Risk Rx

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Vol. 7 No. 3 July—September 2010

UF HSC Self-Insurance Program

BREACHES OF UNSECURED PHI AFTER HITECH: A SUGGESTED FRAMEWORK FOR INVESTIGATION

Barry S. Herrin, FACHE and
Allyson Labban
Smith Moore Leatherwood LLP

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), enacted by Congress as a part of the American Recovery and Reinvestment Act of 2009, places a duty on covered entities to notify patients, the Secretary of the Federal Department of Health and Human Services ("HHS") and, in some cases, the media, of any breach of unsecured protected health information ("PHI"). Because of this obligation, it is important that health care providers develop internal systems for investigating potential breaches of unsecured PHI. While every breach of unsecured PHI is an impermissible disclosure under HIPAA, not every impermissible disclosure is a breach. Being able to tell the difference between the two will help you avoid unnecessary, embarrassing, and potentially costly notification requirements and penalties.

"Unsecured protected health information" is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of encryption technologies or methods of physical destruction approved by the Secretary of HHS. Approved technologies and methods are listed at 74 Fed. Reg. 42742 and will be updated as needed on the HHS website. Currently approved encryption technologies and destruction methodologies are outlined in the National Institute of Standards and Technology ("NIST") Special Publications 800-111, 800-52, 800-77, 800-113, and 800-88, available at http://www.csrc.nist.gov/. Keep in mind that HITECH's breach and notification requirements cover both paper and electronic records: this is not just an expansion of the HIPAA Security Rule.

A breach of unsecured protected health information occurs where (1) the PHI is acquired, accessed, used, or disclosed in a manner not permitted under the HIPAA Privacy Rule (45 C.F.R. § 164.500, *et seq.*); and (2) that compromises the security or privacy of the protected health information. The security or privacy of the information is compromised for the purpose of this analysis where the acquisition, access, use, or disclosure of the information in question poses a significant risk of financial, reputational, or other harm to the individual whose protected health information is impermissibly acquired, accessed, used, or disclosed.

Any time a covered entity or business associate discovers an unauthorized acquisition, access, use, or disclosure of PHI, the covered entity or business associate should evaluate whether the acquisition, access, use, or disclosure fits within the definition of "breach." In order to determine whether a breach of unsecured protected health information has occurred, therefore, you should apply the following analysis:

(1) *Determine if the information is unsecured PHI.* If no, the investigation ends.

(2) *If the information involved is unsecured PHI, determine if the use or disclosure is permitted under the HIPAA Privacy Rule.* If yes, the investigation ends.

(3) *If the information involved is unsecured PHI and the use or disclosure was impermissible under the*

HIPAA Privacy Rule, determine whether the use or disclosure fits within one of the HITECH Act's three exceptions. If yes, the investigation ends.

(4) If it still appears that a potential breach occurred, determine whether the acquisition, access, use, or disclosure poses a "significant risk" of financial, reputational, or other harm to the individual. If no, there is no duty to provide notice as contemplated by HITECH.

In conducting this analysis, imagine yourself in a long, door-lined hallway. Each of the steps above corresponds to a door. If at any point you try the door handle and it opens, you can exit the hallway and avoid the breach notification requirements. If, however, you reach the end of the hallway without being able to exit out any of the side doors, you will be subject to HITECH's breach notification requirements. The process we outline in this article helps you make sure that no door handle goes untried.

STEP 1: Is the Information Unsecured PHI?

If the information in question was rendered unusable, unreadable, or indecipherable to unauthorized individuals through an approved process of encryption or through destruction of the information through shredding, burning, purging, or other approved method, then no breach occurred.

Additionally, the unauthorized acquisition, access, use, or disclosure is not a breach if the information meets any one of the following three (3) criteria:

(1) It is individually identifiable health information held by the covered entity or business associate in its capacity as an employer. For example, workers' compensation information on a hospital's employee would contain health information, but it would not be subject to these provisions.

(2) It is PHI that does not include any of the following:

i. the identifiers listed at 45 C.F.R. § 164.514(e)(2) ((1) names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/ license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images);

ii. the patient's date of birth; and

iii. the patient's zip code.

(3) It is information that has been "de-identified" in accordance with the HIPAA Privacy Rule.

If the information that has been acquired, accessed, used, or disclosed meets any of the above criteria, then the analysis ends, and no breach of unsecured PHI has occurred. Be aware, however, that the acquisition, access, use, or disclosure may still be impermissible under HIPAA.

STEP 2: Is the Acquisition, Access, Use or Disclosure Permitted Under HIPAA?

A breach is an *impermissible* acquisition, access, use, or disclosure of unsecured PHI. Therefore, if the use or disclosure is permitted under the HIPAA Privacy Rule, no breach occurred. Additionally, not every violation of the HIPAA Privacy Rule constitutes a breach. The HIPAA violation must result in the otherwise impermissible acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the protected health information.

<u>STEP 3</u>: Does the Acquisition, Access, Use or Disclosure Fit Within One of the Exceptions to HITECH?

Even if the information in question is unsecured PHI and the acquisition, access, use, or disclosure is not permitted under the HIPAA Privacy Rule, the use or disclosure may fit within one of the three narrowly construed disclosure exceptions in the HITECH Act. The exceptions are as follows:

(1) The unintentional access to, acquisition or use of protected health information by a workforce member acting in good faith and within the course and scope of his or her regularly assigned duties for the covered entity or for a qualified business associate of the covered entity, if it does not result in any further use or disclosure of the protected health information in a manner not permitted by the HIPAA Privacy Rule.

- EXAMPLE: A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse to the misdirected e-mail, and then deletes it without further using or disclosing it. ***The exception applies.***

- EXAMPLE: A member of a hospital's medical staff deliberately looks at information related to his ex-spouse's care in the hospital. Even though the medical staff member might have general access to information of this type, he or she is not the attending or consulting physician. ***The exception does not apply.***

(2) The inadvertent disclosure of protected health information from one workforce member at the covered entity or at a qualified business associate of the covered entity to another workforce member at the covered entity or at the same qualified business associate where all are authorized to access the information, when such protected health information is not subsequently used or disclosed by the recipient in a manner that violates the HIPAA Privacy Rule.

- EXAMPLE: An inadvertent disclosure by a member of a hospital's medical staff, even if that medical staff member is not a hospital employee, to a hospital employee who is authorized in the usual conduct of his or her duties to receive any type of protected health information, provided that the recipient does not subsequently inappropriately use or disclose the information. ***The exception applies.***

(3) An unauthorized disclosure to an unauthorized person of protected health information, if there is a reasonable good faith belief that the recipient would not

(4) reasonably have been able to retain the information.

- EXAMPLE: A nurse mistakenly hands Patient A the discharge instructions for Patient B. Realizing her mistake, the nurse retrieves the protected health information before Patient A has a chance to review the information. ***The exception applies***.

If one of these exceptions applies, the acquisition, access, use, or disclosure is not a breach for purposes of the HITECH Act. It is important to remember that every breach of the HIPAA Privacy Rule does not constitute a reportable "breach" under HITECH. However, a breach of the Privacy Rule is still a breach of the Privacy Rule and needs to be dealt with in your usual manner. Do not make the inappropriate assumption that your ordinary human resource and privacy policies no longer apply simply because HITECH now has a different definition of "breach" for notice purposes.

<u>STEP 4</u>: Does the Acquisition, Access, Use, or Disclosure Result in a Significant Risk of Harm to the Patient?

Steps 1-3 of the analysis are fairly straightforward, black-and-white questions. Step 4 of the analysis, however, requires a "gut check" weighing of various subjective factors. For this reason, it is absolutely critical that you document your reasoning and the justification for your ultimate determination regarding the risk of significant harm to the patient.

There are a set of guidelines to keep in mind when conducting a step 4 analysis. In evaluating whether significant risk of financial, reputational, or other harm may result from the use or disclosure, the following factors are significant:

(1) To whom was the information disclosed/by whom was the information used?

For example, if the information was disclosed to another covered entity or organization that is governed by HIPAA, or to a Federal agency that is required to follow federal privacy regulations, the risk of harm to the individual is fairly low. However, if the information was stolen or disclosed to a person or entity that has no obligations of privacy, the risk is great.

(2) What steps were taken to mitigate the impermissible use or disclosure?

For example, if the covered entity or business associate took immediate steps to mitigate the impermissible use or disclosure, such as retrieving the information from the recipient and obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed, the risk of harm may be low.

(3) What type of information was the subject of the impermissible use or disclosure?

Disclosure of basic demographic data, such as the patient's name and address, is likely low risk, unless the nature of the patient's disease or treatment can be determined. For example, if the information clearly originated from a substance abuse clinic, AIDS treatment facility, or mental health center, there is a high risk of significant harm.

If there is no significant risk, the investigation concludes. If, however, a significant risk is determined to exist, a breach has occurred and the HITECH Act notification requirements must be followed.

There are two examples of disclosures in which harm is presumed to occur. First, any disclosure of information involving sexually transmitted diseases (including HIV/AIDS status) is presumed to create a significant risk of reputational harm. Second, if a medical record deals with abuse of the patient and the name of the alleged abuser is contained in the record that is the subject of the breach, such a breach is presumed to create a significant risk of reputational harm.

We encourage providers to develop a privacy/investigation team whose job it is to evaluate whether an acquisition, access, use, or disclosure of PHI is in fact a breach. Representatives from risk management, the Privacy Officer, the Security Officer (if electronic PHI is involved) and clinicians are all suitable candidates for the team. When setting up your team, it is a good idea to bring together a range of viewpoints and backgrounds so that you can be satisfied that the potential for significant harm has been considered from all points of view and knowledge bases. Also, as noted above, it is essential that your privacy/investigation team document its step-by-step analysis and the justification for its decisions. You also want to be sure to properly train your frontline staff and provide a notification procedure whereby staff members can notify the privacy/investigation team whenever a suspected breach of unsecured PHI has occurred. Staff members should be reminded of the risks posed by electronic mail, fax machines, and any form of portable device, such as PDAs and jump drives. Finally, you should work with your IT staff to evaluate the feasibility of encryption of electronic data, and to ensure that documents and files are being destroyed in compliance with the approved destruction methods.

The investigational process we outline here is akin to word problems in fifth grade mathematics: you only get full credit if you show your work. Documentation of the process, and particularly the analysis of the risk of harm in Step 4, will be critical in defending providers against claims that alleged breaches should have been reported to the government and the media. You should also consider requiring your business associates to adopt similar processes and to notify you if any alleged breach reaches Step 3 of this analysis. We think the providers, and not their contractors, should be making the final decision about whether an alleged breach is one that requires reporting or not.

Overcoming Prescribing Errors Not a Bitter Pill

Georgette Samaritan, RN, BSN

Reprinted with permission from MAG Mutual Insurance Company, Healthcare Risk Manager, Volume 12 / Number 13 - 2006

Medication prescribing errors occur all too frequently. A few key items can spell disaster on a prescription pad: a patient's changing or declining kidney function, a patient's documented drug allergy, the wrong drug name or abbreviation, incorrect dosage calculations, and unusual or critical dosage/frequency considerations. These contributing factors are relatively easy to recognize, and most of the time easy and inexpensive to fix.

The Malpractice Experience

The Physician Insurers Association of America (PIAA) Data Sharing Reports identify "**prescription of medication**" as the second most frequent and second most expensive procedure in claims against physicians insured by PIAA member companies like MAG Mutual.

A 2006 PIAA report reveals that the medical specialties with the highest number of medication-related claims were Family Practice and Internal Medicine. Family Practice and Internal Medicine also had the highest total indemnities paid of all specialties.

A claims analysis conducted by the Harvard Risk Management Foundation (RMF), found that medication-error claims closed with payment more frequently than all claims, and that the payments were substantially higher.

Regarding classes of drugs most frequently involved, the study found that more than 60 percent of alleged errors in liability claims were associated with the following five drug groups:

- Antibiotics
- Anticoagulants
- Steroids
- Narcotics
- Cardiovascular drugs

These findings are similar to those reported by the PIAA in its 1993 Medication Errors Study.

Types and Causes of Errors

According to the PIAA, the greatest risk in prescription errors is for the physician rather than the pharmacist. The predominant root cause of prescribing errors is a lack of knowledge about the drug to be administered, as well as a lack of detailed and timely information about the patient who is to receive the drug. Patients with kidney conditions, liver conditions, or known drug allergies are at great risk.

An Institute of Medicine (IOM) report cites the following factors as causal in medication errors:

- Failure to alter a medication or dosage due to patient's reduced kidney or liver function
- Known allergy to same medication class
- Using the wrong drug name, dosage form or abbreviation
- Incorrect dosage calculation and decimal point misplacements
- Atypical or unusual and critical dosage frequency considerations

Low-Cost, Common-Sense Initiatives to Reduce Errors in Prescription Writing

- Prescribers should print prescriptions clearly
- Prescription orders should include a brief notation of purpose (e.g. for cough), unless considered inappropriate by the prescriber
- All prescription orders should be written in the metric system except for therapies that use standard units such as insulin, vitamins, etc.
- Units should be spelled out rather than writing "U"
- Prescribers should include age and, when appropriate, weight of the patient on the prescription or medication order
- The medication order should include drug name, exact metric weight or concentration and dosage
- A leading zero should always precede a decimal expression of less than one. A terminal or trailing zero should never be used after a decimal

- Review and post the ISMP's List of Error-Prone Abbreviations, Symbols and Dose designations: Remind all prescribers to avoid the use of abbreviations including those for drug names, like MOM, HCTZ and Latin directions for use
- Prescribers should not use vague instructions such as "take as directed" or "take/use as needed" as the sole direction for use

- Recognize the need for dose adjustment in children and elderly patients
- Recognize the hazards of polypharmacy, drug/drug interactions and possible adverse effects
- When co-managing patients with other physicians, make sure that the individual areas of Responsibility are clearly documented in the patient's record (e.g., who is managing the dosage and monitoring the response or complications)
- Encourage patients with multiple physicians, prescriptions or complicated medication regimens to use **one** pharmacy
- Ensure ongoing physician education on new drugs, new uses, unusual uses, etc. and use guidelines from professional organizations
- Instruct staff to always verify questionable or illegible orders with the prescribing physician and encourage staff to ask questions

Verbal or Telephone Orders

Verbal or telephone orders present special problems. They can easily be misheard or misinterpreted, transcribed incorrectly, or not recorded in a patient's chart. They may also be incomplete and confusing. Ideally, verbal orders should be accepted only in emergency situations. Physician's offices should institute a firm policy for regulating verbal or telephone orders. Include the following:

- Ensuring that a caller is properly identified as the individual's physician or other authorized prescriber. Some facilities may use a password/code system to authorize prescribers
- Identifying the patient
- Ensuring that the prescriber is available by phone or other means to confirm or clarify an order if questions arise
- Ensuring that the order is recorded in the chart immediately and later authenticated by the authorized prescriber within a stated amount of time
- Ensuring that recipients verify the order by reading it back as it is written. The patient's record should document that the order was "repeated and confirmed"
- Spelling out all drug names, however simple, and specifying doses carefully

References

PIAA Data Sharing Project, June 2006
Dwyer K, Medication-Related Malpractice Claims, Forum 1998 Fall:19 (4):4-7
Medication Error Study. Physician Insurers Association of America,Washington,
DC. June 1993.
Institute of Medicine (IOM), "To Err Is Human: Building a Safer Health System".
2000, online
Bettman JW. Seven Hundred Medicolegal Cases in Ophthalmology.
Ophthalmology. 1990; 97: 1379-84.
National Coordinating Council for Medication Error Reporting and Prevention
(NCC MERP) c/o U.S. Pharmacopeia NCC MERP Secretariat 12601 Twinbrook
Parkway Rockville, MD 208052 (301) 816-8265, www.nccmerp.org
Institute for Safe Medication Practices, Suite 810, 1800 Byberry Road, Huntingdon
Valley, PA 19006 (215) 947-7797, www.ismp.org

Risk Rx

UF UNIVERSITY of FLORIDA
The Foundation for The Gator Nation

Send comments and/or article suggestions to: rmeduc@shands.ufl.edu

To see Risk Rx archives, log on to:
http://www.sip.ufl.edu/riskrx.php