Catie Heindel

Auditing Emails: A Useful Method for Testing Compliance Program Effectiveness

Five Important Steps to Help Organizations Evaluate Their Program's Effectiveness

Catie Heindel, JD, is a senior associate at Strategic Management Services, LLC.

Email is the most common form of communication used by organizations today. This means that any views, quotes, or discussions made in a company email can be seen to be representative of the organization; however, given the common, casual form of email, people often grow careless in what information they include when communicating with other employees, clients, or colleagues. Therefore, email records provide the perfect type of evidence for the government to prove health care fraud and abuse cases.

Virtually all successful anti-kickback cases begin with a single subpoena requesting emails related to the case issue (for example, physician arrangements). In most cases, the government is able to find damaging information that can be used to support the allegations against the organization. Additionally, simply hitting the "delete" button does not eliminate the email entirely. Sophisticated software can retrieve a message even after it has been deleted. Therefore, where an organization's records are subpoenaed, an email may be used as evidence even after deletion.

The Department of Health and Human Services (HHS) Office of Inspector General (OIG), in its compliance program guidance for health care entities, consistently states that organizations should conduct *"ongoing auditing and monitoring"* of compliance programs to ensure effectiveness. While organizations may provide compliance education and training to all employees, there is no one way to ensure that employees understand and act in conformance with compliance rules and regulations; however, one possible way to audit compliance program effectiveness is to perform a review of employee email communications.

As any email communication made or received by an employee using his or her company email address is the property of the organization, these records provide a wealth of information for review. An email audit can help organizations understand how employees internalize compliance education and training and may uncover the existence of potential compliance risks.

Where an organization decides to conduct an electronic communication review, there are five important steps that it should follow. This article will outline these steps and provide important information to consider during this type of review.

The five steps are as follows:

1. Review organization policies and procedures regarding email communication use.
2. Identify a sample group of email communications to review.
3. Audit email communication in the sample group and identify potential and/or actual compliance issues.
4. Interview individuals involved in potential and/or actual compliance issues.
5. Develop and implement a remediation plan.

Step One

An organization should have strict policies in place to ensure that employees are aware that they are prohibited from using company communication systems for purposes that are illegal or otherwise contrary to the organization's business purpose. Such policies may be outlined in human resources department guides, through an organizational code of conduct, and/or by having employees sign an agreement whereby they promise to only use the Internet/email for the purposes necessary to complete their job description.

Employees also should be aware that any communications made using company email are the property of the organization and not the property of the individual employee. Employees should presume no expectation of privacy in anything they create, store, send, or receive on the company computer and telephonic systems. To clarify and avoid problematic scenarios, organization communications to employees should include examples of correct and incorrect usage of email/Internet resources. Reviewers should be familiar with all organization policies and procedures regarding email communication use before conducting the audit.

Step Two

Before beginning the review, it is necessary to identify the sample size and type of email communications that will be reviewed. Organizations may decide to do a general compliance audit or conduct a more focused review that identifies emails received and sent by particular employees/employee groups or regarding specific subject areas. Where necessary, the focus of a review also can be determined by conducting a risk assessment, examining past hot line compliance issues reported, or considering issues that receive the most attention from government regulators.

When determining the sample size of emails to review, organizations should take into consideration the resources available to conduct the audit. Larger email review projects can take significant time but will produce more thorough results. Organizations can focus on a particular time period (*e.g.*, one year, six months) to limit the review sample size.

Step Three

Once the sample group of emails has been identified, the organization should decide how to conduct the review in an efficient and effective manner. Depending on the organization's information technology network design, reviewers may want to use a software program to help facilitate and streamline the electronic document review process. Several programs exist that allow organizations to store, organize, and review all audited documents electronically. Using these products, reviewers can identify records that have already been reviewed, as well as utilize program components to flag specific documents that contain potential and/or actual issues.

Additionally, some software programs allow reviewers to conduct keyword searches throughout the sample documents, which is extremely useful for reviews that are focused on specific risk areas. Once the email sample has been reviewed, auditors should develop a comprehensive list of any potential or actual compliance issues identified.

Step Four

If potential or actual compliance issues are identified during the review processes, an investigation should be initiated for each relevant issue; however, the relevance of an issue may not be apparent by looking only at the email involved. Therefore, organizations will want to conduct interviews with the employees (sender/receiver of email) involved with the identified issue.

Interviews should include a discussion of the potential compliance issue and should seek to further flush out the nature and degree of employee involvement. Additionally, interviews should address the employee's knowledge of applicable federal and state laws and regulations regarding specific issues as well as related organization policies and procedures. Organizations may want to consider having legal counsel present to further protect against future liability.

Step Five

Where an actual compliance issue is identified during the document review and confirmed through the interview process, the organization should develop and implement, as expediently as possible, a remediation plan. The remediation plan should outline the actions to be taken to handle the compliance issue. The plan may suggest further investigative action or recommend potential sanction activity be taken by human resources.

Depending on the type of compliance issue, disclosure to state and federal government departments also may be required. Additionally, where necessary, organizations should ensure that the issue is discussed and/or reported to appropriate senior-level management and/or board of directors. Any progress with the remediation plan should be documented and reviewed. Again, when developing the remediation plan, the compliance office should ensure that both human resources and legal departments are involved.

Conclusion

By following the five steps listed above, organizations now have another review methodology to help evaluate their compliance program's effectiveness. As noted before, the detail and magnitude of the review will depend on an organization's resources. Before conducting an internal review, organizations should ensure that the employees involved can provide an independent, unbiased outlook on potential internal deficiencies.

Alternatively, organizations also should consider having the review performed by an external resource (*e.g.*, a compliance consultant), who can provide both independent deficiency findings and recommendations for remediation. Further, as noted above, this type of document review potentially may result in the identification of a sensitive, disclosable event. For that reason, organizations should seriously consider engaging an outside consultant to perform the audit under the direction of legal counsel to ensure that the organization appropriately protects itself from liability.

Reprinted from Journal of Health Care Compliance, Volume 14, Number 1, January-February 2012,
pages 51-53, with permission from CCH and Aspen Publishers, Wolters Kluwer businesses.
For permission to reprint, e-mail permissions@cch.com.