Français à la page suivante

Paying the PIPEDA

The legislative behemoth known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) finally staggered into the offices of American physicians this April, demanding compliance with a complicated set of regulations for the protection of patient health information. A brainchild of the Clinton administration, HIPAA (and, more specifically, its accompanying "Privacy Rule") has since been amended into a less protective beast.[1] But, weighing in at 90 pages, its bureaucratic girth intimidates. As one commentator puts it, implementation is "likely to be costly, inconsistent, and frustrating to both physicians and patients."[2] Training, the creation of new administrative processes and tracking systems, and a minor industry in HIPAA consultancies are adding significant costs to an already expensive health care system.[3]

Arguably, the HIPAA Privacy Rule is more about patient records than about patients themselves. It is not an *a priori* definition of privacy rights, but a set of procedural standards for the management of information — the bits of data arising from the digitized patient and transmitted to insurance plans. In the parlance of the rule, the "covered entity" is not the patient, but the person or agency who conducts billing transactions. If HIPAA is a hippopotamus, the patient is a bureaucratic chimera of potential "identifiers." The living, breathing patient-in-the-office is barely mentioned, although a guidance document does address the importance of "reasonable safeguards" for sound privacy and other decorums in hospitals and clinics.[4]

Although the evolution of health information privacy legislation in Canada has engendered less dread than HIPAA in the US, it too is an awkward creature with a similar genesis. The federal Personal Information Protection and Electronic Documents Act (PIPEDA; 1999) was spurred largely by the development of new technologies for keeping track of who we are and what we do: as the privacy commissioner once warned, all of our daily transactions, however innocent, can now easily be merged into a single, potentially harmful "superfile."[5] As PIPEDA appeared on the legislative horizon (it comes fully into force with respect to health information in January 2004) the CMA appealed to the traditional idea that physicians are the keepers of the keys to confidentiality, and strategically wrote a *Health Information Privacy Code* (1998) affirming the "special nature" of health care information.[6]

As the provinces struggle to bring their legislation into line with PIPEDA, one of the subtlest issues has proved to be patient consent for the collection and use of medical information.[7] It remains to be seen how strictly PIPEDA will be interpreted in this regard by the federal privacy commissioner. Will patients need to be informed of their privacy rights at each and every "episode of care"? Will they have to be notified of each new or unanticipated use of their information? What consent must be explicit; what may be inferred? It is not one great beast that is arriving in Canadian physicians' offices but a menagerie of laws, regulations, guidelines, policy statements, consent forms and toolkits.

Requirements for patient consent — ranging from implied consent for the use of one's medical history in guiding treatment, to informed consent for the use of case information (e.g., radiographs) in teaching and anonymized data in research, to explicit consent for the disclosure of genetic testing results — are based on a societal consensus about the value of patient autonomy, the "ownership" of personal information, the need for expediency and efficiency, and the importance of research agendas and public health. These are not trivial issues, and the potential for the misuse of private information should be taken seriously. But, as legislators elaborate the ways and means of managing the particulate matter of "protected health information," let's hope that physicians continue to see their patients whole. And that they do not need a hippopotamus to remind them to discuss cases somewhere more private than elevators and hallways, to hang charts where visitors cannot read them, and to ensure that private disclosures are not overheard by the stranger waiting in the next cubicle. — *CMAJ*

References

1. Pear R. Bush rolls back rules on privacy of medical data. *New York Times* 2002; Aug 10 A1:6.
2. Annas GJ. HIPAA regulations: A new era of medical-record privacy? *N Engl J Med* 2003;348(15):1486-90.
3. Kilbridge P. The cost of HIPAA compliance. *N Engl J Med* 2003;348(15):1423-4.
4. US Office for Civil Rights – HIPAA. OCR guidance explaining significant aspects of the HIPAA Privacy Rule – Dec 2, 2002. Incidental uses and disclosures. Available: www.hhs.gov/ocr/hipaa/privacy.html (accessed 2003 June 16).
5. Privacy Commissioner of Canada. A day in the life … or how to help build your superfile. Available: www.privcom.gc.ca/fs-fi/02_05_d_01_e.asp (accessed 2003 June 17).
6. Health information privacy code [policy summary]. Canadian Medical Association. *CMAJ* 1998;159(8):997-1006 .
7. Upshur RE, Morin B, Goel V. The privacy paradox: laying Orwell's ghost to rest [published erratum appears in *CMAJ* 2001;165(7):888]. *CMAJ* 2001;165(3):307-9.