Health Information Compliance Alert

Enforcement News: Does Your Employee Confidentiality Policy Violate The NLRA?

Plus: Healthcare breaches due to criminal attacks are on the rise.

Even if your employee's conduct violates HIPAA, that doesn't mean terminating that employee won't still violate the National Labor Relations Act (NLRA).

In Rocky Mountain Eye Center, P.C. and International Union of Operating Engineers, Local 400, an administrative law judge (ALJ) decided that despite the employer's "unquestionably legitimate" HIPAA compliance concerns, the employer "seized upon" those concerns to prevent union activity.

Rocky Mountain Eye Center, P.C. (RMEC) in Missoula, Mont. entered into a confidentiality agreement with its employees, stating that employee information is confidential and that breach of "patient or facility confidentiality" may be grounds for termination, according to a May 18 blog posting by **Valerie Breslin Montague** for the law firm **Nixon Peabody LLP.**

When an RMEC employee, **Britta Brown,** used RMEC's data management system to locate colleague contact information, which she sent to a union representative with whom she was discussing organizing efforts, RMEC terminated Brown, Montague explained. RMEC's stated reason for terminating Brown was for providing protected health information (PHI) to a third party in violation of HIPAA and the RMEC confidentiality agreement.

But the ALJ decided that instructions to employees and the practice of using the data management system to access employee contact information removed the confidentiality protections for such information, Montague said. Also, this "precluded RMEC from using the defense that the employee's actions merited discipline under HIPAA."

Moreover, RMEC's confidentiality agreement violated the NLRA because of its overly broad prohibition on discussing employee information without an exception protecting employees' NLRA rights. Under the NLRA, individuals have a right to:

- Form, join, or assist a union;
- Choose representatives to bargain with the **National Labor Relations Board** on an individual's behalf;
- Act together with other employees for an individual's benefit and protection; and
- Choose not engage in any of these protected activities.

As a result of the decision, the ALJ ordered REMC to (among other things):

- Rescind or modify its unlawful confidentiality agreement, to the extent that the agreement prohibits employees from discussing and disclosing information about other employees;
- Offer Brown full reinstatement to her former job or, if that job no longer exists, to a substantially equivalent position, without prejudice to her seniority or any other rights or privileges previously enjoyed; and
- Repay Brown for any loss of earnings and other benefits suffered as a result of the discrimination against her.

Takeaway: "Employers who are HIPAA covered entities or business associates should consider the requirements of both HIPAA and the NLRA when faced with actions that involve both PHI and unionizing activity, and should take care to segregate employee data from patient PHI," Montague advised. "In addition, employee confidentiality policies must not

be so restrictive as to impede upon an employee's NLRA rights."

Link: For more on the RMEC decision, go to www.nlrb.gov/case/19-CA-134567.

Watch Out For Criminal Breach Attacks Above All Else

Criminal attacks are now the leading cause of healthcare data breaches. So says the Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data by the **Ponemon Institute** and sponsored by **ID Experts.**

Over the last five years, criminal attacks on healthcare data have increased by 125 percent, according to the study's findings released on May 7. Employee negligence and lost or stolen devices still result in many data breaches, but "one of the trends we are seeing is a shift of data breaches from accidental to intentional as criminals are increasingly targeting and exploiting healthcare data," Ponemon stated.

Ponemon expanded the study this year to include business associates (BAs), providing a better insight into the impact third parties have on healthcare data privacy and security. And 91 percent of studied healthcare organizations and 59 percent of BAs experienced a data breach. Half of all healthcare organizations and BAs have little or no confidence that they have the ability to detect all patient data loss or theft, the study found.

Cyber criminals are well aware that healthcare organizations manage a treasure trove of financially lucrative personal information, but at the same time do not have the resources, processes and technologies to prevent and detect attacks, Ponemon posited. To receive a copy of the study, go to www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data.

Beware Of Patient Safety Concerns With Lackluster Data Integrity

Data integrity ranked second in the **Emergency Care Research Institute's** (ECRI) top 10 patient safety concerns for healthcare organizations in 2015.

The ECRI's Patient Safety Organization (PSO) recently issued its "top 10" list of safety concerns for a wide range of healthcare settings, including hospitals, physician offices and nursing homes. For data integrity, ECRI specified safety concerns involving:

- Incorrect or missing data in electronic health records (EHRs) and other health IT systems;
- Insufficient testing of EHR systems; and
- Insufficient checks and balances to identify and address missing or incorrect data.

Other patient safety concerns on the top 10 list included alarm hazards, patient violence, mix-up of IV lines, care coordination events, failure to conduct independent double checks, opioid-related events, inadequate reprocessing of endoscopes and surgical instruments, inadequate patient handoffs, and medication errors.

Link: The top 10 list is available at www.ecri.org/PatientSafetyTop10.

Your Liability Insurer Won't Pay For All Breaches

If your liability insurance company thinks that a costly breach was your own fault, it might want you to reimburse the money spent on your claim.

Case in point: In December 2013, **Cottage Health System,** which operates several hospitals in southern California, suffered a relatively small data security breach due to hacking, according to Consumer Affairs. The breach involved the protected health information (PHI) of 33,000 Cottage Health patients becoming exposed on the Internet.

In 2014, former patients filed a class-action lawsuit against Cottage Health, charging that Cottage Health and **inSync** (the company responsible for putting the health system's records in a secure online location) "failed to provide any encryption or other security to prevent anyone from reading the medical records." The lawsuit also alleged that Cottage

Health failed to use proper encryption or other security measures, which violated the California Medical Information Act.

Cottage Health then filed a claim with its insurer, **Columbia Casualty.** But on May 7, 2015, Columbia filed a lawsuit against Cottage Health in the **U.S. District Court for the Central District of California** to recoup what it paid out to settle the data breach class action lawsuit against Cottage Health.

Columbia issued a cyber-liability policy to Cottage Health that provided coverage for a variety of cyber-related risks, according to a May 21 analysis by the law firm **Manatt, Phelps & Phillips, LLP.** The policy contained an exclusion that stated: "Any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing ..."

Columbia claims that Cottage Health's failure to continuously implement the procedures and risk controls identified in its coverage application caused the improper disclosure of patient medical records, Manatt explained. Therefore, Columbia argued that the exclusion applies in this case to preclude coverage for the class action.

Significance: This case is one to watch, because "Cottage Health is one of the first cases nationwide if not the first case in which the scope of a 'best practices' or 'minimum required practices' exclusion within a modern cyber insurance policy is being tested," Manatt stated. "This case could go a long way in determining the value of cyber policies to many current and potential purchasers."

Impact: If you purchase a cyber policy, you must read through the terms carefully "to fully appreciate the potential breadth of these exclusions," Manatt advised. You should also "seek to negotiate appropriate limits to these exclusions, or seek to eliminate them altogether, when purchasing coverage."

Look For New GAO Study On Cybersecurity Of Health Data Soon

The multitude of recent healthcare data breaches have caught the attention of **Congress.** Now, the Senate is calling for a closer look at the cybersecurity of health data.

Headed by Chairman Sen. **Lamar Alexander** (R-Tenn.) and Ranking Member **Patty Murray** (D-Wash.), the Senate Committee on Health, Education, Labor and Pensions has submitted a request to the **Government Accountability Office** (GAO) to conduct a study on healthcare data cybersecurity.

Sens. Alexander and Murray asserted that current legal safeguards and standards have failed to prevent recent cyberattacks on healthcare IT systems, according to a June 5 analysis by the law firm **Venable LLP.** Earlier this year, the same senators formed a bipartisan working group to focus on oversight of health IT security.

Hot topics: The Committee requested that GAO focus on five main issues in its study:

1. Cyber threats to health IT systems and their potential consequences;

2. Whether any gaps or ambiguities exist in the current regulatory framework for health IT, including the HIPAA Privacy and Security Rules;

3. Federal agencies' oversight and enforcement of the Privacy and Security Rules;

4. The healthcare industry's adoption of cybersecurity standards from the **National Institute of Standards and Technology** (NIST); and

5. Case studies of the effectiveness of selected organizations' privacy and information security controls for health data.