Mitigating the Risks of Business Email

Alan A. Ayers, MBA, MAcc
Vice President, Concentra Urgent Care
Content Advisor, Urgent Care Association of America

For urgent care operators, email provides a useful tool in facilitating communication with patients, referral physicians, vendors and the community; between center staff and internal departments in disparate locations; and between a center's management and its employees. But when used irresponsibly, email can also create significant legal and professional liability—putting an operation's finances, stability, and reputation at risk. For urgent care centers, this risk is magnified when HIPAA and other patient privacy regulations are invoked.[1] The instantaneous nature of email, in combination with the large volumes of email sent and received on a daily basis, makes it difficult for management to assure everyone stays within the bounds of acceptable practice. Therefore, a proactive approach to business email that includes development of specific policies and training of management and staff is advised.

You've Got Litigation

The first thing to understand about email is that once created, it's discoverable and generally admissible as evidence in both civil and criminal proceedings. Termed "e-discovery" or "electronically stored information," emails are treated the same as printed documents and thus can be used to instigate new litigation or as evidence in existing disputes. Employee email communications have aided in creating a paper trail in some of the most controversial court decisions,[2] so if a business is in the course of litigation or suspects impending litigation[3], deleting any emails that could be used as evidence can arouse suspicion of deception, create an appearance of guilt, and can be harshly punished by the courts.[4]

In general, "at risk" emails involve some sort of security breach[5], libel[6], slander[7], defamation of character[8], sexual harassment[9], or admissions of negligence in a medical malpractice claim.[10] However, something as simple as forwarding a "joke" can offend someone and land the urgent care center in court.[11]

In the context of adversarial litigation, there are typically two scenarios that occur:

- An employer seeks to use an employee's emails in its defense when the two are engaged in litigation; or
- An employer seeks to shield an employee's emails from purview of an outside litigant.

Underlying both scenarios is an assumption of privacy by employees. Typically, if an employer's electronic communication policy states that business email is monitored, there is no expectation of privacy by anyone utilizing business email, even on a personal mobile device.[12] In effect, "private employees have diminished expectations of personal privacy in the modern workplace."[13] The courts have even ruled that a married couple has no reasonable expectation of privacy using a business email account when an employer's policy clearly states otherwise.[14]

Attorney-client privilege in the form of email communication using a business account is likewise suspect when the employee handbook clearly states there is no reasonable expectation of privacy on business computer systems.[15] Additionally, when email exchanges have been deleted, an employer can utilize electronic forensics to recover and use attorney-client emails sent and received through the business server.[16]

When it comes to accessing a personal email account on a business computer or mobile device, rulings have varied depending on the specificity of the employer's computer use policies. The courts have generally ruled a password-enabled personal account is protected under the Electronic Communications Privacy Act.[17] Also, when a company's policy is vague, utilizing a personal email account on a business computer to communicate with an attorney meets the attorney-client privilege standard.[18] For these reasons—as well as to prevent the unauthorized transfer of confidential patient or business data—many employers prohibit the use of personal email accounts at work.

Employee Implications

Litigation isn't the only consequence of misusing business email. There have been highly publicized cases of employees being fired for inappropriate relationships[19], sexual harassment[20], leaking confidential information, and accidentally receiving confidential emails[21]. Additionally, hurtful, lewd or political emails at work can create a discriminatory or

hostile work environment. Even solicitations for charity or forwarding jokes can be considered inappropriate[22] and incur consequences.

Consider the results of a 2011 survey of public and private businesses in which:

- 34% experienced exposure of sensitive or embarrassing information;
- 31% experienced improper exposure or theft of customer information;
- 29% experienced improper exposure or theft of intellectual property; and
- 24% were ordered by a regulatory body to produce employee email.

On average, these businesses indicated that 19% of email sent from their organizations contained content that posed a legal, financial or regulatory risk.[23]

A potential remedy—although not a complete solution—is to monitor employee emails. According to the American Management Association's 2007 Electronic Monitoring and Surveillance Survey[24], 66% of respondents reported reviewing employees' e-mail messages and 28% had fired employees for misuse of e-mail.

Legitimate reasons[25] for wanting to monitor employee emails include:

- Maintaining the center's professional reputation and image.
- Maintaining employee productivity.
- Preventing and discouraging sexual harassment, workplace bullying, discrimination, and inappropriate behavior.
- Preventing "cyber stalking" by employees.
- Preventing possible defamation liability.
- Preventing employee disclosure of patient data, trade secrets and other confidential information.
- Avoiding copyright and other intellectual property infringement from employees illegally downloading software, music, videos, etc.

Not only is it legal for an employer to monitor email sent and received through its servers, but such is becoming the norm.[26] *Exhibit 1 illustrates a notice that may be displayed when employees log on to a business system indicating that usage is for "business purposes" by "authorized persons" which may be "monitored and audited."*

Exhibit 1: Sample notice against non-business or unauthorized use.

```
This is a business computer and is only to be used by authorized personnel. The business may monitor and audit
the usage of this computer for purposes of compliance with internal policies and applicable regulations. Use of
this computer constitutes consent to having your usage monitored and audited. Unauthorized use of this computer
is strictly prohibited and may be punishable under law.
```

Steps for the Urgent Care Operator

In this day and age of non-stop electronic communication, urgent care operators must actively protect themselves against the legal and business repercussions of employee email. Recommended steps include:

1. Establish and document policies and procedures for work-based electronic communication, including mobile devices. *Exhibit 2 provides content suggestions for an electronic communications policy.*
2. Include the electronic communication policy in the employee handbook, post it in the center, provide email training to management and staff, and have all employees sign that they have read, understand, and will abide by the policy. *Exhibit 3 provides practical suggestions for employee use of email in the workplace.*
3. Encourage employees to place a confidentiality notice at the bottom of all emails. *Exhibit 4 provides sample verbiage for this purpose.*
4. Develop an appropriate email archiving policy and secure archiving systems and processes.
5. Remind employees of the email policy repeatedly. Employees are very likely to forget the specifics of training when they click "send."

Additionally, many of these policies should be considered for employee utilization of social media websites—such as Facebook and Twitter.

Exhibit 2: Points that should be included in an electronic communications policy.

- The urgent care center's computers and email accounts are for business use only.
- Information created by or stored on business systems is property of the business.
- The business reserves the right to monitor the use of its electronic resources.
- The business expects employees to conduct themselves professionally both on and off duty.
- Employees must abide by anti-harassment and anti-discrimination policies.
- The storing of electronic information on portable devices without prior approval is prohibited.
- Forwarding of business or patient information to personal e-mail accounts is prohibited.
- No one may access, or attempt to obtain access to, another's electronic communications without appropriate authorization.
- Business systems may not be used for any illegal activity, including downloading or distributing pirated software, entertainment media, or data.
- Policies governing the use of company logos and other branding and identity apply to electronic communications.
- The business reserves the right to take disciplinary action if the employee's electronic communications violate policy.
- Employees must abide by non-disclosure and confidentiality agreements/policies.
- Employees are prohibited from making defamatory or discriminatory comments when discussing the employer, superiors, co-workers and/or competitors.
- Employees must comply with all other policies with respect to their electronic communications.
- Employees bear full responsibility for the material they post on personal blogs, social networks, websites, etc.
- Employees understand what to do if they suspect they have been sent or have opened a virus.
- Employees understand what language is strictly prohibited.
- Employees understand they should alert a member of management if they receive an inappropriate communication or observe violations of the electronic communications policy.

Exhibit 3: Practical email advice for management and staff.

- Prepare emails as if you are publishing them
- Recheck your "To" line before sending
- Anticipate that recipients will forward emails
- If you need to "vent," pick up the phone or meet in person
- Email can be used as documentation after telephone or face-to-face meetings
- Keep your email boxes cleaned out
- Delete unnecessary attachments—particularly personal photographs
- Include only necessary recipients—to whom a message is addressed can communicate more than the message itself
- Use carbon copy (cc:) or blind carbon copy (bcc:) judiciously. Unnecessary copying—especially of a recipient's supervisors—can generate animosity
- Beware of "reply all"—this should only be used if there's a point to address to the entire group
- Make the subject line meaningful-people receive scores of email daily so make your message stand out
- Consider how email formatting will appear on handheld devices (iPhone, iPad, Blackberry, etc.)
- Include signature line with contact information such as telephone and email address

Exhibit 4: Sample email confidentiality notice.

******** CONFIDENTIALITY NOTICE ********

This e-mail message and all attachments transmitted with it may contain legally privileged and confidential information intended solely for the use of the addressee. If the reader of this message is not the intended recipient, you are hereby notified that any reading, dissemination, distribution, copying, or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately and delete this message from your system. Thank you.

The information transmitted is intended only for the person or entity to which it is addressed and may contain CONFIDENTIAL material. If you receive this material/ information in error, please contact the sender and delete or destroy the material/ information.

References:

[1] John Deutsch, "Secure Corporate Email for Healthcare," Medical Web Experts.com
http://www.medicalwebexperts.com/blog/secure-corporate-email-healthcare/
[2] Mary Clare Jalonick, "Emails Show White House input on Sherrod Ouster, Associated Press. http://www.courthousenews.com/2012/03/07/44474.htm
[3] *VOOM HD Holdings LLC v. EchoStar Satellite L.L.C.*, 600292/08
Holme v. Global Minerals and Metals Corp, 90 A.D.3d 423, 934 N.Y.S.2d 30 (1st Dept. 2011)
[4] Spoliation is defined as, "the destruction or material alteration of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Silvestri v. General Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001).
[5] Geoffrey A. Fowler, "What's a Company's Biggest Security Risk? You.," The Wall Street Journal.
http://online.wsj.com/article/SB10001424053111904836104576556421692299218.html
[6] Martin Langeveld, "Noonan v. Staples: 'The most dangerous libel decision in decades,'" Nieman Journalism Lab.
http://www.niemanlab.org/2009/02/the-most-dangerous-libel-decision-in-decades/
[7] Karli Wood, "Employee Denies Defaming Colleague," The Northerner. http://www.thenortherner.com/news/2012/02/29/emplyee-denies-defaming-collegue/
[8] William Dotinga, "Scorching Complaint Against County Health," Courthouse News Service. http://www.courthousenews.com/2012/02/24/44145.htm
[9] Kim Clark, "Email, Sexual Harassment and Liability, Examiner.com
http://www.examiner.com/workplace-issues-in-salt-lake-city/email-sexual-harassment-and-liability
Tamar Lewin, Chevron Settles Sexual Harassment charges, The New York Times.
http://www.nytimes.com/1995/02/22/us/chevron-settles-sexual-harassment-charges.html
[10] "HIPAA Enforcement Swings From Voluntary Compliance to Punishment for Violation of Privacy and Security Laws," Medical News Today.
http://www.medicalnewstoday.com/releases/57676.php
[11] *EEOC v. Austin Foam Plastics, Inc.,* No. 1:09-CV-00180 (W.D. Tex. Oct. 15, 2010).
[12] *Bourke v. Nissan Motor Corp*., No. B068705 (Cal. Ct. App., July 26, 1993)
Smyth v. Pillsbury, C.A. NO. 95-5712, U.S. District Court for the Eastern District of Pennsylvania, Jan.18, 1996, Decided, Jan. 23, 1996, Filed.
Shoars v. Epson, America, Inc., No. SWC 112749 (Cal. Super. Ct. filed Mar. 26, 1990).
McLaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999)
TBG Insurance Services Corp. v. Superior Ct., 96 Cal. App. 4th 443 (Cal Ct. App. 2002)
Garrity v. John Hancock Mutual Life Insurance Co., 2002 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004)
[13] John C. Barker, Note, *Constitutional Privacy Rights in the Private Workplace, Under The Federal and California Constitutions*, 19 HASTINGS CONST. L.Q. 1107, 1108 (1992).
[14] In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico on April 20, 2010, No. MDL 2179, 2011 WL 1193030 (E.D. La. Mar. 28, 2011)
[15] *Leor Exploration & Prod., LLC v. Aguiar*, 2009 WL 3097207 (S.D. Fla. Sept. 23, 2009)
[16] *Kaufman v. SunGard Inv. Sys*., 2006 WL 1307882 (D.N.J. May 10, 2006) (Unpublished)
[17] The only federal law currently applicable to the issue of workplace e-mail monitoring. The 1986 law states that a government entity generally must provide a subpoena, warrant or court order to obtain email communication information.
[18] *Stengart v. Loving Care Agency, Inc*., 2010 WL 1189458 (N.J. Mar. 30, 2010)
Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006)
[19] Connie Reily, "Fired Navy Captain Unlikely to Regain Sea Command," Virginia-Pilot.
http://www.military.com/news/article/fired-navy-captain-unlikely-to-regain-sea-command.html
[20] Lisa Coston, "Rude Conditions Alleged in Paula Deen's," Courthouse News. http://www.courthousenews.com/2012/03/07/44474.htm
[21] Nancy Dillon, "'Desperate Housewives' creator Marc Cherry nixed from Nicollette Sheridan lawsuit," NY Daily News.
http://articles.nydailynews.com/2012-03-13/news/31161820_1_battery-accusation-mark-baute-judge-elizabeth-allen-white
[22] MJ Lee, "Judge Richard Cebull admits to anti-Obama email," Politico.
http://www.politico.com/news/stories/0312/73486.html
[23] Research Results: Outbound Email and Data Loss Prevention 2011. http://www.proofpoint.com/id/outbound0911/index.php
[24] American Management Association's 2007 Electronic Monitoring and Surveillance Survey
[25] Terence Lawrence, "Monitoring Employee E-mail: Avoid Stalking and illegal Internet Conduct," Pittsburgh Business Times.
http://www.bizjournals.com/pittsburgh/stories/2000/05/22/focus6.html
[26] Schumacher, Susan (2011) "What Employees Should Know About Electronic Performance Monitoring," ESSAI: Vol. 8, Article 38. Available at:
http://dc.cod.edu/essai/vol8/iss1/38