

Editorial Comments ■**Physician PDA Use and the HIPAA Privacy Rule**

PAUL E. PANCOAST, MD, MBA, TIMOTHY B. PATRICK, PhD, JOYCE A. MITCHELL, PhD

■ *J Am Med Inform Assoc.* 2003;10:611–612. DOI 10.1197/jamia.M1388.

Optimal health care delivery requires that providers have access to current clinical information.¹ In the last 25 years, hospitals have dramatically improved diagnostic capabilities for both inpatients and outpatients, but providers often do not have access to the results.² These disruptions in information availability lead to clinical errors and can cause patient injury or death. Many physicians use individual lists with names, hospital identifiers, room numbers, and pertinent clinical information when a decision needs to be made and the patient's record is not at hand. With the ready availability of personal digital assistants (PDAs), many clinicians now keep these patient lists in electronic format.^{3–6} Physicians can improve their access to information by downloading patient data into personal handheld computers that are available wherever decisions need to be made. Hospital administrators may be reluctant to allow such information transfers because of concerns about confidentiality and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. However, careful definition of the HIPAA Designated Record Set can eliminate the need to track the use of information stored in provider PDAs.

All physicians, whether employed by a covered entity or covered entities in their own right, have legal and ethical obligations to protect the confidentiality of patient information.⁷ Medical students and resident physicians are members of the hospital workforce. They have varying levels of autonomy in medical decision making, but the hospital administration regulates their activities in the hospital setting; they are required to follow the privacy regulations of the hospital that employs them. Other physicians are employed by hospitals and health plans that contract their services. These physicians also are under the jurisdiction of the administrative policies of their employers. Physicians who treat patients in multiple locations may be part of multiple

workforces and may encounter different policies in each location. They are ultimately bound by the policies of their primary covered entity (employer) but should follow the policies of each facility when working in that setting. Privacy regulations are set by the privacy officer, a person designated to design the policies and procedures to ensure compliance with HIPAA regulations. Even a solo practitioner must designate a privacy officer for their practice. Physicians generally are aware of their duty to protect confidential information in their care, but they may not be aware of the technical means to protect the information on their PDA.⁸ We recommend several simple precautions that should be taken by every health care provider who stores patient information on a PDA:

- Keep careful physical control of the device at all times.
- Use data encryption technology to protect the information.
- Use a password when turning on the PDA and a time-out to reactivate the password.
- Disable the infrared ports except during use.
- Do not send infrared transmissions in public locations.^{6,9,10}

These recommendations should be followed as a matter of standard practice. The adoption of new technologies has great potential to improve patient outcomes and reduce potential injury but also imposes a burden of precautions in the face of increased risks.¹¹ The use of PDA-based patient lists is no exception. If physicians download patient information into their PDAs, over which they alone have control, they must assume the responsibility for safeguarding the confidentiality of that information.

References ■

1. Institute of Medicine. *Crossing The Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academy Press, 2001.
2. McKnight L, Stetson PD, Bakken S, Curran C, Cimino JJ. Perceived information needs and communication difficulties of inpatient physicians and nurses. *Proc AMIA Symp.* 2001;453–7.
3. Bauer JC. Rural America and the digital transformation of health care. *New perspectives on the future.* *J Leg Med.* 2002;23(1): 73–83.
4. Sokol AJ. The changing standard of care in medicine: e-health, medical errors, and technology add new obstacles. *J Leg Med.* 2002;23(4):449–90.
5. Duncan RG, Shabot MM. Secure remote access to a clinical data repository using a wireless personal digital assistant (PDA). *Proc AMIA Symp.* 2000:210–4.
6. Fischer S, Stewart TE, Mehta S, Wax R, Lapinsky SE. Handheld computing in medicine. *J Am Med Inform Assoc.* 2003;10: 139–49.

Affiliation of the authors: Department of Health Management and Informatics, School of Medicine, University of Missouri, Columbia, Missouri.

This research was supported in part by National Library of Medicine Biomedical and Health Informatics Research Training Grant 2-T15-LM07089-11. Similar material appeared in a poster presentation at the AMIA Fall Symposium 2003.

Correspondence and reprints: Paul E. Pancoast, MD, MBA, 324 Clark Hall, Department of Health Management and Informatics, School of Medicine, University of Missouri, Columbia, MO 65211; e-mail: <pancoastp@health.missouri.edu>.

Received for publication: 04/28/03; accepted for publication: 06/30/03.

7. Wynia MK, Coughlin SS, Alpert S, Cummins DS, Emanuel LL. Shared expectations for protection of identifiable health care information: report of a national consensus process [comment]. *J Gen Intern Med.* 2001;16:100-11.
8. De Ville KA. The ethical and legal implications of handheld medical computers. *J Leg Med.* 2001;22:447-66.
9. Chilton L, Berger JE, Melinkovich P, et al. American Academy of Pediatrics. Pediatric Practice Action Group and Task Force on Medical Informatics. Privacy protection and health information: patient rights and pediatrician responsibilities [comment]. *Pediatrics.* 1999;104(4 pt 1):973-7.
10. Blanton SH. Securing PDAs in the health care environment. SANS Info Sec Reading Room. 09/06/2001. <http://www.sans.org/rr/pdas/health_care.php>. Accessed February 16, 2003.
11. Terry NP. Cyber-malpractice: legal exposure for cybermedicine. *Am J Law Med.* 1999;25:327-66.