



## The Case For Improved Security and Privacy In Relational Database Models ~ An Example in Health Care

When dealing with personal and confidential information in an electronic format, there exists, by default, access rights that are granted to Systems and Database Administrators. These rights are legitimate as they are required for the purposes of operations and management of systems. Under **FIPPA** (Freedom of Information and Protection of Privacy Act) and **MFIPPA** (Municipal Freedom of Information and Protection of Privacy Act) however, such Administrators should not have the right to view or access confidential personal information, which could then be used to identify an individual.

An area where privacy concerns are becoming increasingly paramount is the health industry. With the goal of providing patients better access to health care from anywhere they choose, to creating and maintaining thorough medical records, this industry is moving towards an Electronic Service Delivery Model. With this new model, sensitive patient information is exposed unless essential privacy and security issues are not addressed.

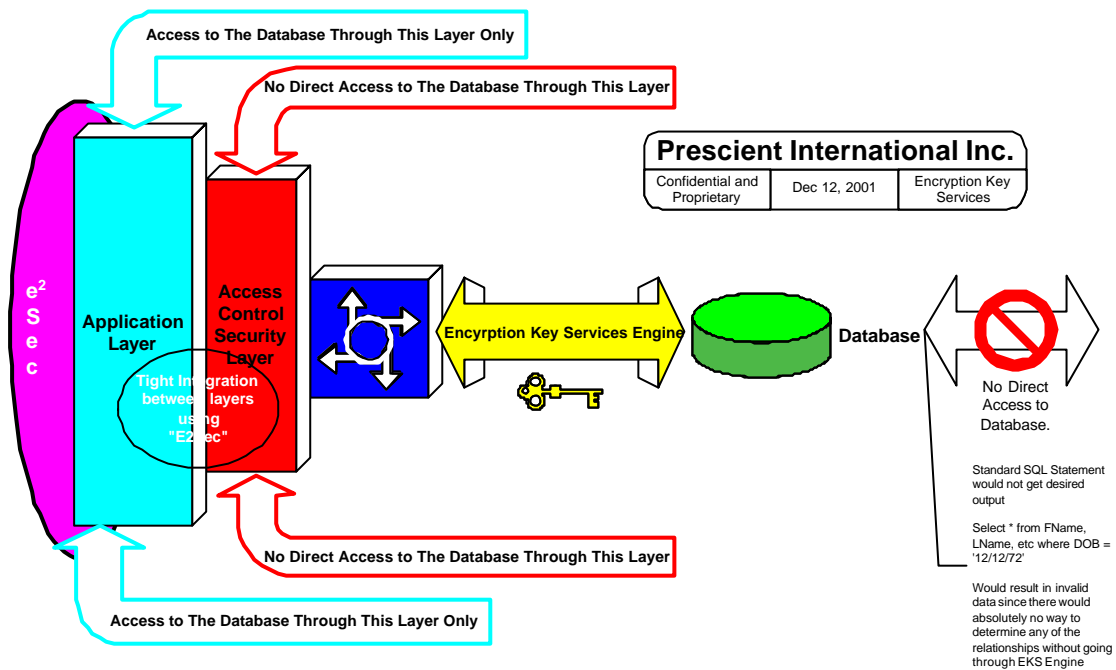
In order to ensure privacy and confidentiality of patient data, a number of issues need to be considered. Access rights and storage of confidential information are vital issues. Furthermore, mitigating the threat of unauthorized access both from within an organization and from beyond also needs to be paramount to any solution. Solutions that do not succeed in addressing these fundamental issues will ultimately fail in protection of confidential data.

Prescient International has developed a tool for Privacy Enhancement. The **Encrypted Relational Database Model (ERDM)** represents a new method of application and data design and management that ensures privacy and confidentiality of patient records, effectively decoupling patient information from medical information. Although itself, not a security model in the strictest sense of data encryption (as a Systems or Database Administrator can still have access to parts of the data tables), relationships between data elements are secured and protected. Neither Systems nor Database Administrators will be able to compile pieces of confidential information on any patient, such as tombstone data (e.g. date of birth, etc.), which could then be used to identify an individual. This solution prevents unauthorized access and ensures that patient data is secure, while reinforcing the fundamental tenets of legislation and societal trust in a public health system.

In order for a malicious hacker to access information that can identify a person, a specific query must be run, such as an SQL (Structured Query Language) query. These queries are similar to a logical statement that has specific qualifiers affecting operators and modifiers such as "if", "what", "and", etc. The difference between traditional relational databases and Prescient's **Encrypted Relational Database Model** is that an administrator (like a DBA or a Systems Administrator) cannot create a qualified query, since no known direct relationship exists between the entities. Therefore, relationships between data entities are secure, even from Systems and Database Administrators.

Recent articles in the news have highlighted issues of privacy and confidentiality with stories on hackers getting access to personal files and raw patient data. Changes to legislation at both the federal and provincial level are attempting to react to these issues by ensuring the rights of citizens are entrenched, and that the law protects the privacy and the confidentiality of personal information. Prescient has anticipated the results of such legislation by developing this relational model that prohibits the compiling of sensitive raw data elements without blocking authorized

access. This means that doctors and other authorized health care providers can access confidential patient data, but that no one who is unauthorized will be able to identify or use this confidential information. Queries can still be run on the data itself, for example, numbers of patients with high blood pressure, or the number of a certain kind of prescriptions that have been filled, but the relationships to personal qualifiers and identifiers are encrypted, meaning that confidential data is secured.



<sup>1</sup> Graeme Smith, "Tests find medical files open to hackers" Globe and Mail Monday, December 10, 2001-Print Edition, Page 1.