A HIPAA Prospective on Bio-Monitoring and Protecting PHI

Prepared by Kenneth E. Rhea, MD, FASHRM

Brought to you by

DUXWARE™

...LEADING THE WAY IN TECHNOLOGY FOR HEALTHCARE PROVIDERS

www.duxware.com

The Event

On a Tuesday morning of a normal practice day at a Family Medicine clinic the senior physician was beginning a busy schedule. The physician used a Samsung Galaxy III smartphone and had taken necessary security precautions for the phone. During a quick check of his Email he noted that he had received a communication from a person he recognized as a current patient. The patient had sent a message to him explaining that data attached to the Email was actually electronic information from his new bio-monitoring wrist band which he would like the physician to review and which he thought the physician would want to include in his medical record. The physician did not recall ever having had any discussion with the patient about using Email communications nor did he ever recall receiving such a communication in the past from this patient or any other patient. What should he now do with the information?

Bio-Monitoring and Protecting PHI

While some forms of medical bio-monitoring have been in use since as early as 1965 there is no question of what now seems to be an almost exponential increase in the public interest and use of mobile devices to monitor personal health information.[1] As one article pointed out many companies see potential profit and are □ □ vying for control of the fitness data space."[2] Those efforts are producing a variety of devices designed to monitor or record for later use personal health information, e.g. Fitbit, Jawbone UP, Nike+ Fuelband, Withings Pulse etc.[3] Many of these devices including Fitbit allows transmission of medical data for later use to smartphones or computer in some manner, e.g. direct connection USB, Bluetooth, or by NFC.[4]

The short summary would be that personal medical information is being obtained and stored on a variety of very portable mobile devices, e.g. wrist bands etc.[5] The information is then in some cases being transmitted to some other storage device or system by direct or wireless connection and in other cases stored on the device for later download. Transmitted information might be sent to a person's smartphone or possibly to the Internet for later access. Should there be a concern for privacy and security of the information and are there potential liability considerations? The short answers are

"information may, if appropriate explanation is provided, be transmitted by unsecured Email"

 yes and yes dependent on many factors including how the information is being used and by whom.

One common question in considerations of medical information transmission involves a scenario in which a physician receives an unsolicited Email or text message from a patient. The usual expressed physician concern is whether or not there is potential liability by receipt of unsecured health information from the patient. In this scenario there would have been no prior arrangement for receipt of the information from the patient. HIPAA federal privacy and security regulations as of the Omnibus Final Rule (OFR) are clear that should a patient request their medical information being held by a physician the information may, if appropriate explanation is provided, be transmitted by unsecured Email even though there may be some level of risk that the information in the email could be read by a third party. [6] The unsolicited receipt of transmitted health information by a patient is not as clearly addressed. In the scenario of the physician sending requested health information the physician has no responsibility for the information which is protected health information (PHI) either while it is in transit or while in transmission . [7] Nor does the physician have any responsibility for safeguarding information once delivered to the patient.[8] In

"There is no physician responsibility for any information, electronic or otherwise, being held by the patient prior to the information transmission to the physician"

the reverse situation of a patient sending electronic information to the physician in an unsecured format, as would be the case of an unsolicited text message, the physician has no knowledge of what is being sent or even when it is being sent and therefore also has no responsibility for the privacy and security of the information as it was originally stored or while it is being transmitted to the physician.

This very clear physician position, based on many physician questions, seems not to be well understood. There is no physician responsibility for any information, electronic or otherwise, being held by the patient prior to the information transmission to the physician or during information transmission to the physician. Federal regulations define as a part of health information a category of individually identifiable health information (IIHI) when the information meets certain requirements.[9] These criteria in part state that,

- The information must have been collected from an individual
- The information must have been created or received by a health care provider
- The information Relates to the past, present, or future physical or mental health or condition

of an individual; the provision of health care to an individual□ □

- □ The information □ □ identifies the individual□ □ or □ □ there is a reasonable basis to believe the information can be used to identify the individual.□ [10]

"Protected health information requires absolute protection of the information by the physician as a covered entity"

If the patient information meets the threshold for "individually identifiable health information" the information then becomes □ protected health information" (PHI) under federal regulations when, with some exceptions, the information is

- □ Transmitted by electronic media;
- □ Maintained in electronic media; or
- □ Transmitted or maintained in any other form or medium."[11]

Protected health information requires absolute protection of the information by the physician as a covered entity (CE) according to federal regulations. While information held by the physician in the case of sending requested medical information to the patient by Email would be □ protected health information□ the information in the situation of text messaging by the patient does not qualify as PHI. While the information being sent to a physician by the patient might relate to the patient's health care and identify the patient, the physician has not

"collected" the information, has not yet "received" the information, and certainly has not "created" the information.

"a further consideration is the physician position once the information though unsolicited has reached the physician"

Therefore the information being sent by the patient is not protected health information and therefore is not the responsibility of the physician just as the physician has no further responsibility for information that was once protected health information, but has now been sent to the patient by unsecured Email.

However, a further consideration is the physician position once the information though unsolicited has reached the physician. Now the information, though not requested, has been "collected", has been "received by a health care provider", relates to the "condition" of the patient, identifies the patient, and therefore qualifies as "individually identifiable health information".[12] It has been transmitted and now is in some manner being "maintained in electronic media" at least temporarily by the physician, e.g. on a smartphone or computer. [13] The information is now protected health information in the control of the physician.[14] Given these regulations what are the considerations for personal health information collected and stored via bio-monitoring devices such as Fitbit?

Just as with the scenario of a patient sending an unsolicited text message to a physician a patient

"the patient might well be exposing their personal information to third parties"

might send or provide to his/her physician health information collected by a bio-monitoring device either solicited or unsolicited. As in the case of the text message the physician would have no responsibility for the information prior to receipt including during any type of transmission. The patient's collection of their own data on their own mobile device would have no liability implications for the physician though, as others have emphasized, the patient might well be exposing their personal information to third parties during collection, storage, or transmission of the information to their personal devices such as smartphones. There are absolutely reasons for a patient collecting such date to be concerned about privacy and security of the information.[15]

Physicians are beginning to use mobile fitness tracking information to a greater degree allowing physicians to "□ get real-time looks□ " at patient medical information outside the medical office.[16] One author sees such use as □ □ part of the larger trend of marshalling technology to produce better patient outcomes and reduce healthcare costs.[17]

As the usage of the fitness tracking information begins to be a greater part of clinical practice it is not difficult to imagine a scenario of physicians providing such devices to patients and collecting information. A physician might provide a tracking

"As complexity of systems increases there might also be direct transmission of the collected information to the physician's EMR system by the patient"

device to a patient making the physician the owner of the device. The patient's medical and identified information would now be "collected" and "created" by the physician and stored on the bio-monitoring device. The information on the device is now protected health information requiring protection in an acceptable manner by the physician assuring that the information is secure , i.e. information that has been □ □ rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary (HHS)□ □ [18] The protection would extend to information "at rest" on the device and for any data transmission "movement" or "syncing" to other devices prior to access by the physician. As complexity of systems increases there might also be direct transmission of the collected information to the physician's EMR system by the patient in compliance with meaningful use stage 2 Core Objective 17 related to using □ □ secure electronic messaging to communicate with patients on relevant health information".[19]

Patients may or may not be too concerned about the privacy of information they collect on their bio-monitoring devices though there is ample reason to be concerned, but as physicians attempt to improve patient medical care by use of patient bio-monitoring devices the physician's potential violations of privacy and security regulation

increase.[20] Unlike the unsolicited receipt of a patient text message about a medical problem, it is probable that receipt of patient bio-monitored medical information would be planned. Potential liability concerns begin with the receipt of such information and will increase as physicians have deeper involvement in the collection process by providing such devices to patients.

"it will be increasingly necessary for physicians and other healthcare providers to clearly understand the basics of HIPAA regulations"

Attorneys are recognizing many legal ramifications and potential liabilities of such bio-monitoring devices outside of federal privacy and security regulations.[21] From the medical practice perspective it will be increasingly necessary for physicians and other healthcare providers to clearly understand the basics of HIPAA regulations. Specifically as use of monitoring systems increases to understand what constitutes protected health information (PHI) and the application to privacy and security of the information. Failure to recognize the required protection of health information and the relationship to activities such as bio-monitoring can lead to severe problems. [22]

Questions and Answers after the Endnotes section.

(Endnotes)

[1]Budinger T. Wireless Biomonitoring for Healthcare. National Center for Biotechnology Information. Site: www.ncbi.nlm.gov. http://www.ncbi.nlm.nih.gov/books/NBK22846/. Pub. 2005. Accessed December 11, 2014

[2]Crawford K. When Fitbit is the Expert Witness. The Atlantic. Site: www.theatlantic.com. http://www.theatlantic.com/technology/print/2014/11/when-fitbit-is-the-expert-witness/382936/. Pub. November 2014. Accessed December 11, 2014

[3]Ibid

[4]O□Brien T. Fitbit Flex Review. Engadget. Site: www.engadget.com. http://www.engadget.com/2013/05/06/fitbit-flex-review/. Pub. May 6, 2013. Accessed December 11, 2014

[5]Gordon B. 2015 Best Fitness Trackers Review. Top Ten Reviews. Site: www.fitness-trackers-review.toptenreviews.com. http://fitness-trackers-review.toptenreviews.com/. Pub. December 2014. Accessed December 11, 2014

[6] Federal Register. Omnibus Final Rule. Government Printing Office.gov. Final Rule. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p 5634

[7]Federal Register. Omnibus Final Rule. Government Printing Office.gov. Final Rule. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17;p 5634

[8] Ibid

[9] Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text §160.103 Definitions p 15 Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. p 15

[10] Ibid

[11] Ibid p 16

[12] Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text §160.103 Definitions p 15 Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. p 15. Pub. March 26, 2013. Accessed December 11, 2013

[13] Ibid

[14] Ibid p. 16

[15] Zhou W. Security/Privacy of Wearable Fitness Tracking Devices. IEEExplore. Site: www.ieeexplore.ieee.org. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6877073&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6877073. Pub. June 18, 2014. Accessed December 11, 2014

[16] McLeod P. Physicians Use Fitness Trackers to Monitor Patients In Real Time. Dark Daily. Site: www.darkdaily.com. http://www.darkdaily.com/physicians-use-fitness-trackers-to-monitor-patients-in-real-time-even-as-developers-work-to-incorporate-medical-laboratory-tests-into-the-devices-528#axzz3Ld23A4rC. Pub. May 28, 2014. Accessed December 11, 2014

[17]Ibid

[18] Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text §160.103 Definitions p 15 Site hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf. p 71. Pub. March 26, 2013. Accessed December 11, 2013

[19] CMS. Stage 2 Core & Menu Objectives. Site:www.cms.gov. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2Overview_Tipsheet.pdf. Pub 2014. Accessed December 11, 2014

[20] Hixon T. Are Health and Fitness Wearables Running Out of Gas? Forbes. Site: www.forbes.com. http://www.forbes.com/sites/toddhixon/2014/04/24/are-health-and-fitness-wearables-running-out-of-gas/. Pub. April 24, 2014. Accessed December 13, 2014

[21] Crawford K. When Fitbit is the Expert Witness. The Atlantic. Site: www.theatlantic.com. http://www.theatlantic.com/technology/print/2014/11/when-fitbit-is-the-expert-witness/382936/. Pub. November 2014. Accessed December 11, 2014

[22] Federal Register. Omnibus Final Rule. Government Printing Office.gov. Final Rule. http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf. Published 1/25/2013. Vol.78; No.17

Review Questions

Question 1 When unsolicited information is received electronically from a patient by a physician related to the health or medical care of the patient, the physician should:

1. Immediately destroy the information since it cannot be authenticated.

2. Send the information to the Office Manger or EMR Manager for verification of the identity of the patient within the next 24 hours before making any response.

3. Review the information in the communication and if the information is protected health information (PHI) assure necessary protection after which a response can be made based on the degree of urgency.

4. Call the patient immediately and request proof that he/she had actually sent the message.

Answer: 3

If the practice has a policy in place for use of Email or other electronic methods of patient communications, which should be the case, the established protocols should be followed. If no such policies or protocols exist and the unsolicited information is in fact protected health information (PHI) there is a responsibility to protect the information once received while held on the receiving device or otherwise. In the latter situation the information can be transferred to a secure EHR system or destroyed after a discussion with the

initiating patient which should include a request to discontinue any future unsecured transmissions.

Question 2 If a patient of a medical practice at the suggestion of his/her physician gathers personal medical information and electronically stores the information, e.g. blood pressure readings stored on a flash drive or bio-monitoring device the following would apply:

1. The Office Manager or Privacy Officer of the medical practice should periodically, at no less than 30 day intervals, check with the patient on the security of the information being stored since the physician under HIPAA regulations is a Covered Entity (CE), the manager or Privacy Officer is a part of the work force of the practice, and the information is protected health information (PHI),

2. The patient may or may not follow the suggestion of the physician and gather the health information. Storage of the information is at the discretion of the patient and the physician has no responsibility for the method of storage or protection of the information collected.

3. Any electronic storage of personal medical information by the patient should have been approved by the physician since the physician initiated the original request for collection and has an implied obligation under HIPAA regulations to assure privacy as well as security of the information,

4. Since the information would not have been collected unless suggested by the physician, the physician via the medical office is in the position of having initiated collection of health information that

Kenneth E. Rhea, MD, FASHM

Dr. Rhea is a medical liability and risk consultant to medical practices and other health related organizations. He was in medical and surgical practice for over 30 years and for the past 17 years has been a consultant in medical risk and liability management. He is the owner and Managing Partner of Medical Education and Risk Consulting, called MER Consulting. Dr. Rhea has been dealing with risk and federal regulatory compliance areas such as the HIPAA privacy and security regulations beginning with the Privacy Rule in 2000.

Dr. Rhea writes monthly white papers on various sections of the HIPAA regulations in regard to those most encountered in office practice. The information will be summarized from actual federal law with both references and multiple choice questions for your teaching use.

HIPAA training is required by the regulations must be ongoing and this monthly information can be used as part of efforts to meet those requirements. These HIPAA articles can be used and documented as part of your staff and administrative training program.

While these educational materials will not by any means cover everything you need to do for HIPAA privacy and security compliance they provide more documented evidence of training and intent to comply.

If you have any questions on the information Dr. Rhea can be contacted directly. krheamd@mdriskconsulting.com

 relates to the past, present, or future physical or mental health or condition of an individual; and therefore should assure under HIPAA regulations the proper electronic storage consistent with information maintained in electronic media .

ANSWER: 2

It was a only a suggestion. There is no responsibility to monitor compliance or methods of collection outside of reasonable efforts to assure patient understanding of information provided in the medical office.