Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Privacy Review:

Chatham-Kent IT Transition

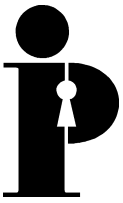
Pilot Project

April 22, 2002

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A9

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

Introduction

Primary Care Reform

In May 1998, the Ministry of Health and Long-Term Care (MOHLTC) and the Ontario Medical Association (OMA) launched a pilot project to reform primary care in Ontario. Primary care is the first level of contact that a patient has with the health care system.

The pilot project involved setting up primary care networks (PCNs) — groups of doctors, nurses and other health professionals who deliver primary care to patients. Under this model, patients are enrolled or "rostered" with a specific PCN. Except for emergency situations, patients agree to see only their family doctor or other doctors within the PCN for primary care medical advice or treatment. Currently, there are 14 PCNs in Ontario. Thirteen of these PCNs, including one in Chatham-Kent, are pilot project sites.

In March 2001, the Ontario government established an agency called the Ontario Family Health Network (OFHN) to implement primary care reform throughout the province. It also decided that future PCNs would be known as "family health networks" (FHNs). The OFHN's target is to have 80 per cent of family physicians join an FHN within three years.

A key component of primary care reform is the use of information technology to deliver health care services to patients in a more effective manner. The Ontario government is investing $250 million to support FHNs, including $150 million for information technology. The MOHLTC, the OFHN and the OMA are also collaborating on a three-year "ePhysician Project" that will support the use of information technology in primary care reform. The OFHN is providing the ePhysician Project with office space and other support services.

The Benefits and Risks of Information Technology

Although computers are used in many doctors' offices for administrative purposes, most patient records continue to be stored in paper format. According to the Canadian Medical Association's 2001 Physician Resource Questionnaire, only 10.8 per cent of general and family practitioners in Canada use a computer for the purpose of creating electronic patient records.[1]

The use of information technology to create, store and transmit electronic patient records has enormous potential for increasing the quality of health care provided to patients in Ontario. If an unconscious patient arrives at a hospital emergency ward, the attending physician could make a

[1] Ontario Ministry of Health and Long-Term Care, *Evaluation of Primary Reform Pilots in Ontario — Phase 2 Interim Report* by PricewaterhouseCoopers, October 31, 2001, p. 78, <www.ontariofamilyhealthnetwork.gov.on.ca/english/pilot/pilot_eval_2.pdf>.

more informed diagnosis and treatment decision if he or she could electronically access that patient's medical records. Similarly, if Health Canada pulls a drug off the market or issues a warning about a specific drug, a family physician who uses electronic patient records could search his or her database and quickly notify patients who are taking the drug.

A 2001 survey by PricewaterhouseCoopers found that Canadians are generally amenable to the possibility of storing personal health records on a computer in a central location. Eighty-two per cent of respondents were somewhat or very willing to have computerized personal health records stored centrally to give their doctors easier and faster access to their own records. Eighty-five per cent expressed a willingness to permit central storage of their personal health records so they could have access to and control over their own records.[2]

However, the creation of electronic patient records also poses numerous risks, particularly from a privacy perspective. Patient records that are stored on a server in a central location may be vulnerable to attacks from both the outside and inside. For example, if the server is open to the Internet, patient records could be vulnerable to computer hackers, especially if there were inadequate security safeguards in place. Moreover, a person who works at the location where the server is housed could potentially download, steal, or compromise patient records in the absence of stringent checks and audit trails having been implemented.

Personal health information is one of the most sensitive forms of personal information. An electronic patient record might contain information about abortions, sexually transmitted diseases, depression, drug abuse or other matters that individuals may not want shared with anyone else except their doctor. As a result, health professionals and institutions with custody of electronic patient records have a duty to ensure that adequate security safeguards are in place to protect the privacy of these records.

Although this review is focusing on electronic patient records, it should be noted that paper records are also vulnerable to privacy abuses. For example, documents containing medical test results and other personal health information were recently found literally blowing in the wind behind a doctor's office in Calgary, Alberta.[3] Similarly, a community newspaper in Toronto recently reported that it had found thousands of OHIP billing slips from a closed medical clinic in clear plastic garbage bags on a sidewalk.[4] Thus, health professionals and institutions should also ensure that they have proper safeguards in place to protect all paper records containing personal health information.

---

[2] S. Martin, "Canadians don't appear to fear electronic medical records" (2001) 164(12) *Canadian Medical Association Journal*, p. 1739, <www.cma.ca/cmaj/vol-164/issue-12/1739a.asp>.

[3] N. Pierson, "Medical mayhem: Private records found on street," *The Calgary Sun*, 20 December 2001, p. 2.

[4] K. Hill, "Personal OHIP records left on Cabbagetown sidewalk," *eye*, 24 January 2002, <www.eye.net/eye/issue/issue_01.24.02/news/ohip.html>.

The Chatham-Kent IT Transition Pilot Project

In October 2001, the physicians in the Chatham-Kent PCN formally agreed to participate in the first "information technology transition pilot project." The purpose of this pilot, which is being supported by the ePhysician Project, is to test the use of certain forms of information technology and to identify any weaknesses or vulnerabilities before the use of such technology is expanded province-wide.

Eight Chatham-Kent physicians agreed to participate in the project. The computer hardware used by the physicians includes desktop computers, laptop computers, and devices known as "tablets." A tablet is a portable, wireless device with a touch screen. When a physician moves from room to room to talk to patients, he or she can use the touch screen on the tablet to enter patient information. This personal health information is sent to a docking station on a desk in the physician's office and then securely transmitted across the Internet to a server, which is owned by the Chatham-Kent physicians, but housed in the SSH data centre.

The physicians have chosen a clinical management system produced by York-Med Systems Inc., a company based in Markham, Ontario. One software program (Purkinje) allows the physicians to manage their patients' clinical information electronically by creating patient records, entering symptoms, recording tests and treatment, checking for drug interactions and printing out legible prescriptions. A second software program (Medical Desktop) enables physicians and their staff to perform administrative functions, such as scheduling appointments for patients and billing OHIP electronically.

The physicians have also selected a software program called Vividesk, which is supplied by iW Technologies, a company based in Edmonton, Alberta. Vividesk is a form of "portal" technology. It acts as a single door or gateway that allows a physician to access the clinical management system, office applications, medical applications (e.g., medical journals and books) and Internet links relevant to physicians, such as the OMA's Web site. Currently, Vividesk has only been installed on one doctor's computer.

Smart Systems for Health (SSH), an office within the MOHLTC, is providing secure infrastructure for the collection, storage, transmission and exchange of personal health information within the Chatham-Kent project, including a secure server environment for hosting personal health information, a high-speed digital network protected by encryption technology and virtual private network software, a secure authentication process for the physicians and their staff and encrypted e-mail within the group of physicians.

The Chatham-Kent pilot project went live on November 1, 2001 with little public fanfare. However, in late November and early December 2001, a reporter with *The Globe and Mail* contacted the Information and Privacy Commissioner of Ontario (IPC). The reporter informed us that a source

had provided him with internal SSH documents. The documents allegedly contained evidence that the personal health information of patients involved in the Chatham-Kent project was not being adequately protected.

The Commissioner immediately contacted Mike Connolly, Chief Executive Lead of SSH. On December 5, 2001, the IPC met with Mr. Connolly and other MOHLTC officials to obtain their preliminary response to the allegations raised by the *Globe* reporter. On December 7, 2001, the reporter interviewed Ken Anderson, the IPC's Director of Legal and Corporate Services, and provided him with more detailed information about the allegations provided by the source.

Allegations Reported by *The Globe and Mail*

On December 10, 2001, an article appeared in the *Globe* that reported the following allegations:

- According to an e-mail from an MOHLTC official, vulnerability tests showed that the system could be "hacked into by anyone with skill" over the Internet. These security problems became apparent on the first day the system was up and running but the IPC was not informed.
- Patients in Chatham-Kent were not fully informed about what happens to their personal health information. Although they were told that other doctors could see their files, most patients were not informed that their information is stored on a server in a government building in Toronto.
- A computer technician took unencrypted backup tapes, containing thousands of medical records, to his home for several nights. Three of the tapes were allegedly lost.
- Three private companies have been granted access to patient information. Two of the companies, software developers that helped build the system, can look at raw data files, including patients' names and medical histories.

On December 12, 2001, we held a further meeting with officials from both SSH and the ePhysician Project to obtain their response to the allegations reported in the *Globe* article. At this meeting, both SSH and ePhysician Project officials expressed support for an IPC review of the Chatham-Kent pilot project. On December 13, 2001, the IPC received a letter from SSH that contained the following statements:

- With respect to the allegation that three tapes containing health records were lost, we confirm that no tapes have been lost and that all backup tapes for the ePhysician pilot systems in Chatham-Kent are fully accounted for.

- With respect to the allegation that vulnerability tests showed that the system can be "hacked into by anyone with skill," and that security problems became apparent on the first day the system was up and running, we confirm that there have been no successful hacking attempts and no unauthorized disclosure of personal health information.

This letter also invited the IPC "to conduct an independent verification to confirm the accuracy of these statements." On December 18, 2001, the IPC received a letter from MOHLTC Deputy Minister Daniel Burns that pledged his ministry's full co-operation with the IPC's review.

During January and February 2002, we interviewed more than 20 individuals involved in the pilot project, including ePhysician Project and SSH officials, outside consultants who had conducted vulnerability tests on the system and the private vendors supplying software to the physicians. We also made a site visit to Chatham-Kent and met with two physicians: Dr. Brian Gamble and Dr. Ian MacLean. During the course of our review, we received the full co-operation of all parties.

IPC Jurisdiction

The IPC's review of the Chatham-Kent pilot project was conducted with the consent of the Ontario government and the Chatham-Kent group of physicians. However, it may be useful to briefly set out the extent of our jurisdiction in this review.

Under section 59(a) of the *Freedom of Information and Protection of Privacy Act*, the Commissioner may offer comment on the privacy protection implications of proposed legislative schemes or government programs. The Chatham-Kent pilot project is the first segment of a proposed ePhysician Project/SSH program to expand the use of information technology at FHNs in Ontario. Consequently, in this review, the IPC will be offering comment on the privacy protection implications of using information technology in the Chatham-Kent pilot project, with a specific focus on the allegations raised in the *Globe* article.

Fair Information Practices

Currently, there are no legislated privacy protection rules for personal health information in Ontario. However, the government recently released draft legislation, the *Privacy of Personal Information Act, 2002*, that would cover the collection, use and disclosure of personal information by private, non-profit and health organizations in the province. The government requested comments from the public on the draft legislation by March 31, 2002. However, it is not clear when the legislation will be introduced in the legislature.

In the interim, we believe that the personal health information of patients, when not in the custody or under the control of a government institution, should be governed by internationally recognized fair information practices. These 10 practices, which are codified in the Canadian Standard Association's *Model Code for the Protection of Personal Information*, outline responsible information-handling practices designed to protect privacy. They form the basis for privacy legislation in virtually all jurisdictions and include:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- Security Safeguards
- Openness
- Challenging Compliance
- Individual Access

A detailed description and definition of each of these principles is included in Appendix A of this report. Many of the allegations reported in the *Globe* article, which we will be addressing in this report, deal with whether SSH has put adequate security safeguards in place to protect the personal health information of Chatham-Kent patients. However, we hasten to add that security is only one tool for protecting privacy. To the maximum extent possible, the ePhysician Project, SSH and the Chatham-Kent physicians should comply with all 10 fair information practices to ensure that the privacy rights of Chatham-Kent patients are being respected, protected and fulfilled.

Issues Arising in the Review

In this review of the Chatham-Kent pilot project, we will be addressing the following five issues:

A. Is SSH taking adequate steps to protect the personal health information of Chatham-Kent patients from outside attacks?

B. Is SSH taking adequate steps to protect the personal health information of Chatham-Kent patients from inside attacks?

C. Did a computer technician take three backup tapes home that contained the personal health information of patients? Were these backup tapes lost?

D. Are patients being fully informed about what is happening with their personal health information?

E. Did the ePhysician Project and SSH conduct a privacy impact assessment on the Chatham-Kent project?

Results of the Review

Issue A: Is SSH taking adequate steps to protect the personal health information of Chatham-Kent patients from outside attacks?

The threat of attacks from hackers is a clear and present danger for any organization that is mandated with the responsibility of storing electronic patient records. In the summer of 2000, a hacker broke into the University of Washington Medical Centre in Seattle and downloaded the personal health information of patients. The hacker used "sniffer" software to access the usernames and passwords of a number of hospital employees from an unprotected server. He then used these credentials to access thousands of medical records. After this incident became public, the hospital acknowledged that at the time of the hacking, there were no firewalls separating the databases containing the electronic patient records from the Internet, and that usernames and passwords were not encrypted.[5]

During the course of our review, we found that SSH has undertaken stringent measures to protect the personal health information of Chatham-Kent patients from outside attacks, including the following five measures:

- **Secure Servers** — Both the clinical management system and the Vividesk program used by the Chatham-Kent physicians are hosted in servers located in a secure SSH data centre in downtown Toronto. Although the clinical management system databases containing the personal health information of patients are not encrypted, SSH has put multiple firewalls in place to protect the servers from outside attacks. Moreover, firewall, intrusion-detection and other logging systems record any unauthorized attempts to access the servers.

- **Physical Security** — The data centre that houses the servers has a high degree of physical security. The servers are located in a steel security cage that is closed and locked during non-working hours. SSH staff monitor the data centre during office hours, and a security guard sits outside the data centre during non-working hours, which provides 24-hour security coverage. Video surveillance cameras record all activity both inside and outside the data centre 24 hours a day. Although the camera feed is not monitored by anyone in real time, the tapes are reviewed by SSH security officers if any suspicious activity is detected or reported.

- **Network Services** — SSH has connected each physician to the Internet using a high-speed digital network. To prevent outside parties from accessing or intercepting information, SSH has secured the network with encryption technology and has installed virtual private network (VPN) software on the physicians' workstations. A firewall has also been installed to protect the physicians' local area networks and workstations from outside attacks.

[5] T. Chin, "Security breach: Hacker gets medical records," *amednews.com — The Newspaper for America's Physicians*, 29 January 2001, <www.ama-assn.org/sci-pubs/amnews/pick_01/tesa0129.htm>.

- **Encrypted E-mail** — The VPN software provides the eight physicians with a secure tunnel that encrypts e-mail sent within the group. However, any e-mail sent outside the group of physicians is not encrypted.

- **Security Authentication** — To ensure that only the physicians and their authorized staff can access the clinical management system on their desktop and laptop computers, SSH has supplemented the traditional user-authentication process with a "key fob." A key fob is a key chain-sized rectangular device that displays a new set of numbers every 60 seconds. The physicians and their staff are required to enter a username, password and a key fob number. The user enters this string of numbers after the password. SSH informed us that a key fob is uniquely assigned to each authorized user. In other words, even if an unauthorized individual were somehow able to obtain an authorized user's username and password, he or she would still not be able to access the system without that user's key fob.

The "Hacking" E-mail

The *Globe* article cites an e-mail from an MOHLTC official that allegedly states that vulnerability tests showed that the SSH system could be "hacked into by anyone with skill" over the Internet.

On February 4, 2002, SSH provided us with a copy of an e-mail that appears to be the one that was quoted in the *Globe* article. The e-mail is dated November 22, 2001 and was authored by SSH's legal counsel. It was sent to an SSH consultant, and copied to three other individuals. In the e-mail, SSH's legal counsel raises four issues that were apparently discussed at an OFHN team meeting on the previous day (November 21, 2001). The passage in the e-mail that apparently gave rise to the quote about hacking in the *Globe* article is as follows: "In the Vividesk application, the physicians' passwords are held on behalf of the physicians in manner [*sic*] that they can be 'hacked into by anyone with skill'?? Who is responsible for the security of these passwords?"

SSH informed us that the reference in the e-mail to the Vividesk application related to a potential, rather than an actual, risk. The Vividesk application has the capacity to store the physicians' usernames and passwords. When SSH was testing the application, it found that the physicians' user credentials would be stored in plain text rather than encrypted form. Consequently, it asked iW Technologies to supply them with an updated version of Vividesk that enables the storage of usernames and passwords in encrypted form. SSH emphasized that no physician user credentials for Vividesk were in danger of being hacked because they were never stored on a server in unencrypted form.

SSH also detected another problem shortly after the *Globe* article was published. It found that Dr. Gamble's user credentials for the Vividesk application were travelling over the Internet to iW Technologies in plain text rather than going through the secure VPN encryption pipeline that

SSH had set up. This problem was caused by the locations of the live and backup sites for Vividesk. SSH found that the sites were wrongly configured — the live site was located at iW Technologies in Edmonton and the backup site was located at SSH in Toronto. Consequently, SSH shut down the test portal until this problem was resolved by iW Technologies.

SSH advised us that Dr. Gamble's Vividesk profile did not include his passwords for the clinical management system. Consequently, even if a hacker had intercepted his Vividesk user credentials while they were travelling over the Internet to iW Technologies in plain text, it would not have been possible to use that information to access any personal health information stored at SSH.

SSH also emphasized that the Vividesk application was in "test mode" between November 2001 and January 2002, which is when the "hacking" e-mail was circulated and the configuration problem with the live and backup sites was identified. SSH advised us that iW Technologies "made numerous changes to their product to meet the high security requirements of the project.... At no time was personal health information at risk or compromised, and the company was extremely co-operative in re-engineering their product to work in the SSH environment."

Vulnerability Tests

We sought information from SSH about the vulnerability tests that it had conducted before the Chatham-Kent project went live on November 1, 2001. SSH informed us that it had asked an independent third party to conduct two vulnerability tests:

- an Internet penetration test on the server at SSH; and
- a simulated doctor's office test.

Both of these tests were conducted by Cinnabar Networks Inc., which is based in Ottawa. SSH provided us with copies of both vulnerability test reports, and we also interviewed the individuals who conducted the tests.

Internet Vulnerability Test

Cinnabar conducted the Internet penetration test starting at 5:00 p.m. on the evening of October 31, 2001 and ending at 7:00 a.m. on November 1, 2001. The test uncovered four low-risk vulnerabilities and two medium-risk vulnerabilities, both of which related to the server. In the Internet penetration test report, Cinnabar characterized the two medium-risk vulnerabilities in the following way:

- "User credentials are sent as plaintext … and are susceptible to interception and replay. An attacker who is able to sniff sessions to the server can collect user credentials and replay them to gain unauthorized access."

- "…[T]he site does not use any form of encrypted tunnel for communicating with the client. An attacker who is able to sniff sessions to the server can collect data requested by the legitimate user."

On January 9, 2002, SSH provided us with an explanation for the two medium-risk vulnerabilities. At the time of the first test, SSH did not inform Cinnabar that it uses a VPN encryption product that provides a secure tunnel between the physicians' offices and the server at SSH. Moreover, SSH has also provided physicians and their staff with key fobs to supplement the traditional user-authentication process, which would prevent a hacker who had only gained access to usernames and passwords from accessing the clinical management system on the server.

In a letter to SSH dated January 4, 2002, Cinnabar stated that, "As a result of the use of a VPN encryption product and strong (token-based) authentication, the remaining Internet vulnerabilities were all rated low-risk." In our interview with the Cinnabar consultant who conducted the Internet penetration test, he indicated that he was satisfied with SSH's explanation. SSH has also assured us that it has addressed the four low-risk vulnerabilities identified in the test.

Simulated Doctor's Office Test

A different Cinnabar consultant conducted a simulated doctor's office test on November 5, 2001 and made a number of observations, including a reference to the potential vulnerabilities of wireless and handheld devices in the medical field. He noted that "[t]he Wireless Equivalent Privacy (WEP) has been broken for 40 bit and … is not as secure as it claims to be. With a wireless network, an attacker only has to be within 300 feet of the AP to attempt to connect to the network."

SSH has assured us that it has addressed any vulnerabilities identified in the simulated doctor's office test. We would urge SSH to maintain a close eye on the potential vulnerabilities associated with wireless devices.

As noted earlier, the Chatham-Kent physicians have been provided with portable, wireless tablets with touch screens. When a physician moves from room to room to talk to patients, he or she can use the touch screen on the tablet to enter patient information. This personal health information is sent to a docking station on a desk in the physician's office and then securely transmitted across the Internet to a server, which is owned by the Chatham-Kent physicians but housed in the SSH data centre.

Wireless networks are notoriously easy to crack if proper security safeguards are not in place. In Canada and the United States, individuals have parked their cars outside buildings that house wireless networks and used a homemade antenna and a laptop with sniffing software to successfully detect unencrypted wireless networks, that could be hacked into with ease.

Most wireless networks use WEP, an encryption mechanism for the 802.11b standard, to protect the transmission of data. However, in August 2001, two programmers released a tool called "AirSnort" that can allegedly crack through WEP encryption and intercept data moving across a wireless network.[6]

Could a hacker use a tool such as "AirSnort" to grab the personal health information of patients when a Chatham-Kent doctor uses the portable tablet? While it is possible that this could happen, it appears unlikely because the wireless tablets used by the physicians are protected by end-to-end encryption. In our interviews with SSH and York-Med Systems Inc. officials, we were told that the VPN software ensures that all data is fully encrypted from the physician's office to the server at SSH, regardless of the device used (i.e., tablet, desktop computer or laptop computer). When a physician enters patient information on a wireless tablet, the data is first encrypted by the VPN software and then sent from the tablet to the docking station using WEP. The data is then securely transmitted across the Internet to the server at SSH. While WEP has weak encryption, the data has already been strongly encrypted by the VPN technology.

Network Review

SSH also asked a Toronto-based company, ITS, to conduct a high-level review of the entire network architecture for the project. In its report, ITS made a series of observations that SSH appears to have addressed. The ITS employee who conducted the network review told us that he believes that the SSH has done "a pretty good job" in designing the network architecture. However, he also stated that he believes that SSH should conduct a penetration test for the whole SSH environment (i.e., an end-to-end security test). In our view, this is a reasonable suggestion that SSH should take into account.

Recommendation:

1. SSH should consider undertaking an end-to-end security test of the entire network.

[6] M. Delio, "Wireless networks in big trouble," *Wired News*, 20 August 2001, <www.wired.com/news/wireless/0,1382,46187,00.html>.

Timing of the Tests

Overall, we believe that SSH should be commended for conducting a number of security measures — an Internet penetration test, a simulated doctor's office test and a high-level network review. However, we have some concerns about the timing of the tests.

The Internet penetration test was conducted on the evening of October 31, 2001 and the morning of November 1, 2001. The simulated doctor's office test was conducted on November 5, 2001. Although Cinnabar provided SSH with preliminary results both orally and in writing shortly after the tests were completed, the final reports were not submitted until November 13, 2001. The network review report was received on October 30, 2001.

The Chatham-Kent project went live on November 1, 2001. In early November, at least some of the Chatham-Kent physicians were entering and storing the personal health information of patients on the server at SSH.

In our view, the vulnerability tests and network review were conducted at unacceptably late dates. If the Internet penetration test or simulated doctor's office test had detected high-risk vulnerabilities that could have exposed the personal health information of patients to outside attacks, SSH may have been compelled to shut down the entire system to remedy these vulnerabilities. Fortunately, this was not the case.

Recommendation:

2. For future pilot projects, SSH should conduct vulnerability tests and a network review at least 14 days before a project goes live. This will ensure that SSH has sufficient time to remedy any vulnerabilities that may be identified.

Privacy-Enhancing Technologies

Privacy-enhancing technologies (PETs) such as strong encryption can play an important role in preventing electronic patient records from being viewed by outside attackers. Ideally, personal health information should be strongly encrypted when it is stored in a computerized database or transmitted over the Internet. Encryption is a mathematical process that changes data from plaintext (i.e., which can be read) to an unintelligible or scrambled form. In order to reconstruct the original data or decrypt it, an individual must have access to a decryption key. The use of strong encryption makes it extremely difficult for outsiders to decipher data that is stored in a database or transmitted across the Internet.

We commend SSH for using encryption technology to protect the privacy of personal health information in certain components of the Chatham-Kent project. For example, all transmission of data between the physicians' workstations and SSH is encrypted using 128-bit VPN technology. This VPN software also provides the eight physicians with a secure tunnel that encrypts e-mail sent within the group. Any e-mail sent outside of the group of physicians (e.g., to hospitals and labs) is not encrypted, although Dr. Gamble informed us that the Chatham-Kent physicians do not send any e-mail containing the personal health information of patients to these institutions. To address this issue, SSH is pursuing a longer-term strategy that would involve issuing Public Key Infrastructure (PKI)[7] certificates to facilitate the use of encrypted e-mail between physicians and outside institutions such as hospitals and labs.

During the course of our review, we found that the clinical management system databases located on the server hosted at SSH are not encrypted. These databases contain personal health information of patients that has been inputted into the clinical management system by the Chatham-Kent physicians. SSH informed us that "[i]n their current form, the Chatham/Kent applications are not capable of using privacy-enhancing technologies such as encryption. While SSH is aware of many privacy-enhancing approaches, the vendors of the Chatham/Kent applications currently do not support these approaches, nor is it a common practice within the vendor community for these types of clinical management systems." It also noted that the encryption solutions that are currently available would have "degraded performance to the point where the application would be unworkable."

Overall, SSH has put in place strong security measures (e.g., multiple firewalls) to prevent an outside attacker from gaining access to the personal health information contained in the databases that are stored on the server. However, before the use of information technology is expanded to other FHNs in Ontario, we would urge SSH to revisit the feasibility of encrypting clinical management system databases, since database encryption would offer an added layer of protection in the event that an outside attacker was able to gain access to the server.

SSH should also consider using other privacy-enhancing technologies, such as pseudonymizing tools. For example, an article published in a British health journal in 1998 examines how PETs can be used in a hospital information system (HIS) to ensure compliance with European data protection laws. Specifically, the article looks at how "pseudo identities" are used in a Dutch HIS to hide the true identity of a data subject in the event an unauthorized user breaches the system. The solution in the Dutch HIS involves the encryption of patient identification numbers to create a pseudonym.[8]

---

[7] A Public Key Infrastructure (PKI) enables users of an insecure public computer network such as the Internet to securely exchange data through the use of a public and private cryptographic pair of keys that was obtained and shared through a trusted authority.

[8] G. van Blarkom, "Guaranteeing requirements of data-protection legislation in a hospital information system with privacy-enhancing technology" (1998) 15(4) *The British Journal of Healthcare Computing & Information Management* at 30.

Recommendation:

3. Before the use of information technology is expanded to other FHNs in Ontario, the ePhysician Project and SSH should:

    a) revisit the feasibility of encrypting any clinical management system databases stored on the server at SSH; and

    b) examine the feasibility of implementing further privacy-enhancing technologies, such as pseudonymizing tools, to prevent outside attackers from linking personal health information to an identifiable individual.

Issue A: Conclusion and Recommendations

In our view, SSH is taking adequate steps overall to protect the personal health information of Chatham-Kent patients from outside attacks. However, we would make the following recommendations:

1. SSH should consider undertaking an end-to-end security test of the entire network.

2. For future pilot projects, SSH should conduct vulnerability tests and a network review at least 14 days before a project goes live. This will ensure that SSH has sufficient time to remedy any vulnerabilities that may be identified.

3. Before the use of information technology is expanded to other FHNs in Ontario, the ePhysician Project and SSH should:

    a) revisit the feasibility of encrypting any clinical management system databases stored on the server at SSH; and

    b) examine the feasibility of implementing further privacy-enhancing technologies, such as pseudonymizing tools, to prevent outside attackers from linking personal health information to an identifiable individual.

Issue B: Is SSH taking adequate steps to protect the personal health information of Chatham-Kent patients from inside attacks?

Although computer networks face potential outside attacks from hackers, inside attacks also pose a real and significant risk to the privacy of personal information. An inside attack occurs when a trusted insider inappropriately accesses, alters or destroys personal information. In the Chatham-Kent pilot project, inside attacks could occur within the SSH environment or in the physicians' offices. The "insiders" include SSH consultants, the employees of software companies such as York-Med Systems Inc. and iW Technologies Inc., and the physicians' staff.

SSH Consultants

SSH consultants are individuals who have been hired to perform work for SSH. Some of these consultants have responsibilities or duties that require them to have access to the data centre. SSH's data centre lead is responsible for determining who has access to the data centre. According to a list provided to us by SSH, dated January 8, 2002, approximately 19 SSH consultants and three security personnel have access to the data centre. SSH acknowledged that four consultants have the ability to see the personal health information of patients on the server but emphasized that such access is "for the express purposes of providing normal system support and maintenance."

Any individual hired by SSH must sign a standard security and confidentiality agreement and is required to comply with SSH's facility access policy and privacy policy. In addition, all SSH consultants requiring access to the data centre must now sign a "third tier" security and confidentiality agreement that was finalized at the end of January 2002.

SSH is also developing a process whereby the Chatham-Kent physicians would sign "Physician Authorization Forms" that give specific SSH consultants access to SSH services. Each SSH consultant who has been authorized to access the system would be required to sign a "User Acceptance" agreement. Under this agreement, the SSH consultants agree to take reasonable steps to protect their passwords and key fobs from loss or unauthorized use and not to share them with anyone else. In addition, they are required to acknowledge that they are "responsible for any unauthorized disclosure of personal information regarding patients through the inappropriate use of my authorized access."

York-Med Systems Inc. Employees

SSH informed us that each physician involved in the Chatham-Kent pilot project has signed a contract with York-Med that requires the company to provide database administration and application support services. SSH acknowledges that "York-Med employees have the ability to see 'patient names and medical histories' but are only legally allowed to do this in performing normal

system support and maintenance activities. This is a standard practice for all Clinical Management System vendors and their clients."

All physicians sign "Physician Authorization Forms" that give specific York-Med employees access to SSH services. We found that 13 York-Med employees have been granted such access. Each York-Med employee who has been authorized to access the system must sign a "User Authorization Agreement." This agreement contains the same obligations as the "User Acceptance" agreement that SSH consultants are required to sign.

SSH also emphasized that York-Med has internal policies and processes in place to protect sensitive information, and that employees must sign a confidentiality agreement. During the course of our review, we interviewed one York-Med employee who has access to the SSH system. He appeared to have a reasonable understanding of his contractual obligations and grasped the importance of not disclosing any personal health information that he may come across while performing his duties.

iW Technologies Inc. Employees

iW Technologies is supplying the physicians with the Vividesk portal application. As with York-Med's clinical management system, the Vividesk application is housed on a server at SSH.

The physicians sign "Physician Authorization Forms" that give specific iW Technologies employees access to SSH services. We found that six iW Technologies employees have been granted such access. Each employee who has been authorized to access the system must sign a "User Authorization Agreement." This agreement contains the same obligations as the agreements that the SSH consultants and York-Med employees are required to sign.

SSH informed us that iW Technologies does not have "explicit access" to the personal health information of Chatham-Kent patients. We interviewed one iW Technologies employee who has been authorized by the physicians to access the SSH system. He stated that he can only access the Vividesk application, not the York-Med clinical management system (Purkinje), which means he does not have access to the personal health information of patients. Although Vividesk has a single sign-in capability that enables an individual to use only one username and password to access both Vividesk and any other programs within the portal, such as the clinical management system, this function has not yet been activated.

Currently, the Vividesk program supplied by iW Technologies has only been installed for Dr. Gamble's use. SSH informed us that Dr. Gamble provided his SSH login credentials (i.e., his username and password for accessing the SSH environment) to iW Technologies in November to facilitate the setup and installation of the Vividesk program. However, iW Technologies did not have access to Dr. Gamble's separate user credentials for the clinical management system, required for accessing actual health data. Therefore, the company could not access the personal health information of any of his patients.

We appreciate that iW Technologies acted in a professional manner in installing the Vividesk program and could not access the personal health information of Dr. Gamble's patients. However, we would discourage the use of a physician's SSH login credentials for software installation purposes. In the case of an unscrupulous insider, access to such login credentials would provide the opportunity to gain a measure of access to the SSH environment. Such unauthorized access would be difficult to detect because the insider would essentially be impersonating the physician when logging on to the system.

Recommendation:

4. SSH should work with iW Technologies to develop a system for installing Vividesk in the remaining Chatham-Kent physicians' offices that does not involve requiring physicians to provide their SSH login credentials.

Physicians' Staff

Some of the staff in the offices of the Chatham-Kent physicians, such as registered nurses and secretaries, are also given access to SSH services, including the clinical management system databases that are housed on the server at SSH. The physicians sign "Physician Authorization Forms" that give specific staff in their offices access to these services.

Each staff member who has been authorized to access the SSH system must sign a "User Authorization Agreement." This agreement contains the same obligations as the agreements that the SSH consultants, York-Med employees, and iW Technologies employees are required to sign.

During our visit to Chatham-Kent, one of Dr. Gamble's assistants gave us a demonstration of the clinical management system. Our impression was that she was highly skilled at using the system and clearly understood the importance of protecting the personal health information of Dr. Gamble's patients.

Other SSH Measures

SSH has undertaken a number of other measures to protect the personal health information of Chatham-Kent patients from inside attacks, including:

- Physical Security — As noted in Issue A of this report, SSH protects the data centre housing the servers with a high degree of physical security. Although this level of physical security deters outsiders from entering the room where the servers are located, it also acts as a bar to unauthorized insiders (e.g., SSH consultants who are not authorized to enter the data centre).

- Logging Procedures and Audit Trails — SSH has implemented comprehensive logging procedures and audit trails to track both authorized and unauthorized attempts to access the SSH infrastructure, such as the server. Specifically, SSH has put in place firewall logging, intrusion-detection logging, VPN logging, VPN user authentication logging, and Windows 2000 logging. These logging procedures record accesses to the SSH system by SSH consultants, York-Med employees, iW Technologies employees and Chatham-Kent physicians and their staff.

Vulnerability Tests

As noted in Issue A of this report, SSH asked an independent third party to conduct an Internet penetration test and a simulated doctor's office test before the Chatham-Kent project went live. The purpose of these tests was to detect any weaknesses that could be exploited by outsiders. However, it appears that SSH has not conducted any internal vulnerability tests to determine whether the SSH environment and the physicians' offices could be exploited by insiders.

Recommendation:

5. SSH should engage an independent third party to conduct vulnerability tests on both the SSH environment and the physicians' offices that simulate an insider's attempts to gain unauthorized access to the personal health information of Chatham-Kent patients.

Key Fobs/Biometrics

We commend SSH for including a physical token ("key fob") in the user-authentication process because it adds an extra layer of security. Even if an unauthorized individual were able to somehow obtain an authorized user's username and password, he or she could not access the SSH system without that user's key fob.

However, key fobs have their own set of vulnerabilities. For example, they can be easily lost or misplaced because of their small size. In addition, key fobs are portable. This means that the physicians and their staff could easily share their usernames, passwords and key fobs, which increases the risk of an "impersonated" inside attack that would be difficult to detect.

One possible alternative is to supplement the username and password authentication process with a biometric device. A biometric is a unique physiological characteristic or trait of a human being used for automatically recognizing or verifying identity. In this case, the biometric would be used on a one-to-one basis to verify a user's identity. Examples of biometric technology include finger scanning, iris recognition, retinal scanning, hand geometry, face recognition, voice recognition and signature recognition.

One advantage of a biometric is that it cannot be lost and is less likely to be shared to gain access to a system. However, it should be noted that the use of biometric technology itself raises unique privacy considerations and should be approached carefully.

In fact, we understand that SSH is considering using biometric technology to tighten access to its data centre, where the servers are kept. We believe that government institutions should put in place specific procedural and technical privacy safeguards before implementing any form of biometric technology. For example, in 1997, the City of Toronto was considering the introduction of a one-to-many biometric measure in its efforts to control welfare fraud. The IPC worked with both the City and the Ministry of Community and Social Services to develop a legislative framework that would define the necessary privacy safeguards.

Recommendation:

6. SSH should consider implementing a supplementary user-authentication method, such as a one-to-one biometric, that cannot be lost or shared. However, it should consult with our office before introducing such a technology to ensure that adequate privacy protections are put in place.

Privacy-Enhancing Technologies

As noted in Issue A of this report, PETs such as strong encryption can play an important role in preventing electronic patient records from being viewed by outside attackers. We would also encourage SSH to examine the feasibility of using PETs to protect personal health information from inside attacks. For example, encrypting the clinical management system databases that are stored on the server at SSH would prevent unauthorized insiders from viewing the personal health information of patients.

It may also be possible to employ other forms of encryption that would allow SSH consultants or private companies to perform system maintenance and backup work, but not allow them to view the personal health information of patients that is stored on the system. We are aware of at least one product that encrypts relationships between the data elements in a database. The creators of this "encrypted relational database" claim that the product allows systems and database administrators to perform data administration tasks, but does not allow them to view personal information. In addition, authorized users, such as physicians, can continue to access personal health information in unencrypted form. Our intention here is not to endorse a particular product but to draw attention to the fact that there are potential solutions available that profess to allow systems administrators to perform maintenance or backup work without seeing the actual personal health information of patients.

Recommendation:

7. Before the use of information technology is expanded to other FHNs in Ontario, SSH should examine the feasibility of implementing further privacy-enhancing technologies, such as encrypted relational databases, that would prevent systems administrators and other insiders from viewing the personal health information of patients in the course of doing their work.

Issue B: Conclusion and Recommendations

In our view, SSH is taking adequate steps overall to protect the personal health information of Chatham-Kent patients from inside attacks. However, we would make the following recommendations:

4. SSH should work with iW Technologies to develop a system for installing Vividesk in the remaining Chatham-Kent physicians' offices that does not involve requiring physicians to provide their SSH login credentials.

5. SSH should engage an independent third party to conduct internal vulnerability tests on both the SSH environment and the physicians' offices that simulate an insider's attempts to gain unauthorized access to the personal health information of Chatham-Kent patients.

6. SSH should consider implementing a supplementary user-authentication method, such as a one-to-one biometric, that cannot be lost or shared. However, it should consult with our office before introducing such a technology to ensure that adequate privacy protections are put in place.

7. Before the use of information technology is expanded to other FHNs in Ontario, SSH should examine the feasibility of implementing further privacy-enhancing technologies, such as encrypted relational databases, that would prevent systems administrators and other insiders from viewing the personal health information of patients in the course of doing their work.

Issue C: Did a computer technician take three backup tapes home that contained the personal health information of patients? Were these backup tapes lost?

One of the allegations in the *Globe* article was that a computer technician took unencrypted backup tapes, containing thousands of medical records, to his home for several nights. The article also reported the allegation that three of the tapes were lost.

On December 13, 2001, we received a letter from SSH that contained the following statement: "With respect to the allegation that three tapes containing health records were lost, we confirm that no tapes have been lost and that all backup tapes for the ePhysician pilot systems in Chatham-Kent are fully accounted for."

The purpose of creating and storing backup tapes off-site is to ensure that the data and software on the servers at SSH are not irretrievably lost in the event of a physical disaster, such as a fire. The SSH data centre lead is responsible for ensuring that backup tapes containing data and software from the SSH system are adequately protected.

SSH informed us that when the Chatham-Kent project went live on November 1, 2001, it was still negotiating a contract with Iron Mountain, a private company that provides secure off-site storage for data and software.

The first full backup tape contained data and software that was stored on the SSH system on October 31, 2001. The second backup tape contained data and software that was stored on the SSH system on November 1, 2001.

The absence of a final contract between SSH and Iron Mountain at that time put the data centre lead in a difficult position when Chatham-Kent project went live on November 1, 2001. Although he was responsible for ensuring that backup tapes were stored in a secure off-site location, no such site was yet available.

Consequently, he discussed the matter with his manager, the SSH infrastructure services lead. They decided that the best option was to temporarily store the tapes at the data centre lead's home, which is not an unknown practice. In our view, this was a reasonable course of action given the circumstances.

During the course of our review, we asked to see the SSH sign-in and sign-out log for the tapes. The log shows that the October 31 tape was signed out by the data centre lead on November 1, 2001 and returned on November 7, 2001. The November 1 tape was signed out on November 2, 2001 and returned on November 7, 2001.

We cannot find any evidence to suggest that the tapes contained "thousands of medical records," or that three tapes were lost. According to SSH, the October 31 tape only contained application and system software data. It did not contain any personal health information because the Chatham-Kent pilot project had not yet gone live.

On November 1, 2001, the Chatham-Kent physicians and their staff were provided with a training session. In our interviews with Dr. Gamble and Dr. MacLean, they advised us that only a small amount of patient information would have been entered on the system during the training sessions. According to SSH, "the amount of clinical data would be very minimal, if there was actually any data at all. There were not thousands of medical records on the system."

SSH has provided us with a copy of the Data Storage and Service Agreement with Iron Mountain. The agreement was signed by the SSH chief executive lead on November 1, 2001. Although an Iron Mountain vice-president did not sign the agreement until November 29, 2001, the parties had agreed in an earlier exchange of correspondence that Iron Mountain would begin to provide its services on November 8, 2001.

The first backup tapes were picked up and stored by Iron Mountain at a secure off-site facility on November 9, 2001. However, SSH did not start to encrypt backup tapes until the week of December 16, 2001.

Iron Mountain provided us with a written submission that says, "Iron Mountain employees cannot decrypt the tapes stored and cannot see any personal information of patients on the tapes. The vault does not have equipment to read any tapes stored, as it is only a storage facility." Iron Mountain employees must also sign an employee contract annually that includes privacy and confidentiality clauses.

The agreement between SSH and Iron Mountain contains "Standard Terms and Conditions" that require the company to "use the same degree of care to safeguard the Confidential Information of Customer as it uses to safeguard its own confidential information." In our view, however, there are two clauses that should be added to the agreement.

The agreement should give SSH the right to audit or have a third-party audit conducted on Iron Mountain's privacy policies and data storage practices as they relate to the storage of SSH backup tapes. Similarly, it should clearly stipulate that the backup tapes must be immediately returned to SSH in the event Iron Mountain goes bankrupt or is dissolved as a corporation. Clauses such as these would ensure that SSH maintains considerable control over the backup tapes.

Issue C: Conclusion and Recommendations

Based on the information provided to us by SSH, we have concluded that the SSH data centre lead took home two unencrypted backup tapes for October 31 and November 1, 2001. In our view, this was a reasonable course of action given the difficult situation he was facing. The November 1 tape may have contained a small amount of personal health information of Chatham-Kent patients. Both tapes were returned to SSH on November 7, 2001. There is no evidence to suggest any tapes were lost.

Recommendations:

8. When the use of information technology is expanded to other FHNs in Ontario, SSH should ensure that it concludes a final contract with an off-site storage provider at least seven days before each new pilot project goes live. In addition, all backup tapes should be encrypted starting on the first day that a project goes live.

9. SSH should seek to modify the agreement with Iron Mountain to include clauses that: (1) give SSH the right to audit or have a third-party audit conducted on Iron Mountain's privacy policies and data storage practices as they relate to the storage of SSH backup tapes; and (2) stipulate that the backup tapes must be immediately returned to SSH in the event Iron Mountain goes bankrupt or is otherwise dissolved as a corporation.

Issue D: Are patients being fully informed about what is happening with their personal health information?

The *Globe* article alleges that patients in Chatham-Kent were not fully informed about what happens to their personal health information. Although they were told that other doctors could see their files, most patients were not informed that their information is stored on a server in a government building in Toronto.

These allegations touch on the issues of notice and consent. According to the Project Charter for the Chatham-Kent IT Transition Pilot Project, "[e]ach physician will be responsible for informing their patients about the roles and responsibilities that the various parties in this IT project will play. In particular, the physician must obtain consent from the patient of the services provided by MOHLTC and SSH."

Dr. Gamble told us that he provides patients with a general description of the project, but he does not inform them that their personal health information may be stored on a server in a government building in Toronto. He stated that the Chatham-Kent physicians simply do not have enough time to orally inform each patient about the technical details of the project.

We can certainly sympathize with Dr. Gamble's position. On the day we visited Chatham-Kent, both his and Dr. MacLean's offices were overflowing with patients. It was clear that both doctors and their staff have extremely heavy workloads and make strenuous efforts to use their time efficiently when seeing patients. Although we did not have an opportunity to interview the other physicians participating in the project, we would assume that they are equally busy and also lack sufficient time to provide patients with a detailed oral description of the pilot project.

We do not believe that the Chatham-Kent physicians need to orally inform patients that their personal health information is being stored on a server in a government building in Toronto. From a privacy perspective, it is more important for patients to know about the safeguards that have been put in place to protect their personal health information rather than the precise location of the server.

In our view, the ePhysician Project should prepare signage, written materials, and a Web site posting that informs patients in plain language about:

- the benefits and risks associated with electronic patient records;
- the roles performed by the OFHN, the ePhysician Project, SSH, and the physicians;
- the technology used in the project;
- how the privacy of their personal health information is protected;
- who is accountable for protecting their personal health information; and
- an ePhysician Project/SSH contact name, address and phone number for additional information.

Once patients have access to this information, they can make an informed decision about whether they wish to participate in the project.

Issue D: Conclusion and Recommendations

Chatham-Kent patients receive general information about what is happening with their personal health information.

Recommendations:

10. The ePhysician Project should prepare a written sign or brochure that notifies Chatham-Kent patients that their doctor is participating in the IT transition pilot project. In the case of a sign, it should be posted in a clear location in each physician's office and direct the patients to the OFHN Web site for more information.

11. The ePhysician Project should prepare a patient information fact sheet on the Chatham-Kent IT transition pilot project. The fact sheet should be written in plain language and posted on the OFHN Web site. Hard copies of these fact sheets could also be made available in the physicians' offices in Chatham-Kent.

Issue E: Did the ePhysician Project and SSH conduct a privacy impact assessment on the Chatham-Kent project?

A privacy impact assessment (PIA) is one of the best tools available for assessing the privacy implications of proposed government programs. It is essentially an analytical framework that government organizations can use to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements.

Before the Chatham-Kent project went live, SSH conducted a "Design Level Privacy Impact Assessment" that focuses on the technology and services provided by SSH. We have reviewed this PIA and believe that it contains sound recommendations for mitigating privacy risks.

However, an end-to-end PIA that examines the roles of all of the parties involved in the project, including the physicians and their staff and the vendors (York-Med and iW Technologies), has not been conducted. In its PIA, SSH notes that the absence of an end-to-end PIA "exposes SSH to the threat that there may be privacy risks as yet unidentified and/or unmitigated in connection with the project." Consequently, it makes the following recommendations:

- SSH must determine the status of the other parties' PIAs at the earliest opportunity;
- SSH ought to work with the other parties involved to develop an end-to-end PIA.

During the course of our review, we found that none of the parties believed that they were responsible for taking the lead in organizing an end-to-end PIA. Consequently, little progress has been made on this front.

According to the ePhysician Project and SSH, the main barrier to conducting an end-to-end PIA is jurisdiction. They advised us that, "[w]hile the Ministry, OFHN and SSH agree with the merits and value of an end-to-end PIA, none of the organizations have jurisdiction over the privacy practices in a physician's office, which would be part of a PIA and the place where most privacy issues must be addressed."

In our view, an end-to-end PIA should be based on fair information practices. However, we would emphasize that the component of the PIA that involves the Chatham-Kent physicians should focus exclusively on privacy practices as they relate to the IT Transition Pilot Project. The ePhysician Project and SSH should negotiate the parameters of an end-to-end PIA with the Chatham-Kent physicians and may also wish to obtain the input of the College of Physicians and Surgeons of Ontario (the self-regulating body for Ontario's medical profession).

Issue E: Conclusion and Recommendation

Although SSH conducted a limited PIA on the Chatham-Kent pilot project, a full end-to-end PIA on the entire project has yet to be conducted.

Recommendation:

12. The ePhysician Project and SSH should work together to conduct an end-to-end PIA on the Chatham-Kent pilot project based on fair information practices. (See Appendix A of this report.) The component of the PIA that involves the Chatham-Kent physicians should focus exclusively on privacy practices as they relate to the IT Transition Pilot Project. The ePhysician Project and SSH should negotiate the parameters of this PIA with the Chatham-Kent physicians and may also wish to obtain the input of the College of Physicians and Surgeons of Ontario (the self-regulating body for Ontario's medical profession).

Summary of Conclusions

Our review has reached the following conclusions, which are subject to the recommendations set out below:

1. SSH is taking adequate steps overall to protect the personal health information of Chatham-Kent patients from outside attacks. (But see Recommendations 1, 2 and 3.)

2. SSH is taking adequate steps overall to protect the personal health information of Chatham-Kent patients from inside attacks. (But see Recommendations 4, 5, 6 and 7.)

3. The SSH data centre lead took home two unencrypted backup tapes for October 31 and November 1, 2001. In our view, this was a reasonable course of action given the difficult situation that he was facing. The November 1 tape may have contained a small amount of personal health information of Chatham-Kent patients. Both tapes were returned to SSH on November 7, 2001. There is no evidence to suggest any tapes were lost. (But see Recommendations 8 and 9.)

4. Chatham-Kent patients receive general information about what is happening with their personal health information. (See Recommendations 10 and 11.)

5. Although SSH conducted a limited privacy impact assessment (PIA) on the Chatham-Kent pilot project, a full end-to-end PIA on the entire project has yet to be conducted. (See Recommendation 12.)

Summary of Recommendations

1. SSH should consider undertaking an end-to-end security test of the entire network.

2. For future pilot projects, SSH should conduct vulnerability tests and a network review at least 14 days before a project goes live. This will ensure that SSH has sufficient time to remedy any vulnerabilities that may be identified.

3. Before the use of information technology is expanded to other FHNs in Ontario, the ePhysician Project and SSH should:

    a) revisit the feasibility of encrypting any clinical management system databases stored on the server at SSH; and

    b) examine the feasibility of implementing further privacy-enhancing technologies, such as pseudonymizing tools, to prevent outside attackers from linking personal health information to an identifiable individual.

4. SSH should work with iW Technologies to develop a system for installing Vividesk in the remaining Chatham-Kent physicians' offices that does not involve requiring physicians to provide their SSH login credentials.

5. SSH should engage an independent third party to conduct internal vulnerability tests on both the SSH environment and the physicians' offices that simulate an insider's attempts to gain unauthorized access to the personal health information of Chatham-Kent patients.

6. SSH should consider implementing a supplementary user-authentication method, such as a one-to-one biometric, that cannot be lost or shared. However, it should consult with our office before introducing such a technology to ensure that adequate privacy protections are put in place.

7. Before the use of information technology is expanded to other FHNs in Ontario, SSH should examine the feasibility of implementing further privacy-enhancing technologies, such as encrypted relational databases, that would prevent systems administrators and other insiders from viewing the personal health information of patients in the course of doing their work.

8. When the use of information technology is expanded to other FHNs in Ontario, SSH should ensure that it concludes a final contract with an off-site storage provider at least seven days before each new pilot project goes live. In addition, all backup tapes should be encrypted starting on the first day that a project goes live.

9. SSH should seek to modify the agreement with Iron Mountain to include clauses that: (1) give SSH the right to audit or have a third-party audit conducted on Iron Mountain's privacy policies and data storage practices as they relate to the storage of SSH backup tapes; and (2) stipulate that the backup tapes must be immediately returned to SSH in the event Iron Mountain goes bankrupt or is otherwise dissolved as a corporation.

10. The ePhysician Project should prepare a written sign or brochure that notifies Chatham-Kent patients that their doctor is participating in the IT transition pilot project. In the case of a sign, it should be posted in a clear location in each physician's office and direct the patients to the OFHN Web site for more information.

11. The ePhysician Project should prepare a patient information fact sheet on the Chatham-Kent IT transition pilot project. The fact sheet should be written in plain language and posted on the OFHN Web site. Hard copies of these fact sheets could also be made available in the physicians' offices in Chatham-Kent.

12. The ePhysician Project and SSH should work together to conduct an end-to-end PIA on the Chatham-Kent pilot project based on fair information practices. (See Appendix A of this report.) The component of the PIA that involves the Chatham-Kent physicians should focus exclusively on privacy practices as they relate to the IT Transition Pilot Project. The ePhysician Project and SSH should negotiate the parameters of this PIA with the Chatham-Kent physicians and may also wish to obtain the input of the College of Physicians and Surgeons of Ontario (the self-regulating body for Ontario's medical profession).

Ann Cavoukian, Ph.D.
Commissioner

April 22, 2002
Date

Appendix A — CSA Model Code for the Protection of Personal Information

1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

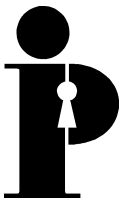
An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designate individual or individuals accountable for the organization's compliance.



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A9

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca