

KO Looking into privacy issues
Rick Garrick Sept. 2008

Keewatinoook Okimakanak is working with Canada's leading authority on eHealth risk management, privacy and security to improve guidelines for privacy issues within its own organization and in the communities.

“He suggested that when we are doing research data gathering, we abide by the Ownership, Control, Access and Possession (OCAP) principles for collective privacy,” says Franz Seibel, researcher with the Keewatinoook Okimakanak Research Institute. “He talked about the importance of following these principles in First Nation communities. KORI has already adopted these principles through our KORI Consultation Standards protocol.”

Brendan Seaton, principal author of the eHealth Risk-Opportunity Report Card, delivered the workshop by videoconference on Sept. 16 to a group of KO staff, including Seibel, Keewatinoook Okimakanak Telemedicine (KOTM) program manager Donna Williams, KOTM regional telemedicine coordinator Nancy Muller, KOTM community engagement coordinator Tina Kakepetum-Schultz and KO health director Robert Thomas.

The OCAP principles are designed to protect community/collective information in a similar manner as privacy principles protect individual information. Ownership refers to the community/group's collective ownership of information pertaining to that community/group, control refers to First Nation aspirations to maintain, regain and control research and data within their community, access refers to First Nation access to information and data about themselves and their communities, wherever it is held, and possession refers to a mechanism to assert and protect ownership of information and data about themselves and their communities.

Seibel adds that the OCAP principles call for destruction of all data once it has been analysed and reported on.

“We only use the data and analyse it for the purposes which we were originally researching for,” Seibel says. “It would be a breach of trust to use the data for something else. That's why destroying the data is important.”

Seaton also discussed Privacy Impact Assessments (PIA), which are a tool for defining privacy requirements for a new system or program; identifying privacy risks and to recommend actions to help manage those risks; and informing management, regulators and patients about the privacy features of a system or program and to advise of any residual privacy risks.

“We at KORI want to be more comprehensive in our research negotiations,” Seibel says. “So the PIA would help us.”

In addition to following the OCAP guidelines and developing their own KORI Consultation Standards in 2006, KORI also follows the CSA Privacy Code and plans to adopt any guidelines which are developed by KO to deal with privacy issues. The CSA Privacy Code refers to the rights of individuals to control the collection, use, disclosure and retention of personal information and contains 10 principles: accountability, defined purposes, consent, limiting collection, limiting use, disclosure, retention, accuracy, safeguards, openness, individual access, and challenging compliance.

“Once these new privacy guidelines are developed,” Seibel says, “KORI will begin using them in all of our research endeavours.”