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.

Health care providers should better protect patients' privacy and medical data.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.

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.

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.