Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

When Taking Health Information Is 'Protected Activity'

Law360, New York (September 22, 2014, 10:33 AM ET) --

Barbara E. Hoey

Your information technology department reports that hundreds of emails have been forwarded to the Gmail account of an employee who is a plaintiff in a charge from the U.S. Equal Employment Opportunity Commission. You confront her, she admits it, and says she gave them to her lawyer. What do you do?

Many employers have been faced with this dilemma, deciding whether an employee was engaged in "protected activity" when, in an attempt to gather evidence to support a claim against the employer, they "help themselves to" (i.e., steal) their employer's data or documents. In this digital era, where such "stealing" can be accomplished with the push of a button, this seems to be happening more frequently, yet employers are understandably confused as to how they can lawfully react to such conduct.

The courts have not always helped as the results of litigation when an employee is fired for theft of "evidence" in the midst of a discrimination lawsuit are mixed. Some courts have sided with the employer, recognizing a company's legitimate right to safeguard its information and documents, while others have sided with the employee, who is attempting to pursue a discrimination claim, yielding what appear to be diametrically opposed outcomes.

The Sixth Circuit recently waded into this thicket in Aldrich v. Rural Health Services Consortium Inc. when it decided that an employee of a health care provider who had been fired for forwarding emails containing confidential patient information to her personal email account — purportedly to preserve evidence for another co-worker's age-bias suit — had not engaged in protected activity. However, in other cases, such as a 2010 decision by the New Jersey Supreme Court,[1] similar conduct was found to be protected. Why the different results? Employers need to understand the factual differences that led to these different outcomes, in order to determine how they should handle such a situation.

The discrimination and whistleblower laws all prohibit retaliation against any employee who has complained about alleged unlawful conduct, or participated in a claim, investigation or litigation. However, in order to be protected from retaliation, an employee must first show that they were engaged in "protected activity."

As explained in Aldrich, “An employee is engaged in protected activity if she has opposed any practice made unlawful by the [Age Discrimination in Employment Act] (the opposition clause),” or "has participated in any manner in an investigation, proceeding or litigation under the ADEA (the participation clause)." The question of whether an employee is just “opposing” discrimination or is “participating” in a suit becomes important in these cases, as “participation” generally gives the employee greater rights and more leeway when engaging in protected conduct. This was a critical distinction in the Aldrich case.

The plaintiff in Aldrich worked for the CEO, Linda Buck, and chief financial officer, Benny Brewster, of Rural Health, a medical facility. Brewster was fired and sued for age discrimination. Shortly thereafter, Buck emailed Aldrich saying “[d]elete this as soon as you reach, and don’t copy anyone. We are going to have to be careful because this may be read by Benny’s lawyers.” Believing Buck was destroying evidence, Aldrich forwarded all emails between Buck and herself to her personal Yahoo account. Many of these emails contained confidential patient information. Rural Health’s policy prohibited the misuse or disclosure of patient information and warned employees that violations could lead to termination. After Rural Health discovered her conduct, the CEO ordered Aldrich to erase the emails from her personal account. Aldrich refused and was fired. She then sued, claiming retaliation.

The Sixth Circuit had to first address whether her conduct — the sending of employer emails to her own account — was “protected activity.” The court first noted that Aldrich was not “participating” in a lawsuit, as she did not have her own claim and was not responding to a subpoena or discovery demand in Brewster’s lawsuit. Also, she had never given any of the emails to Brewster’s counsel. The court noted, “Had she been fired for disclosing the emails in response to a subpoena, or for her deposition testimony in the Brewster litigation, then her conduct would have been protected by the participation clause”

The Sixth Circuit then went on to conclude that Aldrich also was not “opposing” unlawful activity, since “to qualify as protected activity under the opposition clause, the employee’s use of confidential documents must be ‘reasonable under the circumstances.’” The court held that Aldrich’s conduct — "indiscriminately sending confidential documents from Rural Health’s secured servers to her personal Yahoo account" — putting at risk, if not outright invading, the privacy of the company’s patients was "NOT ‘reasonable.’" The content of the emails was highly confidential, they were not related to Brewster’s lawsuit and her conduct was a direct violation of the Health Insurance Portability and Accountability Act and Rural Health’s confidentiality policy. Thus, it concluded, “A reasonably jury could not find that Aldrich was engaged in protected activity.”

While this decision should be a relief to employers — particularly health care companies — they should note that this is still a tricky area. Other courts have found similar behavior to be protected. In 2010, the New Jersey Supreme Court held that a human resources director who had forwarded confidential company documents to her personal email, and then gave them to her lawyer was engaged in “protected activity.” See Quinlan v. Curtiss-Wright Corp., 204 N.J. 239 (N.J. Dec. 2, 2010). Quinlan, who was still employed while she was the plaintiff in litigation, took 1,800 pages of documents containing employees’ confidential personal information. Quinlan’s attorneys used the documents at a deposition, and the company then fired Quinlan for the theft.

The New Jersey Supreme Court ultimately found that Quinlan’s conduct was protected. The court focused on the fact that Quinlan copied documents to which she already had access and only disclosed the documents to her attorneys. Moreover, the documents were directly related to her claim and did not threaten the operation of the company in any way.

Similarly, in Vannoy v. Celanese Corp., No. 09-118, 2011 DOL SOX LEXIS 68 (September 2011, August 2013), a Sarbanes-Oxley Act whistleblower who was terminated after he took company documents and gave them to the Internal Revenue Service, was held to have engaged in protected activity and later won his retaliation claim.

Why the Different Outcomes?

Employers should consider these factors that led to different outcomes to guide their future conduct:

Was the "Thief" Participating in a Lawsuit?

Aldrich did not have her own claim, but alleged she took the emails in order to save evidence relating to Brewster's claim. The fact that she was not "participating" in a lawsuit was a key factor in finding her conduct was not protected. Also, the court noted that the emails she took were never given to Brewster's counsel.

Similarly, in Niswander v. The Cincinnati Insurance Co., 529 F.3d 714 (6th Cir. 2008), the Sixth Circuit also held that a plaintiff's conduct was not protected, even when she disclosed documents in response to a discovery request, because the documents were unrelated to the underlying discrimination claim. In contrast, Quinlan gathered the documents in furtherance of her own claim of discrimination and Vannoy also claimed he had disclosed the documents to further his potential SOX claim.

To Whom were the Documents Disclosed and for What Reason?

Unlike Quinlan, Aldrich never gave the documents to her own attorneys or to Brewster's lawyer. She simply forwarded these confidential documents to her personal email account. Aldrich also refused to delete them despite having been advised of their sensitive nature and resulting violation of company policy. The court found she was not "participating" in or "opposing" discrimination. In contrast, Quinlan was the plaintiff in an action, and provided her attorney with the documents she collected, and had a "colorable" basis to believe that the documents were relevant to her laws. The administrative law judge in Vannoy, the SOX case, also claimed that his "sole purpose" in disclosing the documents to the IRS was to support his whistleblower complaint.

Was Privacy Potentially Violated?

The emails Aldrich forwarded to herself were highly sensitive and contained confidential patient information. They were also not sent over a secure server, thus placing the confidentiality of these patients at risk. In contrast, Quinlan had given the documents only to her lawyer, so there didn't seem to be an issue of privacy. I note however that the documents Quinlan took did contain personal information about other employees, such as Social Security numbers, which could have harmed them if lost. Vannoy, meanwhile, gave documents to the IRS, thus privacy did not seem to concern the administrative review board. It seemed that the court in Aldrich regarded the 'theft' of the medical information as much more serious.

Takeaways

- Have strong confidentiality and anti-theft policies in place and remind employees of these policies early and often. The policies should state that violations will lead to progressive discipline, up to and including suspension and/or termination.

- Monitor your IT systems and make sure employees are not electronically "pilfering" your materials. Computers can be set up to prohibit the copying of information onto remote devices, and IT should watch for employees who are sending large amounts of data to their home or personal accounts. If you do not police your systems, a court could find you were not enforcing your own policies.

- Have a plan in place to promptly investigate a potential theft or breach. If a theft occurs — by an employee at any level of the organization — prompt but thoughtful action should be taken. All steps and decisions should be carefully documented.

- If there has been a data breach, consider statutory obligations to report that breach and notify those affected.

- Know the applicable law. Quinlan drew a clear distinction between the protections afforded under federal law versus those granted under New Jersey's Law against Discrimination. It also seems that a potential SOX whistleblower may be offered greater protections than a discrimination claimant.

- Always, check with counsel prior to taking in any disciplinary action. Remember, you may have a SOX whistleblower and may not even know it. While discipline may be warranted, and indeed necessary, employers need to be careful in handling such matters.

—By Barbara E. Hoey and Evelyn M. Perez, Kelley Drye & Warren LLP

Barbara Hoey is a partner and Evelyn Perez is an associate in Kelley Drye & Warren's New York office.

[1] Quinlan v. Curtiss Wright Corp., 204 N.J. 239 (N.J. 2010)