



PRIVACY ANALYTICS:

It's nothing personal

Amidst growing and legitimate anxieties over the privacy and security of our medical information, **Khaled El Emam's** software company, Privacy Analytics, has created a market-leading technology that will go a long way in putting our concerns to rest.

by Sean Rushton

As we continue our journey into the Information Age, the world is witnessing an unprecedented shift from paper records to electronic databases and online technologies, and our medical records are no exception. While easier access to medical data is extremely valuable for physicians, pharmacists, researchers and ultimately, the patient, it has also led to concerns about both patient privacy and provider confidentiality.

“Everybody wants this type of data, including governments, medical researchers, companies and hospitals,” says Khaled El Emam, who holds the Canada Research Chair in Electronic Health Information at the University of Ottawa and is an associate professor at uOttawa’s Faculty of Medicine and School of Electrical Engineering and Computer Science. “Lots of good things can come from sharing medical data, but procedures and tools must be put in place to make sure that data stays anonymous.”

Making health data more widely available for analysis provides many societal benefits. Hospitals and public health authorities, for example, use admission records to track influenza outbreaks, while researchers use similar patient data to identify promising trends in cancer therapies. However, if individuals feel their privacy has not been protected, they respond by adopting privacy-protective behaviours, often providing misleading information or refusing to disclose information at all.

How to balance societal needs against personal privacy is a difficult exercise, but one that El Emam has tackled head-on. In 2007, he created a spinoff company called Privacy Analytics to commercialize the results of leading-edge work he was doing at the University of Ottawa related to anonymization software—innovative technology that protects the anonymity of medical data by de-identifying it.

“The University has been very supportive of commercialization,” says El Emam. “Most of our employees are uOttawa grads, so the process of commercializing our research has allowed us to keep the best and the brightest here as well as to generate interest among the student body, getting them thinking about how to commercialize their ideas and deploy them in the real world.”

“Commercialization is a great way to shorten the normally lengthy process of translating research into practice.”

Privacy Analytics has fast become the world’s leading provider of automated de-identification solutions and software, which enable the disclosure of sensitive data without compromising individual privacy or anonymity.

“I think you can get a sense of just how big the issue of data privacy is today by simply picking up any daily newspaper,” says El Emam, who is also a senior scientist at the Children’s Hospital of Eastern Ontario Research Institute, where he leads the multidisciplinary Electronic Health Information Laboratory (EHIL) team. “In a few short years, the understanding of the term ‘data privacy’ has grown from a concern for information technology professionals into a

complex social issue affecting both public and private sector organizations.”

Privacy Analytics has developed a way to remove the risk and uncertainty surrounding the secondary use of medical data using a ground-breaking software solution called the Privacy Analytics Risk Assessment Tool, or PARAT. Using peer-reviewed metrics and proprietary de-identification algorithms, PARAT works by allowing users to assess what information in a medical database could identify a patient, measure the re-identification risk of the data and modify (or de-identify) specific pieces of information deemed to represent a considerable risk to patient privacy.

“In other words, family histories, home addresses and occupations are concealed by PARAT, while other valuable aspects of data are preserved. These can then be analyzed and potentially lead to important discoveries,” explains El Emam.

Standards currently in place for de-identification are either too restrictive—removing too much valuable data—or not restrictive enough, allowing the disclosure of data that has a high probability of re-identification. Such data breaches can be catastrophic and have far-reaching implications, not the least of which can be expensive litigation. Even more importantly for El Emam is the issue of public trust, without

which a lot of ground-breaking research and discoveries depending on data disclosure would grind to a halt.

“It only takes one breach of someone’s private health information before you start losing the public’s trust,” adds El Emam. “Data has a lot of value, and can bring about a lot of societal benefits when it is shared and analyzed. But the bottom line is that this has to be done in a way that is protective of privacy.”

With an eye to the future, Khaled El Emam emphasizes that it’s not just health information that’s being affected by privacy concerns.

“Basically, all organizations that have access to your information—your mobile phone habits, your lifestyle and shopping preferences, etc.—are looking for ways to analyze your data in order to capitalize on new insights and provide you with better services,” he explains.

The only commercially available technology of its kind on the market today, El Emam’s software is highly sought-after and has proven its ability to address privacy issues in healthcare organizations in Canada and abroad. And as the demand grows to use personal information of all types—like your web surfing habits—for research and commercial purposes, the potential market for Privacy Analytics’ proprietary software is staggering. **RP**

“Data has a lot of value, and it can bring about a lot of societal benefits when it is shared and analyzed. But the bottom line is that this has to be done in a way that is protective of privacy.” – Khaled El Emam