

DECEMBER 2008

## Patient Emails: Are Providers Ready for This Growing Trend?

By Mark C. Rogers, The Rogers Law Firm, Boston, MA

### I. INTRODUCTION

Arguably one of the most significant issues facing today's health-care providers is the expanding use of health information technology. Providers are, to varying degrees, responding to increased pressure from federal and state government, third-party payors, and consumers to adopt electronic health records (EHRs) and electronic prescribing (e-prescribing) as a means of controlling healthcare costs, increasing efficiency, improving quality of care, and expanding patient access to protected health information. A corollary to this growing use of health information technology is the increase in provider-patient email communications. Physicians, nurse practitioners, nurses, and other providers are utilizing emails to communicate with patients about their continuing care and treatment. This article discusses the growing trend of provider-patient email communications and provides an overview of the important issues that providers need to be aware of before adopting this practice.

### II. GROWING TREND

It is estimated that approximately one-third of physicians communicate with their patients online—either through email or secure messaging services.<sup>1</sup> This number is expected to grow as more resources are dedicated to providers by federal and state government, third-party payors, and hospitals in order to subsidize the costs associated with the adoption of health information technology. Of those U.S. consumers with Internet access, 90% indicate a clear preference for online communications with their providers.<sup>2</sup>

A reluctance by some providers to communicate with their patients via email may be rooted in the belief that such communications will increase their workload through patient abuse of the email access. A recent study from the University of Pittsburgh, however, shows that patients who are allowed to communicate with their physician via email do not abuse such access.<sup>3</sup> The study monitored the use of emails between the parents of pediatric patients and a pediatrician in an academic pediatric

rheumatology practice in Pittsburgh, PA. Of the 328 families who were offered the email service, 306 enrolled, and 121 used the service. The pediatrician received 1.2 emails per day from parents.<sup>4</sup> Forty percent of the emails were sent outside business hours and messages that required emergent attention made up only .002% of the emails to the pediatrician. More importantly, however, the pediatrician was able to respond to patient questions 58% faster than using the telephone.<sup>5</sup> Furthermore, families who responded to a survey about the study agreed that the use of the email increased access to the pediatrician and improved the quality of care.<sup>6</sup>

A sign of the increasing use of online communications between providers and their patients is the recent announcement by health insurers such as Aetna and Cigna that they are planning to begin reimbursing physicians for "online physician visits" through a secure website.<sup>7</sup> Insurers believe that patients will utilize the service because it can improve efficiency and prevent more costly problems.<sup>8</sup> It is expected that over time other

insurers will follow along with this practice of reimbursing providers for their online interactions with patients.

### III. LIABILITY EXPOSURE

Before providers respond to the increased demand for email communication with their patients, they need to first be aware of the potential liability exposure that follows such communications. In particular, providers need to be sure that they comply with the numerous requirements of the HIPAA Security Rule. A violation of the Security Rule in the context of a provider's email communications with patients subjects the provider, or "covered entity," to potential fines from the U.S. Department of Health and Human Services. Furthermore, provider-patient email communications can serve as demonstrable evidence of a provider's negligence in a medical malpractice action.

Of those U.S. consumers with Internet access, 90% indicate a clear preference for online communications with their providers.

#### A. HIPAA Security Rule

The HIPAA Security Rule is the lesser known of the two major administrative simplification provisions of the Health Insurance Portability and Accountability Act. The other, of course, is the HIPAA Privacy Rule. The HIPAA Security Rule sets forth a series of administrative, technical, and physical security procedures for providers to utilize to ensure the confidentiality of electronic protected health information—which is

any protected health information maintained in electronic form, including provider-patient emails.<sup>9</sup> There are both civil and criminal penalties associated with violations of the HIPAA Security Rule. The civil penalties range from \$100 per violation to up to \$25,000 per year for each requirement violated.<sup>10</sup> The criminal penalties range from \$50,000 in fines and one year in prison up to \$250,000 in fines and 10 years in prison.<sup>11</sup>

The HIPAA Security Rule is broken down into "Standards" and "Implementation Specifications." The Standards refer to certain principles that a provider must meet in order to comply with the Security Rule. The Implementation Specifications describe how a provider is to meet those principles. There are a number of HIPAA Security Rule Standards and Implementation Specifications that arise in the context of

Your compensation consultant  
should be focused on one goal:

**YOURS.**



Executive and physician compensation becomes more and more complex every day. That's why boards, compensation committees, and executives look to SullivanCotter—for help creating total compensation packages that support your business objectives and mission while meeting regulatory requirements. Because we offer no ancillary products or services, you always know that our recommendations are based on what's right for your organization. Now more than ever, you need someone you can trust to help you navigate this ever-changing environment. Talk to SullivanCotter today.

**sullivancotter**  
AND ASSOCIATES, INC.

INTEGRITY. INDEPENDENCE. INSIGHT.

[www.sullivancotter.com](http://www.sullivancotter.com) | 888.739.7039

online communications between providers and their patients. How these standards and specifications are met will vary from provider to provider, depending upon the size and available resources of the provider. Although it is important for a provider to address all of the Security Rule Standards and Implementation Specifications before engaging in the practice of communicating with patients via email, particular focus should be given to the Security Rule's Technical Safeguards.<sup>12</sup> Included within the Technical Safeguards is the Transmission Security Standard, which is one of the more critical standards for providers to be aware of when emailing their patients. This Standard requires providers to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.<sup>13</sup>

The Transmission Security Standard also includes an Encryption Implementation Specification that requires a covered entity, assuming it is reasonable and appropriate, to implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.<sup>14</sup> Encryption is a "method of converting an original message of regular text into encoded or unreadable text that is eventually decrypted into plain comprehensive text".<sup>15</sup> In layman terms this means that providers should not be sending emails to patients using online commercial email services. Rather, providers who send emails to their patients should utilize a secure network in which information technology experts can confirm the emails are encrypted.

The importance of complying with the HIPAA Security Rule is

Before providers respond to the increasing demand for email communication with their patients, they need to first be aware of the potential liability exposure that follows such communications.

underscored by recent reports of computer hackers breaking into the data systems of providers and obtaining the personal information of patients. For example, two separate computer databases belonging to Akron Children's Hospital in Ohio were breached by computer hackers in 2006. The databases contained the personal information of over 240,000 people, including donors, hospital patients and their parents and guardians.<sup>16</sup> Examples of such breaches are expected to increase as the online databases of providers are seen as particularly vulnerable to hackers based on their belief that less attention has been focused on online security in the healthcare industry as there has been in other industries such as finance and retail.

**B. Medical Malpractice Implications**

A common scene played out in medical malpractice trials throughout the country each day is a patient's attorney questioning a physician on the witness stand about a note the physician wrote in the patient's medical record several years earlier regarding some aspect of the physician's care and treatment. In order to assist the jury, the attorney will use a "chalk" or cardboard blow-up of

the note. Through testimony, the note is analyzed for several hours and in some instances, several days, by the parties and their respective experts. Now fast forward to five or ten years from today. It is highly likely that we will begin seeing chalks of patient-provider emails in medical malpractice trials. Although some will argue that emails present providers with an excellent opportunity to demonstrate to a jury their appropriate care and treatment of a patient, they also can be seen, in some instances, as evidence of the provider's failure to clearly communicate with the patient.

Providers who communicate with patients via email need to ensure that such communications are clear and appropriate. Acronyms, abbreviations, and short-hand that is all-too-common in a medical record, is not appropriate in an email to a patient. A misunderstanding or misinterpretation by the patient or a subsequent treating provider can have dire consequences for the patient.

**IV. BEST PRACTICES**

Providers who communicate with patients via email can minimize their potential liability exposure by adopting a comprehensive policy that includes best practices for provider-patient emails. Such a policy should address the following:

- Encryption: Email communications from a provider to a patient should be encrypted utilizing updated encryption security technology.
- Informed Consent: A provider should obtain written informed consent from every patient with whom the provider may communicate via email.

The informed consent form should specifically authorize the provider to communicate with the patient via email and should inform the patient of the following:

- Although all reasonable attempts will be made by the provider to maintain the confidentiality of email communications, the provider cannot guarantee that such communications will not be intercepted, misdirected, or undelivered;
  - The provider will only email the patient at the email address specifically identified by the patient on the informed consent form;
  - Email communications from the patient to the provider should be limited to those that pertain to the patient's care and treatment;
  - The patient should not email the provider in an emergency situation, but rather should contact emergency medical services;
  - The patient should only respond to email communications from the provider that come from email addresses that have been previously identified to the patient by the provider; and
  - If the patient does not conform to the requirements of the informed consent form, the provider reserves the right to terminate email communications with the patient.
- Retention: All email communications between a provider

The importance of complying with the HIPAA Security Rule is underscored by recent reports of computer hackers breaking into the data systems of providers and obtaining the personal information of patients.

and his/her patients should be transferred to the patient's medical record within a reasonable period of time and produced in response to an appropriate authorization for release of the patient's

medical record. It is critical that a subsequent treating provider be able to review a patient's medical record and understand the current state of the patient's overall health. The email communications between the previous treating provider and the patient are a necessary component of that understanding.

- Auto-Reply Message: A provider should set-up an auto-reply message on their email system stating that (1) patient email communications will be responded to in a specified time period (i.e. next business day); and (2) if you are a patient experiencing an emergency situation to immediately contact emergency medical services.

coding | Compliance  
solutions

SIMPLY THE BEST

JUST ASK OUR CLIENTS

GEORGEANN EDFORD & ASSOCIATES

1000 S. WOODWARD • SUITE 105

BIRMINGHAM MI 48009

1-800-832-4144

GEDFORD@CODINGCOMPLIANCE.COM

- Confidentiality Notice: All emails from a provider to a patient should include a standard confidentiality notice informing the recipient of the email that the email message is confidential and is intended only for the individual to whom it is addressed. The notice should also state that if the individual has received the email in error to immediately notify the provider and to delete the message from any hard drive, disk, or other means of electronic storage.
- Email Use Restrictions: The following restrictions should be observed by any provider who communicates with a patient via email:
  - emails should only contain the minimum necessary amount of protected health information;
  - emails should be written in clear and complete sentences without acronyms or abbreviations;
  - any email to a patient that is misdirected must be documented on the patient's accounting of disclosures;
  - unless an individual is designated as the patient's personal representative, a provider should only email the patient; and
  - if a provider believes that a patient will, by reason of the subject matter, not understand an email communication or if it appears to the provider that the patient did not understand a previous email communication, the provider should no longer

Although some will argue that emails present providers with an excellent opportunity to demonstrate to a jury their appropriate care and treatment of a patient, they also can be seen, in some instances, as evidence of the provider's failure to clearly communicate with the patient.

communicate with the patient via email regarding such subject matter, but rather should attempt to contact the patient via telephone.

It is important to keep in mind that in many instances it may not be the physician who communicates via email with the patient. Often times such communications take place between a patient and a nurse practitioner or a nurse. Therefore, a provider's patient email policy should be broad enough to include non-physician staff.

#### V. CONCLUSION

Email communication with patients is an inevitable part of almost every provider's future healthcare practice. In order to be prepared for this growing trend, providers need to work with legal counsel and their information services department or vendor to address the potential

liability exposure they face from such communications.

*Mr. Rogers is a member of the Health Care and Corporate Practice Groups at The Rogers Law Firm in Boston, MA. He is also a member of the firm's Consulting Division ([www.trogsolutions.com](http://www.trogsolutions.com)). He focuses his practice primarily on healthcare law. He has written and lectured extensively on legal issues in the healthcare field. Mr. Rogers is Co-Editor of The Boston Health Law Reporter and is an adjunct faculty member at New England School of Law, where he teaches Hospital Law.*

- 1 The Doctor Is In...Your Inbox?, Manhattan Research, Press Release, June 23, 2008.
- 2 Herrick D., Telemedicine Provides Benefits, But Security and Privacy Risks Abound. Health Care News, [www.heartland.org/Article.cfm?artid=19110](http://www.heartland.org/Article.cfm?artid=19110) (last accessed on Sept. 3, 2008).
- 3 Rosen, Paul and Kuch, C. Kent, Patient-Physician E-mail: An Opportunity to Transform Pediatric Health Care Delivery, 120 Pediatrics 701 (Oct. 2007).
- 4 See id.
- 5 See id.
- 6 See id.
- 7 Insurers Begin to Reimburse Physicians for Online Visits, [www.ihealthbeat.org/articles/2008/3/31/Insurers-Begin-To-Reimburse-Physicians-for-Online-Visits.aspx?topicID=57](http://www.ihealthbeat.org/articles/2008/3/31/Insurers-Begin-To-Reimburse-Physicians-for-Online-Visits.aspx?topicID=57) (Mar. 31, 2008) (last accessed on Sept. 3, 2008).
- 8 See id.
- 9 45 C.F.R. Part 160 and Part 164, Subparts A and C.
- 10 45 C.F.R. § 160.404.
- 11 42 U.S.C. § 1320d-6.
- 12 42 C.F.R. § 164.312.
- 13 45 C.F.R. § 164.304.
- 14 45 C.F.R. § 164.312 (e)(2) (ii).
- 15 See HIPAA Security Series - Volume 2, Page 4, Centers for Medicare and Medicaid Services; p. 12 (revised 3/2007).
- 16 Washkuch, Jr., Frank, Hackers breach Ohio hospital's databases, obtain personal information of 240,000, SC Magazine (Oct. 30, 2006).