, no. 8, 13 Jan. 2010; <http://edocket.access.gpo.gov/2010/pdf/E9-31217.pdf>.
  10. “Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule,” *Federal Register*, vol. 75, no. 144, 28 July 2010; <http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf>.
  11. “Breach Notification for Unsecured Protected Health Information; Interim Final Rule,” *Federal Register*, vol. 74, no. 162, 24 Aug. 2009; <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.
  12. “Rules and Regulations,” *Federal Register*, vol. 74, no. 209, 30 Oct. 2009; [www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf](http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf).
  13. M.E. Johnson and N. Willey, “Will HITECH Heal Patient Data Hemorrhages?” *Proc. 44th Hawaii Int’l Conf. System Sciences (HICSS 11)*, 2011.
  14. A. Moscaritolo, “Breaches Cost Health Care Industry \$6 Billion Annually,” *SC Magazine*, 9 Nov. 2010; [www.scmagazineus.com/breaches-cost-health-care-industry-6-billion-annually/article/190493](http://www.scmagazineus.com/breaches-cost-health-care-industry-6-billion-annually/article/190493).

**M. Eric Johnson** is the director of Tuck’s Glassmeyer/McNamee Center for Digital Strategies and the Benjamin Ames Kimball Professor of the science of administration at the Tuck School of Business at Dartmouth College. His teaching and research focuses on information technology and security’s impact on

supply chain management. Johnson has a PhD in engineering from Stanford University. Contact him at [m.eric.johnson@dartmouth.edu](mailto:m.eric.johnson@dartmouth.edu).

**Nicholas D. Willey** was a research associate at Dartmouth College. His research interests include health care, privacy, and Web 2.0. Willey has an MS in engineering management from Dartmouth College’s Thayer School of Engineering. Contact him at [nicholas.d.willey.06@alum.dartmouth.edu](mailto:nicholas.d.willey.06@alum.dartmouth.edu).



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.