An Ounce of Prevention is Worth a Pound of Cure: The Role of Compliance in the Digital Customer Experience
By Andrew Hellard, Healthcare Customer Communications Management Expert, GMC Software Technology

The phone rings in a company’s human resources department. The caller explains he is from the Internal Revenue Service, and is conducting an audit of the company’s use of consultants. The company may have wrongly classified employees as consultants. If the company did misclassify, huge fines will be coming. In order to clear up this misunderstanding, he needs historical W-2 data from all employees. The HR employee knows the company did nothing wrong, so he exports digital copies of all W-2 documents and sends them to the specified email address. By this point the alert reader should be horrified at both this obvious scam and the poor HR employee who will shortly be unemployed. Most people are familiar with the concept of phishing, which is targeting a specific person and using social tactics to elicit private information. From the clinical perspective of this article, it is easy to dismiss this approach as useful only against the unsophisticated. It would be much harder to dismiss if your phone rang from a Washington DC number and the caller already had your company’s tax identification information.

In other scenarios, there is no ill intent, only poor oversight. A health insurance company is preparing Explanations of Benefits (EOB) mailings, which include sensitive and private information about healthcare services. This company generates millions of EOBs each month, and saves a copy in each member’s account on the company’s website. A batch process reads the member account number from the EOB and places the document into the correct website location. Recent regulatory changes forced the IT department to perform a series of last-minute adjustments to these documents, and the process updated the format of the account numbers. No one told the batch team, and the process that posts these documents was not updated. Millions of EOBs are posted to the wrong account, revealing everything from drug test results to cancer treatments.

In both nightmare situations, digital communications have exposed a company to huge fines as well as public embarrassment and customer attrition. These dangers are not new. Traditional paper communications could have had the same effect. What is different in a digital environment is the speed with which a small mistake can reach millions of customers. With digital communications, no one can rush down to the mailroom and stop a stack of envelopes from going out. Automated processes massively increase efficiency, but these same processes, by their very nature, lack human oversight. This transition from traditional forms of communication to digital communication is critical for customer experience, but companies must update processes and procedures along with technology to avoid these dangerous situations.

What can a company do to modernize communications processes while also remaining compliant with regulations? There are two considerations: prevention and recovery. Prevention is the most important approach. Recovery requires recognizing that eventually someone will make a mistake, and a proactive company will have the technology in place to minimize the impact of that mistake.

Prevention is not an exciting topic. Communications and customer experience professionals generally do not enjoy working with compliance departments. Compliance reviews can slow projects, and sometimes
prevent exciting new communications from even being launched. Because of this aversion, often what happens is that at the end of a project, someone will remember to call compliance for a last minute review. Compliance is upset because their schedule is disrupted, those responsible for customer experience are anxious because their project is delayed, and IT is angry because their work might have been wasted. The key to avoiding this situation is internal communication. Compliance should be an integral part of any new communications project, especially one that involves new technology or new delivery channels. Reviewing compliance challenges early keeps projects on schedule, and integrating compliance knowledge into communication design reduces the chances of an expensive mistake.

Recovery is also an important consideration. In the first scenario above, every current and past employee was affected. Contacting current employees is easy, contacting former employees is not. Even with addresses on file, does the company have the technology in place to generate the appropriate notifications and follow-ups? Manual processes are slow and labor-intensive. Proof of notification is also critical to show that the company did everything in its power to inform the affected people. Creating this automated notification and auditing system after a breach has taken place is generally not feasible.

Digital communications bring huge benefits to organizations, but they also bring new data privacy challenges. Any company that is in the midst of a digital transformation cannot afford to ignore these concerns. By focusing on prevention and recovery before a breach occurs, organizations can minimize the financial and legal effects and reputational risk. Spending the time and money now can prevent a much larger problem later.

Andrew Hellard is healthcare customer communications management expert at GMC Software, a leading provider of customer communications management software. A Neopost Digital company, GMC Software provides the means for business users to develop contextual, highly individualized communications across all channels that span the entire customer journey.

###