JRM®
The Journal of Reproductive Medicine®

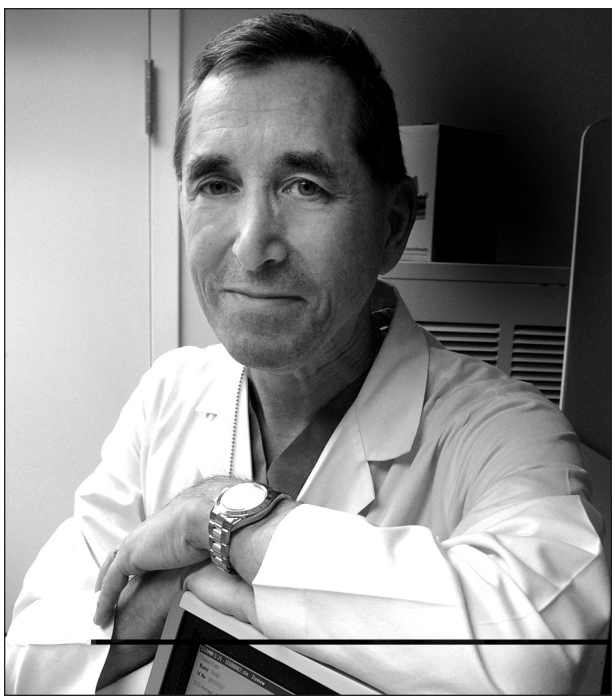
Volume 62, No. 11-12/November-December 2017

EDITORIAL

A Note from the Editor-in-Chief

Lawrence D. Devoe, M.D.

Welcome to the November-December 2017 Editor-in-Chief's page. This editorial column focuses on a growing concern for patient privacy and safety that has been spawned by the adoption of cyber-based technologies involved in documentation and healthcare.



Lawrence D. Devoe, M.D., Editor-in-Chief

Two years ago, the Affordable Care Act mandated that American physicians begin to use an electronic health record (EHR) in their routine provision of patient care. While this seemed to be a reasonable requirement at the time, the events that have followed have shown that there have been unintended consequences that have actually compromised not only patient care but the protection of personal information that is attached to each medical encounter.

Since the inception of the Affordable Care Act in 2013, there has been a full-frontal attack on the security of electronic patient healthcare records that has now swelled through relentless hacking, largely from overseas agencies. What makes this a huge problem is the nature of the data that is acquired when patients' personal information is no longer private nor encrypted. Getting access to names, birth dates, home addresses, diagnostic codes, and billing details opens up a treasure trove of information that can be used to generate fraudulent invoices to patients and their insurers, to set up other types of individual accounts, and, in some instances, generate credit card applications. In this day and age, it would seem inconceivable that such important data could be so vulnerable to hackers. However, as illustrated by the recent case of a large credit-reporting corporation that was similarly compromised, the answers are straightforward. First and foremost, many data management companies use relatively ancient legacy computer plat-

0024-7758/17/6211-12–0591/$18.00/0

forms that are no longer fully supported. Security patches have been made available to shore up these outdated operating systems but require that the companies actually install them—all too often not the case. What makes this situation even more insidious is that, unlike credit card hacking and its subsequent fraud protection process, it may take months to years to discover that healthcare information has been compromised on a patient-by-patient basis.

Of perhaps even greater concern is the hacking of medical devices, as illustrated by a recent U.S. Food and Drug Administration warning regarding—in that particular case—cardiac pacemakers. The portal involved is that used for remote transmission of data stored on such devices to a clinical repository where it is reviewed and then used, in some instances, for reprogramming. Besides creating personal data vulnerability, it is possible that ill-intentioned hackers could interfere with the function of these devices and cause harm to patients. Firmware upgrades have been made possible when patients present to their providers, but the cautionary note sounded is that any medical device systems that remotely transmit patient data are now targets for unscrupulous cyber criminals.

It has become clear that the healthcare community has entered a brave new world of disease management from which there is no turning back. Because data system hacking has become a regular fact of life, it behooves both patients and their physicians to become better educated in the process of personal data protection since we will be living in the era of cyber-based care in perpetuity.