HIPAA on Phones, Faxes & E-mail

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

My wife Deborah Black (light of my life) is a neuropsychiatrist who works at two different clinics. Sometimes patients are referred from one clinic to the other, and the question arises of how to transmit the details of their medical record from one team to the other. Anything concerning the privacy of medical data in the USA is governed by the Health Insurance Portability and Accountability Act (HIPAA)< http://www.law.cornell.edu/usc-cgi/get_external.cgi?type=pubL&target=104-191 > passed in 1996. The legislation is complex, and the US Department of Health & Human Services (HHS)< http://www.hhs.gov > has set up an extensive Web site with detailed information and instructions about HIPAA.< http://www.hhs.gov/ocr/privacy/ >

One of the questions I've been asked by my wife's staff is whether it is acceptable to send medical information by fax or e-mail; some of the security and information technology staff at her clinics have flatly forbidden such transmission, asserting baldly that HIPAA forbids such transmission. Unfortunately, their medical records systems are incompatible, so the data cannot be sent automatically from one clinic to the another with appropriate encryption and other safeguards.

However, the IT/security staff are wrong in their absolute interdiction of faxes and e-mail for medical records.

In the document entitled, "Does the HIPAA Privacy Rule permit a doctor, laboratory, or other health care provider to share patient health information for treatment purposes by fax, e-mail, or over the phone?"< http://www.hhs.gov/hipaafaq/providers/smaller/482.html >, the HHS writes (quoting in full),

Yes. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise.

For example:

- A laboratory may fax, or communicate over the phone, a patient's medical test results to a physician.
- A physician may mail or fax a copy of a patient's medical record to a specialist who intends to treat the patient.
- A hospital may fax a patient's health care instructions to a nursing home to which the patient is to be transferred.
- A doctor may discuss a patient's condition over the phone with an emergency room physician who is providing the patient with emergency care.
- A doctor may orally discuss a patient's treatment regimen with a nurse who will be involved in the patient's care.

- A physician may consult with another physician by e-mail about a patient's condition.
- A hospital may share an organ donor's medical information with another hospital treating the organ recipient.

The Privacy Rule requires that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. These safeguards may vary depending on the mode of communication used. For example, when faxing protected health information to a telephone number that is not regularly used, a reasonable safeguard may involve a provider first confirming the fax number with the intended recipient. Similarly, a covered entity may pre-program frequently used numbers directly into the fax machine to avoid misdirecting the information. When discussing patient health information orally with another provider in proximity of others, a doctor may be able to reasonably safeguard the information by lowering his or her voice."

In the next of this two-part series, I'll look at what's reasonable in transmitting patient data.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >