

## Attorney-Client Privilege in the Work Place

By Wade Pearson Miller, Esq  
Amy Bailey Muckler, CHC, CPC-I, CPC-H-I, CCS-P  
Sarah Spry, CHC, CPC, PCS

Health Care Providers and their employees frequently have occasion to work with attorneys and often expect those communications to be covered by the attorney-client privilege. The application of the attorney-client privilege in the workplace can be complicated, leading to confusion as to when communications are privileged.

A recent case involving a New York hospital raised the question of whether an employee's communications with his or her own, individual counsel, is protected by the attorney client privilege when the communication is made using the employer's computer and email server. This case raises interesting questions about the application of the attorney-client privilege in the hospital setting, particularly given employees' reliance on email and internet services to perform their jobs.

### Background

#### Basics of the attorney/client privilege

The attorney client privilege protects confidential communications that are exchanged between an attorney and client and made for the purpose of seeking or rendering legal advice. It is the client's privilege to refuse to disclose and to prevent others, including the attorney, from disclosing confidential communications between lawyer and client. It is important to note that the privilege protects communications—not the underlying facts.<sup>1</sup>

In the health care provider context, the privilege generally exists when the communications at issue are made by employees of the health care provider client to counsel at the direction of superiors in order to obtain legal advice from counsel for the health care provider.

The health care provider's attorney client privilege can protect interviews of employees conducted by the organization's counsel, attorney's notes, and summaries of interviews—to the extent these materials quote, contain or reflect communications to or from employees of the health care provider. Importantly, because the privilege belongs to the health care provider, it can be waived and communications between the health care provider's counsel and its employees can be disclosed by the organization without the employee's consent.

#### Basics of the work product doctrine

The work product privilege is narrower than the attorney client privilege. The work product privilege provides qualified protection to documents prepared in anticipation of

---

<sup>1</sup> *Upjohn Co. v. United States*, 449 U.S. 383 (1981).

litigation or for trial by or for a party, or by or for a party's representative.<sup>2</sup> Opinions, conclusions, legal theories, mental impressions, etc. of an attorney or other representative are also protected under the privilege. This privilege is held by both the client and the attorney.

### Summary of *Scott v. Beth Israel Medical Center, Inc.*, 847 N.Y.S.2d 436 (2007)

A physician employed by Beth Israel Medical Center in New York sued Beth Israel for breach of his employment contract. During the discovery process, Beth Israel learned that the physician had been using Beth Israel's computer and email server to communicate with his own personal attorney. Beth Israel took the position that such communications were not protected by the attorney client privilege or work product doctrine. The physician disagreed and demanded return of all email communication made between him and his attorney.

The court in *Beth Israel* found that the test for determining whether a communication between attorney and client is privileged is whether the client communicates with the attorney *in confidence* for the purpose of obtaining legal advice. Using that test, the New York Supreme Court found that the physician's email communications on the hospital's computer were not confidential in nature and therefore the attorney client privilege did not apply.

In reaching its determination, the court looked to Beth Israel's email policy. The policy governing Beth Israel's computer and communication system stated as follows:

*1. All Medical Center computer systems, telephone systems, voice mail systems, facsimile equipment, electronic mail systems, Internet access systems, related technology systems, and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purposes only.*

*2. All information and documents created, received, saved or sent on the Medical Center's computer or communications systems are of the Medical Center. Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice.*

The physician argued that privileged communications do not lose their privileged character by being communicated electronically. While the court recognized that communicating electronically alone does not waive the privileged nature of the communication, there may be other reasons that the privilege is lost. The relevant

---

<sup>2</sup> See Fed. R. Civ. P. 26(b)(3).

inquiry, regardless of how the communication is made, is whether the communication was made in confidence. Because the court found that Beth Israel had a “no personal use” policy and specifically reserved its right to monitor communications and disclose them without prior notice and that the physician was aware of the policy, the court concluded that the physician did not have a reasonable expectation that the communications would be confidential.

The physician also argued that the emails with his counsel were protected as privileged work product. The court looked at whether the physician and his attorney took adequate steps to protect the information from the physician’s adversary, in this case, the hospital. The physician argued that his attorney took steps to prevent disclosure by including a notice on the email that the emails may be confidential and to notify the attorney if anyone other than the intended recipient received the emails. The court found that the pro forma notice on the emails was not sufficient to prevent waiver of the work product privilege.

### **Other Cases**

Other courts looking at this issue have also placed great weight on the employer’s policy with respect to personal email usage and whether that policy was enforced.

For example, in *Kaufman v. Sungard Invest. Sys.*,<sup>3</sup> the court upheld the magistrate judge’s finding that an employee waived the attorney client privilege because she knowingly utilized her employer’s computer network with the knowledge that her employer’s email policy provided that it could search and monitor email communications at any time. In *Kaufman*, it was undisputed that the employee agreed to abide by the policy which specifically stated, “the Company has the right to access and inspect all electronic systems...and computer files and electronic mail, even if protected with a password.”<sup>4</sup> Based on the policy and the employee’s knowledge of its provisions, the court found the employee had no reasonable expectation of privacy as to communications with her attorney.

In *Curto v. Medical World Communications, Inc.*, the court considered whether there was enforcement of any computer usage policy and found that lack of enforcement lulled employees into a false sense of security. In *Curto*, the employee sent emails to her attorney using her personal email account which did not go through her employer’s computer servers and attempted to delete the privileged material before returning the company’s laptop. The court found enforcement of the policy was relevant to whether the employee’s conduct was so careless as to suggest that it was not concerned with the protection of the privilege. Because there were few instances of actual monitoring of employee email accounts and because large numbers of employees had personal email accounts at work, the court found that the employee had not waived the attorney client privilege occurred. The court also considered the fact that the employee’s laptop was not connected to employer’s computer server, the privileged communications were made from employee’s home on her personal email account and she attempted to

---

<sup>3</sup> No. 05-cv-1236, 2006 WL 1307882 (D.N.J. May 10, 2006).

<sup>4</sup> *Id.* at \*4.

delete the privileged communications prior to returning the laptop in reaching its determination the attorney client privilege had not been waived.

In another recent case, the defendant employer argued that an employee who communicated with his own lawyer on the employer's computer waived the attorney client privilege because its policy specifically reserved the employer's right to view any email communication at any time and informed employees they had no expectation of privacy in email communication.<sup>5</sup> The court considered whether the employee had actual knowledge of the policy and absent such a showing refused to find a waiver of the privilege.

Given these rulings, questions arise for employers, employees and attorneys of health care providers.

### **Employer Concerns**

Given health care providers' reliance on electronic communications and data transmission and storage, employers are finding it more difficult to promote the efficient and necessary use of technology while policing the employees' use of employer computer systems for inappropriate, personal employee communication. In addition, employers must be constantly concerned with allegations of invasion of privacy and improper grounds for termination.

One of the keys to any organization's success is to develop clear, defined policies and procedures which govern the day to day affairs of the organization. As part of the effort, employers should implement processes to ensure that employees are aware of all policies and that the policies are enforced consistently.

Organizations that choose to monitor computer usage and email should implement explicit policies, in accordance with applicable state and Federal law, regarding personal use of company property. For example, the policy should indicate that use of company computers for personal use is strictly prohibited, personal email communications are property of the organization and are not confidential and the organization will perform routine monitoring of all computer activity and may disclose any information discovered through the monitoring process. The policy should also define disciplinary action for detected violations. Additionally, organizations should maintain adequate records to support the performance of routine monitoring and consistent application of the policy. Most importantly, the monitoring of email communications in the absence of a clearly defined policy may violate the Electronic Communications Privacy Act, a Federal Law enacted in 1986.<sup>6</sup>

Many organizations require employees to sign and date an attestation acknowledging that they have received a copy of, are aware of and will abide by all company policies. Generally this statement is retained in the personnel file and maintained by the Human Resources department.

---

<sup>5</sup> *Mason v. ILS Technologies, LLC*, NO. 3:04-CV-139, 2008 WL 731557 (W.D.N.C, Feb. 29, 2008).

<sup>6</sup> 18 USC §2510

## **Employee Concerns**

Employees should use caution in communicating with their personal attorneys on their employer's computer system and in light of the case law above, should consider avoiding it altogether. The employee should familiarize himself with his employer's policy and discuss it with his attorney prior to having privileged communications by email.

If you are unsure if your employer has a policy governing the use of company property and the monitoring of personal communications, you should contact Human Resources, or other appropriate department, for clarification to ensure compliance with organizational policies and to maintain your privacy.

## **Attorney Concerns**

It is commonplace in today's internet age for lawyers to communicate with their clients via email. The American Bar Association has addressed the issue of electronic communication in light of Model Rule 1.6 which imposes on a lawyer a duty to take reasonable steps in the circumstances to protect confidential client information against unauthorized use or disclosure. The ABA concluded that lawyers have a reasonable expectation of privacy in communications made by all forms of email, including unencrypted email. However, in deciding whether to communicate with a client via his or her company email, the attorney should consider the sensitivity of the communication, the costs of its disclosure, and the relative security of the contemplated mode of communication. Ultimately, the lawyer must follow the client's directive regarding the means of communication.

In *Beth Israel*, the court found the standard pro forma notice that we see on almost all email communications from attorneys was not alone sufficient to protect communications from disclosure. So what else can the lawyer do? If there is a concern about preserving confidentiality, the attorney may consider taking additional security measures such as encrypting emails and making them password protected—as hospitals often do when emailing confidential patient identifying information. If the attorney has serious concerns about protecting confidentiality of communication, the attorney may simply avoid communicating substantively by email.

## **Things to Consider**

The same considerations that apply to email also apply to use of employer's telephone system, voicemail, and facsimiles. Indeed, given that many businesses voicemails and facsimiles are transmitted through the computer network, the same concerns about confidentiality apply and employer's policies should address those electronic medium as well.

While the facts and circumstances of each case will be different, attorneys and clients should be mindful of policies and procedures governing use of employer property and take adequate steps to ensure confidentiality of any privileged information is preserved.