The NEW ENGLAND JOURNAL of MEDICINE

Perspective

MARCH 14, 2013

Protecting Patient Privacy and Data Security

Julie K. Taitsman, M.D., J.D., Christi Macrina Grimm, M.P.A., and Shantanu Agrawal, M.D.

On December 4, 2012, two Australian radio DJs called London's King Edward VII's Hospital, identified themselves, in fake British accents, as Queen Elizabeth and Prince Charles, and asked about a celebrity patient who had been admitted for pregnancy complications. A nurse, filling in at the reception desk in the early morning hours, answered the phone and, without attempting to verify the callers' identities, transferred them to the duty nurse caring for the Duchess of Cambridge. The duty nurse then provided them with confidential patient information.[1] The Australian DJs broadcast the phone call, considering it a humorous prank, but as the world knows, it had disastrous consequences.

How confident are U.S. hospitals, nursing homes, and physicians' offices that their staff would appropriately deny patient information to an unknown caller?

Too often, unauthorized people succeed in extracting protected information from health care providers. Invasion of privacy also affects noncelebrities, when anyone seeks health information the patient has not chosen to share. More often, though, scam artists seek patients' billing information for financial gain. The patient's insurance identifier is then used by an uninsured person to obtain medical services or by a fraudulent health care provider to bill for medical services that were never rendered. Data security breaches and medical identity theft are growing concerns, with thousands of cases reported each year. The Centers for Medicare and Medicaid Services (CMS) tracks nearly 300,000 compromised Medicare-beneficiary numbers.[2] The Office for Civil Rights has received more than 77,000 complaints regarding breaches of health information privacy and completed more than 27,000 investigations, which have resulted in more than 18,000 corrective actions.[3]

Beyond privacy concerns, breaches of health information security exact a weighty financial toll and endanger patients. Abuse of insurance identifiers drains money that would be better spent funding legitimate health care services. When Medicare and Medicaid overpay for services, taxpayers bear those costs. When private insurers overpay, policy-

holders face higher premiums and copayments. The most obvious toll on the individual beneficiary is financial liability for services that are fraudulently obtained in the beneficiary's name. The beneficiary may also run up against service limits when he or she later seeks reimbursable medical services.

And identity breaches can deleteriously affect the quality of care. Incorrect information can infiltrate the beneficiary's medical record and corrupt later medical decision making. Beneficiaries have been wrongly labeled as diabetic or HIV-positive when people with those conditions obtained services using a beneficiary's medical identity. Pharmacists have rejected beneficiaries' legitimate prescriptions and suppliers have refused to furnish needed wheelchairs when records have incorrectly shown that the beneficiary recently received the items in question.

Health care providers should better protect patients' privacy and medical data (see table). Traditionally, hospitals posted notices in elevators and cafeterias warning staff members not to discuss patients in public areas. The risk of electronic eavesdropping further complicates health care providers' responsibility to protect patient privacy. In a series of compliance audits undertaken by the Office of Inspector General (OIG) of the Department of Health and Human Services, government auditors sitting in hospital parking lots with simple laptop computers could obtain patient information from unsecured hospital wireless networks.[4] Health care providers should follow best practices to ensure that computer networks are more secure. As progress continues toward the development of a national infrastructure for electronic health information, security of electronic data becomes increasingly important. Firewalls, strong security protocols, antivirus programming, and password protections are essential. Too often, health care professionals undermine password protection, remaining signed in under their usernames on multiple computers when the devices are out of their immediate control. The minor convenience this practice affords comes at the cost of greatly endangered data security. Automatic, timed logouts and employee training can address this problem. Similarly, attention to data security must not stop at the clinic doors; health care professionals should follow secure procedures when using portable electronic devices and home computers (see box).

Some patient data are stolen, whereas other data are volunteered by or elicited from helpful staff members or even the patients themselves. The OIG has warned Medicare and Medicaid beneficiaries about common scams perpetrated to obtain their insurance information. Health care providers should also educate staff members about protecting patient information. At times, people call physicians' offices or hospitals posing as referring physicians, specialists, pharmacies, vendors, friends, relatives,

Selected Privacy and Security Safeguards.

Type of Safeguard	Examples
Physical	
Confidential patient care	Private examination and consultation rooms; conducting phone calls and other conversations where unlikely to be overheard; attention to eavesdropping risks
Document storage	Secure-access filing for medical records and bills; controlled prescription pads
Document disposal and destruction	Shredding
Electronic	
User authentication	Passwords; biometric identification; automatic logouts
Systems protections	Firewalls; antivirus programming; active audit trails
Safe hardware disposal	Erasing hard drives from rented photocopiers; proper disposal of used computers
Human capital	
Careful hiring practices	Careful vetting of potential hires, including the use of background checks
Training and education	Education about individually identifiable information; appropriate information sharing; protocols for screening information seekers
Termination and separation protocols	Timely deactivation of electronic and physical access

or insurance representatives. Providers must teach their staff to authenticate such calls and release only information to which the caller is entitled.

Patients can be important partners in protecting privacy and combating identity theft. Providers and insurers can help educate patients to protect themselves. The OIG encourages health care providers to print multiple copies of the brochure it developed advising patients on ways to avoid falling prey to medical identity theft.[5]

Insurers can also do a better job of protecting patient information. Ideally, all insurers would adopt best practices that experience has proven effective. For example, Medicare and many private insurers send beneficiaries explanation-of-benefits statements or other notices whenever a service has been charged to their insurance policies. Beneficiaries are encouraged to review these statements, even if no out-of-pocket payment is owed, since review affords an early opportunity to identify misuse of insurance benefits, such as claims submitted by a provider the beneficiary never used or for a service the beneficiary never received. Unfortunately, most state Medicaid programs do not routinely send such statements to beneficiaries, forgoing one effective tool for identifying security breaches early.

Federal law affords American patients strong privacy protections. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act established legal mechanisms to ensure privacy and security of medical identity and protected health information. HIPAA created transactional security requirements for the exchange of certain health information and regulated its disclosure. HITECH expanded HIPAA in a number of ways, including by requiring notification of victims of breaches of protected health information held by HIPAA-covered entities and vendors of personal health records. Unfortunately, however, practice often falls short of intended statutory protections.

CMS and the OIG have collaborated to create instructive educational materials offering best practices for promoting privacy and data security. It is crucial that patients and health care professionals work together to safeguard patient information and prevent security breaches. Patients and providers deserve greater assurance that the next time a health care professional answers the phone and it's "London calling," the inquiry will be handled properly and patient privacy and health data will be adequately protected.

Steps to Protect and Secure Information When Using Mobile Devices.*

- Install and enable encryption
- Use a password or other user authentication
- Install and activate wiping, remote disabling, or both to erase data on lost or stolen devices
- Disable and do not install or use file-sharing applications
- Install and enable a firewall to block unauthorized access
- Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks
- Keep security software up to date
- Research mobile applications before downloading
- Maintain physical control of mobile devices
- Use adequate security to send or receive health information over public Wi-Fi networks
- Delete all stored health information on mobile devices before discarding the devices

* Recommended by the Office of the National Coordinator for Health Information Technology.

The views expressed in this article are those of the authors and do not necessarily reflect the views of the U.S. Department of Health and Human Services, Office of Inspector General, or the Centers for Medicare and Medicaid Services.

Disclosure forms provided by the authors are available with the full text of this article at NEJM.org.

From the Office of Inspector General, Department of Health and Human Services, Washington, DC (J.K.T., C.M.G.); and the Center for Program Integrity, Centers for Medicare and Medicaid Services, Baltimore (S.A.).

This article was published on February 27, 2013, at NEJM.org.

1. Lyall S. Prank call seeking royal family secrets takes horrifying turn. New York Times. December 7, 2012.
2. Agrawal S, Budetti P. Physician medical identity theft. JAMA 2012;307:459-60.
3. Office for Civil Rights. Health information privacy. Numbers at a glance. (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/indexnumbers.html).
4. Office of Inspector General, Office of Audit Services. Audit of information technology security included in health information technology standards. May 2011 (https://oig.hhs.gov/oas/reports/other/180930160.pdf).
5. Medical identity theft/fraud information (https://oig.hhs.gov/fraud/medical-id-theft/OIG_Medical_Identity_Theft_Brochure.pdf).

DOI: 10.1056/NEJMp1215258