THE ROZOVSKY GROUP, INC.
RMS RISK MANAGEMENT SERVICES
OneBeacon PROFESSIONAL INSURANCE™
NEWSLETTER

Volume Ten - Number Two **February 2014**

Is Strict Liability Next for a Purposeful Data Breach?

"A hospital should owe a duty to keep a patient's health information confidential, and a hospital should be directly liable for its own failure to prevent breaches of confidentiality by employees who act outside the scope of their employment."[1]

It was not the first time that a healthcare professional gave into the inquisitive urge to view a patient's electronic health record without authorization to do so. Indeed, it was not the first time that such behavior became the basis for litigation.[2]

What was different was the nature of the legal inquiry:

> "Whether, under New York law, the common law right of action for breach of the fiduciary duty of confidentiality for the unauthorized disclosure of medical information may run directly against medical corporations, even when the employee responsible for the breach is not a physician and acts outside the scope of her employment?"[3]

The question was certified to the New York Court of Appeals by the United States Court of Appeals for the Second Circuit.[4] The response of the highest court in New York, and a related dissenting opinion, that may help legal counsel and risk management professionals alike, focus on what might be the "800-pound elephant" in the healthcare entity: will courts recognize strict liability for intentional breaches of confidential health information by a colleague acting beyond the confines of his or her employment? Perhaps the answer is less one of "if" and

more of a "when." The prospect of such litigation merits important legal and risk management initiatives.

The New York Case.

J.D. was receiving treatment at G.C., a private medical clinic. The treatment provided was for a sexually transmitted disease. One of the employed nurses at the clinic recognized J.D. as being her sister-in-law's boyfriend. The nurse accessed J.D.'s medical record and learned that he was receiving care for a sexually transmitted disease. As J.D. was waiting for treatment, the nurse sent some text messages to her sister-in-law telling her about J.D.'s condition. The sister-in-law in turn forwarded these messages to J.D. He asserted that the messages suggested that staff at the medical clinic were making fun of his medical condition.[5]

J.D. called the medical clinic five days later to complain about the nurse's behavior. J.D. met with the administrator of the medical clinic and the nurse was fired from her job. Subsequently, J.D. received a letter from the President and CEO of G.C. who confirmed that there had been an unauthorized disclosure of J.D.'s confidential health information. The correspondence noted that the clinic had taken "appropriate disciplinary actions"[6] and that measures had been implemented to prevent similar breaches in the future.[7]

J.D. filed a lawsuit in federal court in which he alleged eight causes of action:

> "(1) common law breach of fiduciary duty to maintain the confidentiality of personal health information, (2) breach of contract, (3) negligent hiring, training, retention and/or supervision of employees, (4) negligent infliction of emotional distress, (5) intentional infliction of emotional distress, (6) breach of duty to maintain the confidentiality of personal health information under *New York CPLR § 4504*, (7) breach of duty to maintain the confidentiality of personal health information under *New York Public Health Law § 4410*, and (8) breach of duty to maintain the confidentiality of personal health information under *New York Public Health Law § 2803-c*."[8]

The U.S. District Court for the Western District of New York dismissed all the claims.[9] J.D. appealed the ruling as to the first five bases for claim. The U.S. Circuit Court of Appeal for the Second Circuit affirmed the decision to dismiss four of the five causes of action. It reserved making a decision on the claim for

breach of fiduciary duty. The appellate court certified the question to the New York Court of Appeal.[10]

In addition to these legal proceedings, the Second Circuit issued another decision that involved the actions of the fired nurse. In this ruling, the Second Circuit found that the actions of the fired employee were not foreseeable to the defendants and that her actions were not within the scope of her employment. Indeed, the court noted that in his complaint J.D. alleged that the nurse was motivated by personal reasons that were not related to treatment provided to J.D. Thus, the court determined that the wrongful actions of the nurse could not be imputed to the defendants on the basis of respondeat superior.[11]

The federal court then certified the question to the New York Court of Appeal:

> "whether [J.D.] may assert a specific and legally distinct cause of action against defendant for breach of the fiduciary duty of confidentiality, even when respondeat superior liability is absent."[12]

The New York Court of Appeal noted that in general terms a hospital or a medical corporation could be held vicariously liable for the wrongful acts of an employee. Under the legal principle of respondeat superior the employer is responsible for the employee's wrongful acts only when those actions further the employer's business and occurred within the scope of the individual's employment. Actions that take place outside the scope of employment generally mean that the hospital or medical corporation is not liable in such cases.[13]

The New York Court of Appeal discussed the notion of an employer having a "heightened duty"[14] of care for employee misconduct. Referencing earlier case precedent, the New York high court rejected a heightened obligation on the part of a hospital.[15]

The court went further, expressly rejecting a plaintiff's suggestion that the court impose absolute liability of the medical corporation for the wrong actions of the nurse disseminating confidential patient medical data. The actions of the nurse were not reasonably foreseeable and occurred beyond the scope of her employment. However, the court noted that the plaintiff had another recourse, namely to sue the employer in a direct rather than vicarious cause of action for negligent hiring and negligent supervision. Also, the medical corporation could be held liable for the failure to establish

> "adequate policies and procedures to safeguard the confidentiality of patient information or to train their employees to properly discharge their duties under these policies and procedures. These potential claims provide the requisite incentive for medical providers to put in place appropriate safeguards to ensure protection of a patient's confidential information."[16]

Having noted that these possible causes of action had been resolved by the federal courts, the court chose not to address these bases for claim. Instead, it ruled that the certified question should be answered in the negative.[17]

Observations on the New York Court of Appeal Ruling.

Given the legal precedent established in earlier cases, the court's ruling was quite understandable. The ability to foresee abhorrent employee behavior is a challenge for a hospital or medical corporation. Nurses and other care providers are provided orientation and in-service training about maintaining confidentiality of patient health information. Nurses are expected to follow well-recognized standards of professionalism and ethics to refrain from disseminating patient information to unauthorized individuals.

One can understand that a hospital or medical corporation should reasonably foresee professional conduct on the part of nurses with access to protected patient health information.

One justice of the New York Court of Appeal disagreed with the underlying basis for the majority ruling. For Justice Rivera, writing in dissent, the court's ruling served to limit J.D.'s ability to seek recompense when a medical corporation failed to protect confidential medical information. As the dissenting justice suggested:

> "I believe that a medical corporation's duty extends beyond an employee's conduct within the scope of employment, and I would answer the certified question in the affirmative."[18]

For Justice Rivera, the court's decision undermined public policy on confidentiality of patient information in medical records as reflected in the New York Public Health Law.[19]

Justice Rivera pointed out that

> "A cause of action directly against a medical corporation, unhampered by questions as to whether an employee's conduct occurred within the scope of employment, *ensures the fullest protections for patients* and best addresses the current realities of medical service delivery."[20] [Emphasis added]

Justice Rivera took the position that a hospital should be "directly liable" when it failed to prevent breaches of confidentiality by employees whose actions take place outside the scope of their employment. As he concluded:

> "In order to protect the patient's privacy interests given the competing need to disclose, such a cause of action would provide a powerful incentive to medical corporations to implement protections against disclosures. Given the highly personal nature of medical data at risk of disclosure, the harm associated with dissemination of such sensitive private information, the ease with which employees of a medical corporation may access confidential data disseminate it through the use of a commonly held and inexpensive device, a cellular telephone, and the inability of patients to protect themselves from employee misconduct, such an incentive furthers the State's public policy in protecting the confidentiality of medical records."[21]

One can understand Justice Rivera's frustration about the ease with which patient medical record confidentiality may be breached using a handheld device. However, creating what the majority termed "absolute liability" is not a practical solution.

The burden of liability in strict or absolute liability falls on the shoulders of the medical corporation, not the individual acting improperly.

Certainly, organizational culpability is on the table if the facility does not offer training, establish appropriate safeguards and enforce policy and procedures. But if all those mechanisms are in place perhaps the more appropriate safeguard is professional misconduct proceedings that lead to removal of a person's ability to practice as a healthcare professional. Further, intentional, wrongful actions destined to cause harm to a patient might serve as the context for criminal charges against the healthcare professional. If the interest is in incentivizing good practices, de-licensure and criminal proceedings against the unruly individual may go a long way to promote a public policy focused on safeguarding confidentiality of patient medical information.

Risk Management Strategies to Reduce Intentional Data Breach by Staff.

There is little doubt that inadvertent or unintentional data breaches by staff are a source of frustration and disappointment for senior leadership. Resources expended on orientation, training and in-service programs are geared to reducing the likelihood of such patient health information data breaches. When, however, patient health information is disseminated intentionally without authorization, the reaction may go to the core of the hospital or medical corporation, questioning systems and processes intended to prevent such breaches. Strategies intended to reduce the likelihood of an intentional data breach include the following:

1. **Complete a Security Assessment of Patient Health Information Systems.**
   Conduct a thorough security review of patient health systems, taking into consideration authorized access, penetration testing, and the ability of personnel to copy or forward patient health information behind the organization. Use the result of the assessment to make necessary changes to enhance data security.

2. **Implement a "Lock Down" Response After Unauthorized Patient Health Information Access.**
   Use data security surveillance methods to identify and block unauthorized access to patient health information. Work with IT professionals to identify the source of attempted unauthorized access. Communicate findings to the privacy officer, compliance officer and human resources. Recognize the utility of establishing role-based access control on all protected health information and other sensitive data – so that only those with a "need to know" can obtain access.

3. **Implement a Zero Tolerance Approach to Unauthorized Access to Patient Health Information.**
   Work with the compliance officer and legal counsel to develop and implement a so-called "Zero Tolerance" policy for any care provider or employee who intentionally accesses or attempts to gain access to patient health information without permission to do so. Build the "Zero Tolerance" policy language into the employee handbook and employment contracts.

4. **Offer Orientation and In-Service Education.**
   Build into orientation and regular in-service training information on the "Zero Tolerance" policy toward intentional unauthorized access to patient health information. Provide case examples to highlight the consequences for the individual who engages in such practices.

5. **Restrict Use of Personal Communication Devices.**
   Recognizing that data obtained improperly from patient health information systems may be subject to repurposing or transmission on a personal communication device (smartphone, tablet, or computer), consider imposing limitations on the use of such personal devices while on duty in the workplace.

6. **Respond Promptly to Unauthorized Access to Patient Health Information.**
   Have a response plan in place for managing known or suspected situations involving intentional, unauthorized access to patient health information by staff. Include in the response the ability to stop further unauthorized data dissemination, investigation, evaluation of the extent of the breach, notification requirements and use of the "Zero Tolerance" policy for confirmed situations.

Conclusion.

Patient safety and integrity of health information systems are integral components to a quality healthcare delivery system. Improper use of patient health information can have a ripple effect. Once it is known to have occurred, a hospital or medical corporation might face reduced market share. Regulatory scrutiny should be anticipated. Patients may be reluctant to share important information based on a concern about confidentiality of their data.

When a staff member intentionally disseminates patient health information outside the system without permission to do so, the response should be severe and prompt. Even in an organization following Just Culture principles, the intentional act merits a response commensurate with the harm caused, including job termination and notification to applicable professional licensure bodies.

Taking such an approach may seem harsh. However, it is likely to be a strong deterrent to others attempting such actions in future. Further, it places accountability on the perpetrator of the wrongful behavior and not the

organization that tried to avoid such practices. The dissenting opinion in the New York Case suggested a shift to strict liability making the health care organization liable for the intentional acts of the healthcare professional. Such an approach seems imprudent, as it does not focus on the wrongful intentional behavior of a healthcare professional that should know better than to use their position in the organization to intrude on the rights of a patient.

If you would like assistance in developing a breach-prevention risk management program please contact us:

www.therozovskygroup.com
or
(860) 242-1302

[1] J.D. v. G.C.L., 2014 NY LEXIS 2, 16 (No. 224, Court of Appeals of New York, January 9, 2014).
[2] C.Y. v. F.C., N.P., 767 N.W.2d 34 (Minn.App. 2009). To read an analysis of the case See, "Social Networking Gone Wrong," in *Dialogues in Healthcare,* Volume 4, No. 1, January, 2010.
[3] J.D., v. G.C.L, supra note 1.
[4] See, J.D. v. G.C.L., 710 F.3d 492; 2013 U.S. App. LEXIS 5935 (March 25, 2013).
[5] J.D., v. G.C.L., supra note 1 at 2.
[6] Id.
[7] Id.
[8] Id. at 3.
[9] 2012 U.S. Dist LEXIS 20507 [U.S. Dist. Ct. WD NY, February 17, 2012].
[10] J.D., v. G.C.L., supra note 1 at 3, referencing 519 Fed Appx 719 (2d Cir 2013).
[11] J.D., v. G.C.L., supra note 1 at 3, reference 710 F.3d 492 (2d Cir. 2013).
[12] Id.
[13] J.D., v. G.C.L., supra note 1 at 5.
[14] Id.
[15] Id at 5-6. The court referenced its ruling in N.X. v. Cabrini Medical Center, 739 N.Y.S.2 348 (2002). In that case the court ruled:
"A hospital has a duty to safeguard the welfare of its patients, even from harm inflicted by third persons, measured by the capacity of the patient to provide for his or her own safety . . . . This sliding scale of duty is limited, however; it does not render a hospital an insurer of patient safety or require it to keep each patient under constant surveillance . . . . As with any liability in tort, the scope of a hospital's duty is circumscribed by those risks which are reasonably foreseeable."

[16] J.D., v. G.C.L., supra note 1 at 8.
[17] Id.
[18] Id.
[19] Id. at 9, referencing N.Y. Pub. Health Law §28030c [1][3][f].
[20] J.D. v. G.C.L., supra note 1 at 9.
[21] Id. at 14-15.

