PHILLIPS & MAREK

Successful Data Breach Communication Begins *Before* the Incident

Most organizations do a good job staffing their data security teams with appropriate people from the leadership and technology areas. However, one discipline that is often overlooked, but critically important, is public relations.

The best time to prepare your data breach communications plan is *before* an incident occurs. At right is a high-level checklist and on the back page are some of the basics to help you get started.

1. Select the Organization's Spokespeople
2. Draft the Messaging
3. Train Spokespeople
4. Develop a Rapid Internal Communications Plan
5. Determine How to Notify Those Affected
6. Know How to Work with the Outsourced Call Center
7. Establish an Internal Escalation Line
8. Have a Process for Notifying the Media

WORKING WITH LEGAL COUNSEL

Mark every document "Privileged & Confidential – Prepared at the Request of Counsel." (Consult with your attorney for the exact wording.)

Have all work products, from internal notifications to press release, approved by legal counsel.

Retain all internal and external communications and assume they may someday be discoverable in court.

1 Select the Organization's Spokespeople

Only a handful of people from the organization should be selected to serve as incident spokespeople. This generally includes the CEO, HIPAA compliance officer and head of technology. Keeping this group small will help ensure everyone remains focused on the key messages.

2 Draft the Messaging

While it's difficult to develop messaging before anything happens, it's never too early to think through common situations and even draft messaging (that can be edited later) in terms of:

- What happened?
- When and how was the incident discovered?
- What is the organization doing in response?

3 Train Spokespeople

Since it's common for people to speculate and say too much in the heat of the moment, holding periodic spokesperson trainings based on hypothetical situations and commonly asked questions can be extremely helpful. This is a good time to teach them how to stay on message, bridge back to important topics and even de-escalate heated situations.

4 Develop a Rapid Internal Communications Plan

Employees (and sometimes even vendors) should be notified about the data breach from someone on the internal data security team. For large organizations where employees work different shifts, this can be difficult. Fortunately, there are ways to quickly create and disseminate information from a trusted internal source, as well as instruct them how to triage breach-related questions so they can remain focused on the business at hand.

5 Determine How to Notify Those Affected

The most common way to notify those whose information has been potentially impacted by a data breach is by mail. Whenever possible, mail letters directly from the organization rather than from an outside source. This will eliminate floods of calls from people confirming the letter is legitimate. Sometimes those notifications can be sent via email when people opt for paperless communication.

6 Know How to Work with the Outsourced Call Center

If your organization is large, your HIPAA technology firm and/or attorney will most likely contract with a vendor to help notify those whose information may have been compromised, answer their questions and enroll them in a credit protection program. You will, however, be responsible for developing a Q&A document that call center employees will use as a script.

A word of warning… Someone must regularly monitor the quality of information that is being provided to callers through a series of test calls. Like retail "secret shoppers," this coordinated process involves providing people with specific scenarios to use when they reach out to the call center, then report back about their experiences.

7 Establish an Internal Escalation Line

No matter how great the outsourced call center is, many people will insist on speaking with someone internally. Also, the nature of some calls will quickly exceed the ability of the outsourced call center to handle. Those people should be referred to an internal escalation line.

A "soft phone" is the best way to establish this line so it has an internal number, but can be staffed from anywhere. Records of these calls must be maintained in a HIPAA compliant format that can easily be shared when callers are referred to others within the organization.

8 Have a Process for Notifying the Media

Many government agencies have regulatory compliance requirements that a press release about the incident be sent to the local media. This must be carefully coordinated with and approved by legal counsel, and must cover the basics like what happened, who was affected, what information was likely involved and what is the organization doing in response. Unlike most media relations endeavors, the hope for data breach press releases is that they receive little or no coverage.

If your organization isn't large enough to have someone with public relations skills on staff, ask your attorney or HIPAA consulting firm for a recommendation because there are special skillsets that will be necessary to help your organization prepare for and respond to an incident.

To discuss how your organization can prepare its communication plan *before* a data breach occurs, contact Phillips & Marek today.