



How the Rimouski smart health card pilot project in Quebec protected privacy

The 70,000 people of Rimouski, on the St Lawrence River, 300 kilometres east of Québec City, have been pioneers in a two year health smart card project which is evaluated here by its joint chairman, Paul-André Comeau, Chairman of the Commission D'Acces à l'Information du Québec.

Under a programme called *Concerted Action - Eurocards*, headed by Professor Yves Pouillet of the University of Namur and Paul-André Comeau, Québec Privacy Commissioner, the European Commission set up an in-depth study of the sociological conditions and legal questions to be taken into account when setting up a pilot project or going ahead with full-scale implementation of smart card technology.

The pilot project in Rimouski ended in March 1995 and the experiment lasted exactly 2 years. Altogether the experiment and its preliminary stages extended over more than 5 years. Currently, although the experiment is over, the card is still widely used in this community.

The Québec Health Insurance Board launched this project and provided the financial resources for a joint team from the Social and Preventative Medicine Department of Laval University, Québec City and the Community Health Centre, in Rimouski. The project was authorised by the Québec Government late in 1989. At the same time, the Québec Information and Privacy Commissioner was called on to assess privacy.

The objective of the project was, among other things, to improve communications between health professionals and patients in order to promote more efficient services. With the patient's medical record on the chip, the GP could ask more relevant questions and spend more time looking at the problems of the patient.

How the project was conducted

Four target groups were selected:

1. people over 60 years of age
2. pregnant women
3. infants from birth to eighteen months of age

4. and the entire population of a small nearby village which acted as a control group.

At the end of the project, a little less than 7,500 cards had been issued, mostly to elderly people in Rimouski. It is interesting to note that more than 70% of the population of the control village volunteered for the experiment. In this group, as well as in Rimouski itself, card holders joined the project on a voluntary basis.

Enrolment was entirely up to the patient, and the patient was also free to use his card or not when visiting his GP or going to the local hospital. He was also allowed to refuse to have data entered on his portable file.

About 100 health professionals also volunteered for the project. Most of them were GP's, Specialists, pharmacists, nurses and ambulance operators also took an active part.

Patients could use their cards at the local hospital, mainly in the emergency ward, local drugstores, private GP offices and local health care centres.

How the card worked

The card used for the project proved quite adequate. It had a capacity of 6 kilobytes. In plain language, there was enough space on the chip to hold more than 8 full pages of typed text. At the end of the experiment, not a single card had been filled to capacity. With the new cards available on the market, there does not seem to be any problem as far as capacity is concerned.

The smart card, or more precisely its chip, was divided into five independent parts or fields. These fields were designed with one very specific goal: to grant special access rights to each group of health professionals.

The chip contained the following fields:

- *Administrative or ID field*: essential data e.g. name, date of birth, health insurance number, and other standard administrative data
- *Emergency field*: all the information required in the first few minutes of an emergency e.g. blood group, allergies, intolerance to drugs, visual or hearing aids etc.
- *Vaccination field*: list of all vaccinations received by the patient
- *Medication field*: patient's drug profile e.g. prescription drugs taken regularly etc.



- *Medical care field*: clinical information from consultations, hospitalisation, personal and family history. This field is a resumé, not a complete medical record.

One important fact has to be explicit: because of the nature of the information in each of these fields, this card must be considered as a check list, not a complete medical record.

The card was filled at first with information taken from the patient's hospital medical record or from the GP's own data bank. If lost or stolen, a new card had to be issued, because there was no central data bank or back-up system. Fortunately, just a few cards were lost during the experiment.

Integration into an information system

The patient's card was integrated into a larger information system. This system was given an added value which proved to be both useful and interesting for GP's because it included decision-making or expert systems such as a drug advisor.

The pilot project proved successful. When it ended, more than 15 months ago, a notice was circulated in Rimouski, explaining why the card is still used by the elderly. But no new card has been issued and no replacement card can be provided, when lost or stolen.

The privacy assessment

The Québec Information and Privacy Commission was invited by the government, at the very early stages of the experiment, to submit its recommendations and, eventually, its conclusions.

After thorough analysis of the experiment, the Commission gave its approval. The guidelines for the project were as follows:

1. The Commission considered it essential that *card holders' basic rights be maintained*, including the right to the confidentiality of personal information.
2. There was general agreement on *voluntary participation in the experiment*. This principle requires that users be allowed to ask for a health smart card. It was also entirely up to the patient to decide whether or not he wanted to give his card to a health professional and whether or not he wanted certain information entered on it.
3. The Commission was satisfied with the assurances given by the promoters

respecting the *rights of access and correction recognised in our Privacy Act*. The patient could either view the information on a screen or get a print-out from the health professional or the health card office. If data on the card was inaccurate or the patient felt that it was not true, he could apply to get it corrected. Only the physician who entered the data in the medical care field was allowed to correct it.

4. There was a broad consensus on the *principle of confidentiality and security of information*. The right to privacy means that only persons authorised by law can have access to information entered on the card.

Our independent and, at times, parallel assessment of the project was based on these principles or guidelines. In order to make the assessment as foolproof as possible, we reviewed most of the literature in the field and maintained close contact with research teams in Europe interested in the same questions.

Opinion surveys conducted

We also commissioned an opinion poll at the very beginning of the experiment. The survey included most of the population of the control group. When the project was almost over, we asked the same private company to organise five focus group sessions in Rimouski, Québec City and Montreal. Of course, we were very attentive to the ups and downs of the experiment and we also conducted some in-depth interviews at various stages of the project.

Majority considered health card secure

75% of the survey respondents considered that the process established by the card management was *secure and confidential*. Eight people out of ten felt that the access procedure for health care professionals guaranteed sufficient protection of privacy. The information entered in each of the fields of the health card was perceived as secure by 7 out of 10 people, and a larger proportion, 84%, felt that the card would not jeopardise their privacy. To sum up this point, the issue of confidentiality did not seem to raise much concern.

Also, the principle of *voluntary participation* should be maintained. The decision to hold and use



the card, and to have sensitive data entered on the card should be left to the individual.

It was no surprise that health professionals felt that the smart card offered a real guarantee of confidentiality and could even represent an *improvement over paper records*. On the other hand, health care professionals expressed *doubts about the possibility of maintaining the principle of voluntary participation*.

Checking the privacy principles

As far as privacy and principles related to privacy are concerned, we checked the most important points or issues extensively:

- The *quality of the consent* given by the card holders at various stages, such as their free acceptance of the card and its use at the hospital, the drugstore or the GP's office;
- The *confidentiality of the data*;
- the *security of the information entered on the card*, which is important because of the sensitive nature of the data;
- the *disclosure of valid information*, which was strictly limited to the health professional directly involved with the patient's care. Only the GP was allowed to read the entire card; access by the hospital administrative staff was strictly limited e.g. to the ID field of the card;
- *No wrongful disclosure of information* to other people, like employers, insurers or police was reported. The holder's right to access and correct the data could be complied with easily. The access to information is increased when the computer screen is positioned so that both the health professional and the patient can read the information at the same time. This form of access to the information on the card makes the patient realise that he really is the primary person concerned by it. It can even promote a better dialogue between him and the health professional;
- The Québec Information and Privacy Commission, which acted as a watchdog, did not receive a single complaint during the two years the experiment lasted.

Privacy laws help consumer acceptance

I am deeply convinced that health smart card projects can be carried out smoothly while respecting the imperative provisions of most

privacy laws. Far from being an impediment to the introduction of this technology, these laws ensure that there is a safety net, which makes easier the acceptance of the card by its users.

The Rimouski project proved it was possible to introduce health smart cards while respecting privacy, and also to use the technology as a powerful tool for protecting personal information.

Given that the user is the sole holder of the card and that he controls its use and the circulation of the information on it, the patient sees his personal information protected in a way that cannot be achieved with a standard paper file.

One of the less obvious conclusions of this experiment concerns the role of the Information and Privacy Commissioner. This kind of technological assessment has to be undertaken when we Commissioners give useful advice and make recommendations.

Smart cards - the way ahead

Finally, what of the future of smart card technology - not only for health care but in other fields? Right now, VISA, the world's leading credit card, is winding up a large-scale pilot project in Australia using the same technology. In the near future, our credit cards, at least from VISA and also Mastercard, will no longer bear the magnetic strip which has been a standard feature for years. Both VISA and Mastercard will use smart card technology in order to secure transactions on the Internet as well as other types of commercial or credit applications in cyberspace.

This paper is an edited version of a presentation by Paul-André Comeau, Chairman of the Commission D'Acces à l'Information du Québec at the Privacy Laws & Business 9th Annual Conference, Cambridge, July 1996.

Smart Cards: New Policy Frameworks

Conference: October 16th-17th, 1996

The Landmark Hotel,
222, Marylebone Road, London NW1 6JQ

For further information contact:
Katy Searles, IBC Technical Services Ltd,
Gillmoora House, 57-61 Mortimer Street,
London W1N 8JX, United Kingdom.

Tel: +44 (0) 171 453 2700

Fax: +44 (0) 171 636 1976