



**Information and Privacy  
Commissioner/Ontario**

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

---

---

## **INVESTIGATION REPORT**

### **PHIPA REPORT HI06-45**

#### **Initiate Systems Inc. and the Ontario Ministry of Health and Long-Term Care**

---

---

August 25, 2006

# **The Use of the Enterprise Master Person Index Software of Initiate Systems Inc. by the Ontario Ministry of Health and Long-Term Care**

## **INTRODUCTION**

### **Background of the Investigation**

The *Personal Health Information Protection Act* (PHIPA) was enacted in November 2004 to establish rules for the collection, use and disclosure of personal health information in order to protect the confidentiality of that information and the privacy of individuals with respect to that information. PHIPA designates the Office of the Information and Privacy Commissioner of Ontario (IPC) as the body responsible for overseeing compliance with the provisions of PHIPA.

On the afternoon of Friday, August 11, 2006, the IPC was alerted to an article appearing that day in the publication "Government Health IT" with the headline "Privacy Advocates Concerned about CIA Investment in e-health Firm." In the article, privacy advocates expressed concerns that In-Q-Tel, the venture capital arm of the Central Intelligence Agency (CIA), may gain access to the personal health information of Canadians due to their March 2006 investment in the software company, Initiate Systems Inc. (Initiate Systems).

Canada Health Infoway, a federally funded non-profit corporation that leads electronic health initiatives in Canada, signed an agreement in 2004 which sets out a framework for provinces to acquire the enterprise master person index software of Initiate Systems, (the Initiate<sup>TM</sup> Software) for provincial electronic health applications, if they chose to do so.

The Initiate<sup>TM</sup> Software (Initiate Software) is used in Ontario and in other provinces, including British Columbia, Alberta, Saskatchewan, Manitoba, and Newfoundland and Labrador, to advance the integration of health services by enabling personal health information pertaining to an individual to be consistently linked across the health sector, to the correct individual. In the Government Health IT article, privacy advocates requested that the federal and provincial Privacy Commissioners investigate any potential access that the CIA may have to the records of personal health information as a result of In-Q-Tel's investment in Initiate Systems.

The Information and Privacy Commissioner for the Province of Ontario (the Commissioner) launched an investigation into the article's allegations to determine if personal health information is being collected, used or disclosed in contravention of PHIPA through the use of the Initiate Software in Ontario.

The investigation unfolded as follows:

- On August 14, 2006, the Commissioner had a telephone conversation about this matter with Richard Alvarez, President and CEO of Canada Health Infoway (CHI). During this telephone conversation, the Commissioner was advised of the technical merits of the Initiate Software in comparison to other software options that CHI had considered.

- On August 15, 2006, the Commissioner and her staff held a teleconference with Joan Roch, Chief Privacy Strategist for CHI. Ms. Roch has the responsibility for ensuring that privacy issues are being addressed by CHI in its development of electronic health record systems. During this teleconference, Ms. Roch provided an overview of the situation and background information from CHI's perspective and facilitated contact with Initiate Systems.
- On August 15, 2006, the Commissioner and her staff also held a teleconference with Initiate Systems concerning its role in Ontario's Enterprise Master Person Index (EMPI) and its relationship to In-Q-Tel. Initiate Systems advised that the EMPI is the only application for which the Initiate Software is being used in Ontario.
- On August 17, 2006, the Commissioner received details from Initiate Systems about its role in the EMPI and its relationship to In-Q-Tel.
- On August 18, 2006, the Commissioner and her staff held a teleconference with Cancer Care Ontario (CCO). CCO is the agent of the Ministry of Health and Long-Term Care (MOHLTC) designated to implement, operate and manage the EMPI. CCO provided the Commissioner with the confidentiality and privacy obligations which Initiate Systems agreed to meet in its Master Software License and Services Agreement (the agreement) with CCO and advised the Commissioner that the EMPI is the only application for which the Initiate Software is being used in Ontario.

Throughout the course of our investigation, we received full and complete cooperation from CHI, Initiate Systems, CCO, and the MOHLTC.

### **Findings of Fact**

- The EMPI is a directory of identifiers pertaining to individuals that have been assigned by one or more organizations in the health sector, including hospitals and the MOHLTC. The rationale for creating the EMPI is to ensure that personal health information for an individual in the custody and control of organizations in the health sector may be consistently linked to the correct individual. The long-term goal of the EMPI is to provide the cornerstone for an electronic record of personal health information in the Province of Ontario.
- The MOHLTC is the health information custodian with custody or control of the personal health information in the EMPI and is subject to the rules respecting the collection, use and disclosure of personal health information in PHIPA.
- The EMPI is being implemented, operated and managed by CCO as an "agent" of the MOHLTC as defined in section 2 of PHIPA.

- An “agent”, in relation to a health information custodian, is defined under section 2 of PHIPA as a person that, with the authorization of the health information custodian, acts for or on behalf of the health information custodian in respect of personal health information for the purposes of the health information custodian, and not the agent’s own purposes.
- CCO has signed a PHIPA Agent Agreement with the MOHLTC that sets out the terms and conditions for CCO’s collection, use, disclosure, retention and disposal of personal health information. This PHIPA Agent Agreement recognizes that CCO is responsible for its agents and that each of its agents must sign a privacy and confidentiality agreement which sets out the agent’s obligations for protecting personal health information.
- CCO is a “prescribed entity” under section 45(1) of PHIPA and therefore must collect, use and disclose personal health information in accordance with section 45 of PHIPA and section 18 of Regulation 329/04 to PHIPA. As a prescribed entity, CCO must have in place practices and procedures approved by the IPC to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. The IPC’s report on its review of CCO’s practices and procedures is located on the IPC’s website at: <http://www.ipc.on.ca/docs/ent-cco.pdf>.
- In April 2006, CCO completed a comprehensive Privacy Impact Assessment of the EMPI. A Privacy Impact Assessment is a tool designed to assist organizations in reviewing the impact that a proposed information system, technology or program may have on the privacy of individuals’ personal information.
- Hosting, access control and network services for the EMPI are being provided by Ontario Smart Systems for Health Agency (SSHA). SSHA was created by the Province of Ontario to provide a secure, integrated, province-wide information technology infrastructure allowing electronic communication among organizations in the health sector in Ontario.
- SSHA is an electronic provider of goods or services and a “health information network provider” under PHIPA and Regulation 329/04 to PHIPA and therefore is required to comply with the requirements in section 10 of PHIPA and section 6 of Regulation 329/04 to PHIPA.
- In 2005, Initiate Systems was selected in Ontario to provide the Initiate Software, for use in the EMPI and to provide services in relation to the EMPI including analysis, configuring, updating or resolving the Initiate Software, uploading personal health information to the EMPI and reviewing error logs generated by the EMPI in order to troubleshoot errors.

- The agreement between Initiate Systems and CCO states that when providing services relating to the EMPI, Initiate Systems is acting as an “agent” within the meaning of PHIPA for organizations in the health sector participating in the EMPI. These organizations in the health sector participating in the EMPI are all health information custodians within the meaning of section 3 of PHIPA. Therefore, the collection, use and disclosure of personal health information by the participating organizations is governed by PHIPA.
- As an “agent”, Initiate Systems is permitted to collect, use, disclose, retain or dispose of personal health information in accordance with section 17 of PHIPA only if the health information custodian is permitted or required to do so and only in the course of the duties of Initiate Systems.
- Section 6(1) of PHIPA states that the providing of personal health information between a health information custodian and an agent of the health information custodian is a “use” by the health information custodian, and not a “disclosure” by the person providing the information or a “collection” by the person to whom the information is provided. Accordingly, when personal health information is provided to Initiate Systems, this is considered to be a use of the personal health information by the participating health information custodians rather than a disclosure of personal health information to Initiate Systems or a collection of personal health information by Initiate Systems.
- According to information provided by Initiate Systems and on In-Q-Tel’s website, In-Q-Tel is a private, independent, not-for-profit venture capital group established by the CIA that invests in companies in order to help make innovative technology already available in the commercial market, available to the intelligence community. In-Q-Tel concentrates its investments in three broad commercial technology areas: software, infrastructure and physical and biological materials.
- In-Q-Tel invested in Initiate Systems in March 2006. This investment was made after Initiate Systems was selected to provide its software for the EMPI in 2005.
- In-Q-Tel does not have a member on the Board of Directors nor any decision-making power in Initiate Systems. In-Q-Tel’s ownership in Initiate Systems is less than 2 percent.

### **Issues Arising from the Investigation**

The following issues were identified as arising from this investigation:

- (A) Is the information contained in the EMPI “personal health information” as defined in section 4 of PHIPA?
- (B) Is the “personal health information” contained in the EMPI being provided to Initiate Systems in accordance with PHIPA?

- (C) Does the relationship between Initiate Systems and In-Q-Tel allow In-Q-Tel to access any personal health information contained in the EMPI?

## **RESULTS OF THE INVESTIGATION**

### **Issue A: Is the information contained in the EMPI “personal health information” as defined in section 4 of PHIPA?**

Section 4(1) of PHIPA states, in part, that “personal health information” means identifying information about an individual in oral or recorded form, if the information:

[...]

- (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,

[...]

- (f) is the individual’s health number.

[...]

Identifying information is defined in section 4(2) of PHIPA as information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be used, either alone or with other information, to identify an individual.

Although the EMPI does not contain information relating to the physical or mental health of individuals, including diagnosis, prognosis or any other clinical information, because the EMPI contains the name, gender and address of individuals as well as their health card numbers and other unique health identifiers assigned by health care providers, the information contained in the EMPI is “personal health information” as defined in section 4 of PHIPA.

### **Issue B: Is the personal health information contained in the EMPI being provided to Initiate Systems in accordance with PHIPA?**

Health information custodians generally collect personal health information, with the implied consent of individuals, for the purpose of providing health care. Under section 37(1) of PHIPA, health information custodians are permitted to use personal health information for the purpose for which it is collected and for all functions necessary for carrying out that purpose. In using personal health information, section 30(2) requires health information custodians to use no more personal health information than is reasonably necessary to meet the purpose. In accordance with section 17 of PHIPA, agents of health information custodians are only permitted to use personal health information if the health information custodian is permitted or required to do so and only in the course of the duties of the agent.

In addition to the above, section 12(1) of PHIPA requires health information custodians to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorised use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

The Commissioner has determined that the use of personal health information for the operation of the EMPI falls within the scope of the permitted uses of personal health information by health information custodians. Accordingly, health information custodians may authorize one or more of their agents to use personal health information for this purpose, on their behalf.

In its agreement with CCO, Initiate Systems acknowledges that in the course of providing services for the EMPI it is acting as an “agent” for the health information custodians that are participating in the EMPI. Initiate Systems also acknowledges that it is being provided with personal health information contained in the EMPI to configure, update or resolve the Initiate Software, to upload personal health information into the EMPI, and for troubleshooting errors. In addition, CCO has indicated that access by Initiate Systems is only required for the implementation phases of the EMPI. Once the EMPI is fully operating at all sites, technical support from Initiate Systems will no longer be required.

Personal health information is only provided to Initiate Systems under very limited, restricted and controlled conditions. Initiate Systems does not have any remote access to the personal health information contained in the EMPI and all services are provided, on-site, at locations within the Province of Ontario. Initiate Systems cannot remove personal health information from these locations or transmit personal health information outside of these locations.

Initiate Systems only provides services in respect of the EMPI at the following locations:

1. **SSHA data centre.** Initiate Systems must be physically present at the SSHA data centre to provide services. Initiate Systems staff are monitored by SSHA staff while they are in the data centre. The services provided at the SSHA data centre include configuring, updating and resolving the Initiate Software and uploading EMPI data extracts from organizations that participate in the EMPI.
2. **CCO’s offices.** The EMPI sends error logs which contain personal health information to a secure space on the SSHA network. The EMPI Office, operated and maintained by CCO, reviews the error logs through a secure virtual private network connection to the SSHA network. It is only when EMPI Office staff cannot troubleshoot an error that Initiate Systems is called for support. Staff of Initiate Systems must view the error logs at CCO’s premises and are monitored by EMPI Office staff. Initiate Systems’s access is limited to the secure folder which contains the error logs. The error logs are purged from the network every one to two days.

The security of the personal health information contained in the EMPI is strengthened because there is no “backdoor access” or “gated access” to the EMPI. Backdoor or gated access can be provided through the source code for certain applications. When present, backdoor or gated access to applications may undermine data defenses by allowing a limited window of opportunity to bypass the security features of the software and to gain access to the data.

In addition to the above safeguards, Initiate Systems staff must be granted access to the EMPI through the SSHA registration process. All access by staff of Initiate Systems must be approved and verified by CCO. Before granting access, CCO verifies that confidentiality agreements are in place. SSHA verifies the identity of the requestor and grants access accordingly. Currently, only two staff of Initiate Systems may access personal health information in the EMPI on-site, for the purposes of configuring and updating the Initiate Software.

Additional provisions have been included in CCO’s agreement with Initiate Systems to protect the confidentiality of the personal health information contained in the EMPI and the privacy of individuals whose personal health information is contained in the EMPI. These measures include:

- Requiring Initiate Systems to keep personal health information confidential;
- Prohibiting Initiate Systems from using personal health information other than in connection with the performance of services in accordance with the agreement;
- Prohibiting Initiate Systems from divulging personal health information to its personnel or advisors unless the personnel or advisors have a need to know, have undertaken an oath of secrecy and agreed in writing to keep the personal health information confidential;
- Prohibiting Initiate Systems from disclosing personal health information except in response to an order by a Canadian court or Canadian government body or as required by Canadian law;
- Prohibiting Initiate Systems from disclosing any personal health information outside Ontario without the prior written consent of the health information custodians participating in the EMPI;
- Requiring personal health information to be stored within Ontario in a secure manner;
- Requiring Initiate Systems to provide all services within Ontario;
- Requiring Initiate Systems to comply with all Canadian laws including PHIPA;
- Prohibiting Initiate Systems from disclosing personal health information to any party (other than Initiate Systems Canada), without the prior written consent of the health information custodians participating in the EMPI;



- Requiring Initiate Systems to notify the health information custodians participating in the EMPI and CCO of any practice or procedure in which it is engaged that contravenes applicable privacy laws and of any complaint about the theft, loss, destruction or unauthorized access, disclosure, copying, use or modification of personal health information; and
- Permitting the health information custodians participating in the EMPI to conduct audits and to monitor compliance of Initiate Systems with the contractual agreement for the EMPI.

Based on this information, the Commissioner has determined that personal health information contained in the EMPI is being provided to Initiate Systems in accordance with PHIPA.

**Issue C: Does the relationship between Initiate Systems and In-Q-Tel allow In-Q-Tel to access personal health information contained in the EMPI?**

Initiate Systems does not have any remote access to the personal health information contained in the EMPI. All the services provided by Initiate Systems in respect of the EMPI are being provided on-site, at locations within the Province of Ontario, namely the SSHA data centre and the offices of CCO. Personal health information does not flow outside of Ontario.

Further, Initiate Systems confirmed that there is no mechanism in their investment agreement with In-Q-Tel that would allow In-Q-Tel to access any personal health information contained in the EMPI. The same applies to all agreements that Initiate Systems has in place with other investors. Consequently, In-Q-Tel has no access to any personal health information contained in the EMPI.

**SUMMARY OF CONCLUSIONS**

Our investigation has concluded that:

- (A) The information contained in the EMPI is “personal health information” as defined in section 4 of PHIPA.
- (B) In the course of providing services for the EMPI, Initiate Systems is acting as an “agent” within the meaning of PHIPA for the health information custodians participating in the EMPI.
- (C) The provision of personal health information to Initiate Systems is a use by the health information custodians participating in the EMPI and not a disclosure of personal health information to Initiate Systems, or a collection of personal health information by Initiate Systems.

- (D) Personal health information is provided to Initiate Systems under very controlled and limited conditions.
- (E) The relationship between Initiate Systems and In-Q-Tel does not allow In-Q-Tel to access any personal health information contained in the EMPI.

In investigating the concerns raised by privacy advocates in the Government Health IT article, the Commissioner has determined that reasonable steps have been taken to ensure that the personal health information of Ontarians is not accessed by In-Q-Tel as a result of its relationship to Initiate Systems.

Initiate Systems is only provided personal health information under very restricted conditions and for narrowly defined technical support purposes. Initiate Systems is only able to view personal health information under direct supervision at the offices of CCO and SSHA in Ontario and is not able to view the personal health information remotely. Further, there is no “backdoor” or “gated” access to personal health information in the EMPI. Finally, the relationship between Initiate Systems and In-Q-Tel does not allow In-Q-Tel to access any personal health information contained in the EMPI.

Accordingly, the Commissioner has determined that personal health information is not being collected, used, or disclosed in contravention of PHIPA through the use of Initiate Software in Ontario, nor does any health information leave the province.

**RECOMMENDATIONS**

- (1) The Commissioner should be consulted concerning any proposed amendments or changes to the confidentiality or privacy obligations contained in the agreement between CCO and Initiate Systems.
- (2) The MOHLTC or any other person who operates the EMPI in the future should advise the Commissioner if there is a breach of the confidentiality or privacy obligations of the agreement by Initiate Systems, and the steps taken to mitigate the breach, the measures taken to prevent subsequent breaches, and the manner and nature of the notification provided to individuals whose personal health information is contained in the EMPI.
- (3) The MOHLTC or any other person who operates the EMPI in the future using the Initiate Software should advise the Commissioner when changes will be made to the source code for the Initiate Software, as well as the nature and rationale for these changes.

Original signed by: \_\_\_\_\_  
 Ann Cavoukian, Ph.D.  
 Commissioner

\_\_\_\_\_  
 Date