the context of criminal proceedings." Members of the university's research ethics boards also pressed for support for the professors, writing Rock that a board had approved the research on condition of the participants' confidentiality, and months later, university administrators agreed to cover about half CAUT's expense, or $150 000.

The hearing took place in April 2013 before Justice Sophie Bourque of Québec Superior Court. Her 37-page decision issued Jan. 21, follows a legal framework known as the Wigmore criteria, a four-step analysis to determine if a particular communication should be protected against disclosure. The case hinged on whether the public interest in obtaining the "Jimmy" interview for the investigation and suppression of crime outweighed the interest in what Justice Bourque described as "the free flow of accurate and pertinent information," which could dry up without a reliable promise of confidentiality. She broke the seal and reviewed the interview transcript privately, but did not share its contents, writing that its relevancy to the charges against Magnotta or to a "not criminally responsible" defence was "minimal at most and marginal." Bourque quashed the search warrant, concluding that "the confidential interview is covered by the researcher–participant confidentiality privilege and … it should not be disclosed."

The Crown had until late February to appeal the decision but as of press time (Feb. 6) the case had already prompted rethinking of researchers' duties. New guidelines at the University of Toronto, for example, list principles to be followed in "research where external pressure to disclose is reasonably foreseeable" and the federal Interagency Advisory Panel on Research Ethics told *CMAJ* it would issue a new interpretation of the duty of confidentiality in the next two months. — Miriam Shuchman, Toronto, Ont.

CMAJ 2014. DOI:10.1503/cmaj.109-4717

New tools to improve safety of electronic health records

The US government has created a set of guides and tools to help health care providers more safely use electronic health records (EHRs). *The Safety Assurance Factors for EHR Resilience (SAFER) Guides* — which include self-assessment checklists, practice worksheets and recommended practices — were released by the US Department of Health and Human Services on Jan. 15.

"With the release of these guides, stakeholders now have ready access to additional evidence-based knowledge and practical tools to optimize EHR safety," Dr. Jon White, director of the Health Information Technology Portfolio for the Agency for Healthcare Research and Quality, said in a press release. "Consistent with the Health IT Safety Plan, health care providers and those who support them will use these guides to develop a culture of safety, shared responsibility, and continuous improvement around health IT."

Nine areas are addressed by the *SAFER Guides*, including organizational responsibilities, patient identification, clinical communication, test results review and follow-up, system configuration and contingency planning.

A contingency plan is necessary when an EHR system has an unexpected shutdown, which could be due to software failure, hardware malfunction, power outage or any number of unplanned events.

Wavebreak Media/Thinkstock

The United States government has created a set of online guides and tools to help health care providers more safely use electronic health records.

Many problems and delays can arise when electronic records become unavailable, says Dean Sittig, a professor in the School of Biomedical Informatics at the University of Texas Health Science Center at Houston.

It can become difficult to register patients, obtain test results from labs, communicate between departments and bill for medical services, to name but a few common problems. And not all hospitals are adequately prepared to function well during an outage.

"The hospitals where there have been downtimes in the past fare better than those that haven't," says Sittig. "For some reason, people don't want to learn this lesson when it happens to their neighbours."

To prevent EHR downtimes, health care providers should duplicate all critical hardware, have generators support their electronic systems during power outages and implement comprehensive testing and monitoring strategies. If a shutdown still occurs, there should be paper forms available, polices in place to ensure accurate patient identification and a communication strategy that doesn't rely on an electronic system.

"The recommended practices in the *SAFER Guides* are intended to be useful for all EHR users, developers, patient safety organizations and others who are concerned with optimizing the safe use of Health IT," states the guides' website. — Roger Collier, *CMAJ*

CMAJ 2014. DOI:10.1503/cmaj.109-4715