ERDM and the 10 Privacy Principles

Introduction

The cornerstones of the current Privacy Legislation in Canada and Ontario have been laid based on the dimensions of ten Privacy Principles in particular. These ten principles can be seen together in the Canadian Standard's Association's *CAN/CSA-Q830-96 Model Code for the Protection of Personal Information*, a voluntary-compliance document created in 1996. This document will refer to the code and its principles throughout.

In response to the issues of technology, information exchange and privacy, key Industry Leaders and Stakeholders were consulted as part of the Technical Committee on Privacy for the Standards Association. Included in source material for the code were the Freedom Of Information and Protection Of Privacy Act of Ontario of 1992, and federal The Privacy Act of 1983. The code has also been assimilated into Privacy legislation that has been enacted since 1996. Included in this recent legislation is Bill C-6 (Personal Information Protection of Privacy and Electronic Documents Act, PIPEDA), Ontario's pending legislation, the Protection of Personal Information Act, and the internal government policy paper the Electronic Service Delivery Privacy Standard, which is currently in force for provincial ministries.

Current legislation treats the private and public sectors differently. As Electronic Service Delivery moves forward, and the lines between publicly funded organizations and private, for-profit organizations blur (as becomes the case with the outsourcing of IT management responsibilities), it is important to retain the integrity of our ability to manage and maintain information in the public sphere. As personal, private, and confidential information is being increasingly stored in electronic format, there is a heightened need for strong standards that will address the individual areas of privacy, security and confidentiality.

These three areas are not independent of one another, but neither are they synonymous terms; privacy, security and confidentiality are all separate areas that must each have special attention paid to them in order to properly support Canada and Ontario's privacy legislation and its underlying democratic principles.

The ten Privacy Principles as detailed by the *CAN/CSA-Q830-96 Model Code for the Protection of Personal Information* are:

1. **Accountability**;
2. **Identifying Purposes**;
3. **Consent**;
4. **Limiting Collection**;
5. **Limiting Use, Disclosure and Retention**;

6. **Accuracy**;
7. **Safeguards**;
8. **Openness**;
9. **Individual Access**; and
10. **Challenging Compliance**.

The Encrypted Relational Database Model (ERDM) developed by Prescient addresses each one of these fundamental principles in its design, deployment and use.

1. Accountability

The ERDM is able to solve a difficult issue that is inherent in this principle. Sub Section 4.1.1 of the principle states, "Accountability for the organization's compliance rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information[1]"(section 4.1.1, p.2). However, in section 4.1.3, the Code states, "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing" (ibid).

The ability for a Head (the person within an organization who has ultimate responsibility for the adherence to the Code) to ensure that both of these guidelines are adhered to is difficult, particularly in the case where outsourcing provides the IT Service Management. In these cases, information may leave the host organization for the purposes of transaction back up or maintenance. This implies that people who have not sworn an oath to secrecy handle raw personal, private, and confidential material. Although section 4.1.3 goes on to clarify that any third-party who processes information should be bound by contractual or other means to provide a comparable level of protection of information, there is currently no real way to prevent aggregated information from falling into the wrong hands.

The ERDM is one of the only systems in the world that can, in this light, allow the outsourcing of IT management to be safe and secure. With the ERDM, third party IT service providers can process private, personal, and confidential information, but cannot access raw tombstone data identifying individuals. In this way, the ERDM bridges the gap between the need for governments and other large organizations to trust other service providers, but to still maintain control and accountability for the raw information as it resides in electronic form. This is a new development in the IT Industry, as previously, the common understanding was that for the purposes of service provision, access to all raw (and potentially identifying) private, personal and confidential, disaggregated information was required. Prescient has shown, with the ERDM, that this is not the case.

2. Identifying Purposes

The ERDM is not intended to include Business Process directives *per se* in its design. This means that for this principle, under which the purpose for collecting information must be identified upon the collection of that information, the ERDM does not have a design feature that will necessarily ensure this principle is met. This is largely due to the fact that this principle is predicated on a point-of-contact activity. The collector must identify to the person about whom they are collecting information why that information is being collected.

However, it is a design feature of the ERDM that only authorized access is granted to aggregate records (there will be more on access rights in Individual Access, section 9). Documentation of information collection can be easily achieved due to the tight auditing capability of the database model. No transaction takes place without an audit log being generated. This means that any discrepancies can be clearly identified and addressed on a case-by-case basis, a concern for a system where records are being kept in an electronic format, especially in one single, large database. It is possible with current database implementations that a Systems or Database Administrator could access information without having a log generated. With the ERDM, not only could a Systems or Database administrator not access information to which they had not been granted access, but any access of that information would be logged for auditing purposes.

The ERDM does address one of the clauses in Identifying Purposes principle (4.2.4) in a new way, however. It is possible that if an existing piece of information is to be used for another purpose (any purpose that was not stated at the time of original collection), a flag could be used to send an alert to affected parties (administrators, heads, subjects, etc.) notifying them of the new use.

This feature can also accommodate the issues of Limiting Collection and Consent.

3. Consent

{Note: There are certain legal and legislative conditions that are set upon this principle. Please refer to the Model Code for the Protection of Personal Information for clarification on those conditions.}

As the ERDM protects the relationships between tables within a database, there is no way that information about an individual (or, more accurately, an individual's information) can be sent in any useable form to another organization without the individual's explicit consent (again, please see the above caveat for clarification).

For the use of information, the purposes for which were not originally identified at the time of collection, the ERDM can be set to flag an alert for proper compliance action. Please see principle 2, Identifying Purposes.

The issue of forms relating to the reason for collection of information can also be addressed by the ERDM. In the case where there is a large organization (such as government) that must collect and retain information on an individual in several different program areas or ministries, it may be required that there are differing forms for the collection of private, personal, or confidential information. As, in this case, each ministry is actually a different legal entity, no one ministry is allowed to view the records of any other ministry (please refer to the Code for clarification on this point).

It is possible with the ERDM to separate both records and access to files stored in an electronic form. The forms for one ministry's collection may be kept separate from the forms of (for example) another ministry, as well as any information that each ministry keeps on an individual.

Access rights, as determined by legislation and legal requirements, control who has access to what information stored within an electronic format. Examples of access rights could be based on the rights of patient-physician confidentiality, or client-solicitor privilege.

As well, multiple forms could potentially be kept (in exclusion of one another) for multiple programs or services, without any one authorized user (e.g. physician, or program area) being able to see another's "paperwork." This holds particular importance for issues such as payment processing in an On Line format where multiple program area's transactions must be kept separate from one another, but for whom the authorized user must still be able to aggregate all pertinent information. Integrated and cross-jurisdictional, cross-ministry, -program area, and -organization Electronic Service Delivery will continue to drive this issue in the near future.

4. Limiting Collection

As with some of the other Privacy Principles (in particular, Identifying Purposes, and Consent), compliance and enforcement are predicated more on Business Rules and actual practices rather than on technology. Having said this, the ERDM is able to enhance some of those practices by granting specific and purposed rights-of-access, creating authorized and unauthorized categories of users.

User authorization is not, in and of itself new. The means by which information within the database is kept, however, is different with the ERDM than with other, more conventional security models. This means that where collection is concerned, the reason for collection can be clearly linked to the repository of information providing better knowledge management capability, while maintaining strict access rights for users.

5. Limiting Use, Disclosure, and Retention

In as much as Use, Retention and Disclosure falls under an administrative purview, the ERDM will not necessarily affect these duties one way or the other. However, in as much as Use, Retention, and Disclosure are Information Technology and Information Management issues, the ERDM is able to enhance the ability for IT administrators to complete tasks for which the Head would be responsible to Privacy Legislation.

The Freedom of Personal Information and Protection of Privacy Act (FIPPA) states that a Head of an organization is accountable for those records under his or her purview. This includes records of retention and destruction. By virtue of the way in which the ERDM is designed, each time records within the database are accessed an audit log is created. This means that records for not only access and management, but also destruction can be accurately kept.

Section 4.5.3 of the Model Code states that, "Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous" (section 4.5.3, p. 6). As anonymity of information within the ERDM is a default state, the concerns regarding the ability for a user to be positively identified are successfully allayed.

In addition, the clause states, "Organizations should develop guidelines and implement procedures to govern the destruction of personal information" (ibid). Again, this suggests more of a principle in practice instead of a design feature of a database, but the fact remains: the ability of the ERDM to log and audit access to records will prove invaluable to those responsible for implementing these principles.

The ERDM is also able to automate delete dates for records. If, in the case of document management, there is a requirement for a certain document or piece of information to be cleared from records after a certain amount of time has elapsed (for example, two years), the system could be programmed to flag and delete that document. It is also possible to have a level of human verification to approve the system's deletion of that piece of information, so that no piece stays on record when it isn't supposed to. This also works both ways: the system can delete records in accordance with stale dates, but can also prevent the early deletion of records that should be kept on file (this is sometimes referred to as grandfathering, or referential integrity).

As ESD moves forward, especially in the case of eHealth where there will be millions and millions of records, this type of automation is highly advantageous and assists the Head in complying with the Privacy directives. This feature can also apply to expiry dates on the sharing of data between organizations or across program areas (where such sharing is in compliance with legislation).

6. Accuracy

As with other principles, the ability of the ERDM to ensure accurate, complete, and up-to-date information is residing within it is the responsibility of a human operator, not of the ERDM itself. It is possible though, through the auditing and access controls of the ERDM, to verify the accuracy of kept records, access, and deletion. This is a great step towards database and electronic records accuracy.

7. Safeguards

"The Security Safeguards shall protect personal information against loss, or theft, as well as unauthorized access, disclosure, copying, use, or modification" (section 4.7.1, p.6). Currently, Systems and or Database Administrators grant access-to-information rights. By virtue of the fact that they are the ones who grant access, they are also in a position to access all raw, disaggregated information residing in the databases under their purview. This is a breach of privacy legislation and directives in as much as the information residing within an electronic database can be collected, used, stolen or sold by those very guardians. As well, any hacker, cracker, or malicious user can access that information and positively identify the individuals to whom the information relates.

The ERDM is able to mitigate both of these very palpable threats from actually happening, because only an authorized user will have access to raw, aggregate information about an individual. Only those users (such as doctors, in the case of electronic health) who have been given access can see the aggregate information identifying an individual. All other users see only parts of the information, based on their individual access rights.

The accountability of those who are responsible for safeguarding this information by law (senior managers, etc. who may not actually do the hands-on work of managing the electronic information) is strengthened by the ERDM's technology solution.

Furthermore, if a third party is inputting data (as might be the case for outsourced IT management), it is also possible to break up the data being input. This means that no single operator sees all the information in its entirety, preventing the positive identification of any one individual.

8. Openness

The principle of Openness is one to which the ERDM relates only indirectly. In as much as an organization is responsible for making readily available to individuals information about its specific policies and practices relating to the management of personal information, the ERDM can act as a one-stop-shop for the highest level of information security.

This principle is more a business directive than an Information Technology driver, but the ERDM can nonetheless support the key responsibilities of this directive.

9. Individual Access

{Note: There are certain legal and legislative conditions that are set upon this principle. Please refer to the Model Code for the Protection of Personal Information for clarification on those conditions.}

Under the Individual Access principle, the right for an individual to view the records of transactions of their information is clearly stated. The ERDM is able to keep accurate logs of who accessed what parts of which information, when. Due to the tight security inherent in the ERDM, individuals can, for the first time, be absolutely sure about where their information has gone. Previous IT solutions have only placed security as a layer added to the operating environment. The ERDM improves on this vulnerability by making security part of the operating environment, while enabling speed of access, enhanced privacy, and the assurance that confidentiality of records is held to the highest standard.

10. Challenging Compliance

The final principle is again, a principle that is largely a Business Practice rather than an IT-related directive.

The comprehensive structure of the ERDM makes compliance with the principle easier for whichever organization is being queried, of whom information is being requested, or who is being audited. By ensuring that a comprehensive solution exists for the management of all information within a database (in this case, one protected and secured by encrypting the relationships between tables within the database), those within an organization responsible for ensuring compliance can be assured that at least half of their job is done for them.

Synopsis

In the field of Information Technology, Information Management and Information Security, there exist a whole range of services that can address different aspects of the ten privacy principles as outlined in the *CAN/CSA-Q830-96 Model Code for the Protection of Personal Information*, the basic tenets of which have been adopted or are at least reflected in most of the current and binding legislation for Privacy. It is true that many products exist that can successfully address parts of the principles. The ERDM is different, in that it is able to incorporate the spirit of the code, and of existing legislation. That spirit is one that protects the rights and privileges of living in a democratic society, where a person can control the information relating to them and where the ability to do so is protected by law.

[1] Adragna, Maria, et al. CAN/CSA-Q830-96 Model Code for the Protection of Personal Information. Etobicoke: Canadian Standards Association, 1996.