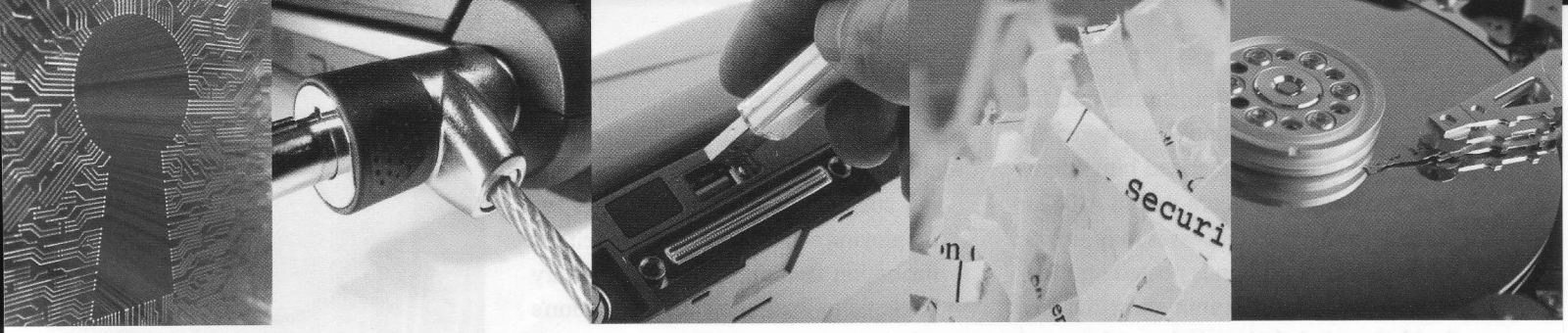


Data Privacy for Religious Institutions

After a long day of visiting ill church members in the hospital, Reverend Smith sat at a table in the cafeteria and reviewed one more time the list he keeps on his laptop of church member names, illnesses, and room numbers, just to make sure he did not forget to stop by and see anyone. Rev. Smith also took a few moments to review emails he received earlier in the day. One was from a prospective youth volunteer who had attached a copy of his driver's license, so the church could do a background check on him. Rev. Smith forwarded the email to another staff member, instructing her not to approve Greg, because he is "unreliable" and of "questionable character." Another was from a church member whom Rev. Smith was counseling due to her marital problems. He was shocked to read Ms. Shackton's confession that she is involved with another married church member. Ruminating over how to respond and in need of a cup of coffee anyway, Rev. Smith went to the counter to place an order. When he returned, his laptop was gone.

by Shannon Hartsfield Salimone and Nathan A. Adams, IV

RARELY, do churches and other religious institutions think about data privacy until confronted with an emergency like Rev. Smith's, yet people entrust some of their most confidential information to the clergy and other staff members of religious institutions. This may include financial data related to tithing, planned giving, and fundraising campaigns or personal secrets learned in counseling or confession. Evidentiary law specially protects many of these confidences. When they are disclosed anyway as a result of a data breach, Rev. Smith and others like him will reasonably be concerned about the legal ramifications, as well as the harm to those involved and to the institution's own reputation.

Secular companies have long had to comply with myriad statutes dealing with data privacy. On the federal side, banks and other financial institutions must follow the Gramm-Leach-Bliley law. In addition, the Health Insurance Portability and Accountability Act (HIPAA) regulates how certain members of the healthcare sector may use and disclose protected health information. Many schools must also comply with the Family Educational Rights and Privacy Act (FERPA). In addition, the vast majority of states have implemented their own data privacy statutes. Religious institutions are exempt from some of these laws, but their standards may, nevertheless, bear indirectly on them under the common law of negligence, defamation, and privacy.

Consider a few examples of how this could impact Rev. Smith: Ms. Shackton and her paramour will likely have even more serious marital problems if their spouses and others learn about what she told Rev. Smith. All parties concerned will be looking for somebody to blame. They may consider suing Rev. Smith, the church, and the denomination or diocese of which the church is part for negligence, defamation, invasion of privacy and emotional distress. Negligence raises the question what a reasonable person should have done in the circumstances, which indirectly relates to the standard of care secular companies are held to under the law.

Another problem will be the church members whose identities and health conditions are now known to the thief. Greg's driver's license may wind up altered with somebody else's name next to it. His identity may be used to commit crimes or purchase goods and services. Greg may seek

reimbursement from the church and file an action for defamation, because of the way Rev. Smith characterized him. Members receiving healthcare due to AIDS or sexually-transmitted diseases may also be upset if their condition is posted on Facebook. They may sue, contending that Rev. Smith invaded their privacy and caused them emotional harm. Any particular data breach or the mishandling of it may also violate local, state or federal statutes, depending upon the circumstances.

Obviously, churches and other religious institutions entrusted with personal information have as much reason as secular companies do—if not more—to take reasonable measures to ensure that the information is confidential, used only as necessary to accomplish the mission of the organization, and handled in a manner consistent with the purposes for which it was originally disclosed. Data breaches can arise in a wide variety of ways from the simplest similar to that faced by Rev. Smith to more advanced Internet hacking techniques such as perpetrated by WikiLeaks. An institution must be prepared to handle data breaches regardless of their origin.

TAKE REASONABLE PRECAUTIONS

As any institution will attest that has experienced a data breach without prior planning, it is far more expensive to deal with the aftermath than to adopt a sound data privacy protocol intended to avoid, mitigate, and deal with data breaches before they occur. The best such protocols can be detailed. You should consult with a professional about developing one right for your organization's needs, rather than trying to adopt a cookie-cutter model which could wind up doing your organization more harm than good. A few of the commonsense principles and precautions that any sound data privacy protocol will operationalize include the following:

DO NOT GATHER WHAT YOU DO NOT NEED.

Churches and other religious organizations receive sensitive information from a variety of sources. While they cannot always control the information that flows into the institution, they should use caution to avoid conducting surveys, using questionnaires, or employing other methods to solicit information that are really unnecessary in terms of furthering the institution's mission.

IMPLEMENT REASONABLE PRECAUTIONS TO KEEP INFORMATION SECURE.

If the institution does need to gather private information, it should be maintained securely and used and disclosed only for necessary purposes. The organization should implement technical, administrative and physical safeguards. Technical safeguards would involve the use of adequate passwords, firewalls, and encryption. Administra-tive safeguards include appointing someone to oversee privacy and security for the organization, and to implement and document adequate policies and procedures. Physical safeguards involve securing areas where information is housed through locked doors, locked file cabinets, and similar measures.

SECURELY DISPOSE OF DATA WHEN IT IS NO LONGER NEEDED.

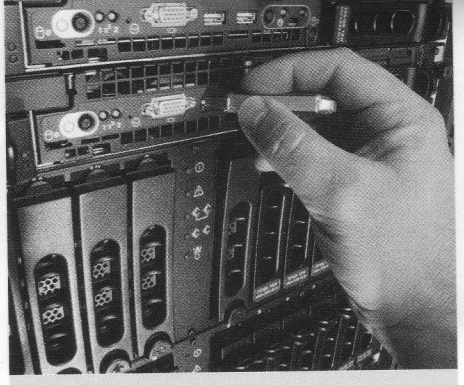
Once information is no longer needed, assuming no laws or pending litigation dictate that it be maintained, it should be discarded. Consequently, a corollary of a satisfactory data security policy is a data retention policy which defines how long each category of documents will be retained and when they should be discarded. It is critical that information be discarded in a secure manner. For example, paper records should be shredded or burned. Computer hard drives and disks should be properly wiped to remove data.

TRAIN STAFF.

An organization can have the best policies and procedures, and the most robust physical and technical security, but all of those measures are useless if staff disregards them or fails to practice the data protocols adopted by the institution, either out of ignorance or malfeasance. The policy itself will become a standard (although a more forgiving one than some juries will impose) that if not met could lead to liability against the institution. Often, data breaches are "inside jobs." Religious institutions need to have robust training programs to help minimize employee error. It is also important to monitor compliance with policies and procedures to try to guard against malicious activities.

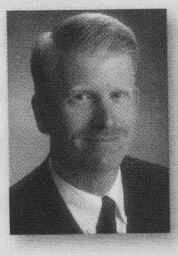
DAMAGE CONTROL FOR DATA BREACHES

From following the headlines we know that data breaches can occur notwithstanding implementation of the best data privacy plans, as a result of criminal conduct or inadvertence, but the chances can be reduced, the consequences mitigated, and an emergency plan triggered that runs on autopilot rather than haphazard. Your data



Authors

Shannon Hartsfield Salimone is a partner in the Tallahassee office of Holland & Knight. She can be reached at shannon.salimone@hklaw.com. Nathan A. Adams, IV, is a partner in the Tallahassee office of Holland & Knight. He can be reached at nathan.adams@hklaw.com.



privacy protocol needs to plan for emergencies and will usually incorporate at least three damage control stages.

GATHER DATA

When dealing with a data breach, the first step is to gather as many facts as feasible about the extent of the breach as quickly as possible. In the example above, Rev. Smith needs to determine, as best he can, exactly what personal information was on the hard drive that could be accessible to the thief. If a data protocol was followed prior to the breach, it will be much easier to grasp the extent of a breach than otherwise, because the baseline should be fixed by policy.

DIAGNOSE YOUR EXPOSURE

Once the scope of the breach is diagnosed, the next step is to consult with outside experts to determine what violations of law may be implicated, the potential extent of the risk, and what can be done to mitigate the harm. In the scenario described above, although the laptop contained a significant amount of health information, it is unlikely that HIPAA applies, because the stolen information was not held by a health care provider or health plan. In contrast, HIPAA would likely apply if Rev. Smith received the information in his role as a hospital staff member, such as a chaplain.

NOTIFY AFFECTED PERSONS AS REQUIRED

If the laptop was not encrypted and information contained in it is vulnerable to unauthorized access, state law may require notifying the individuals who are the subject of the data, as well as law enforcement. Florida is one state that has a breach notification law. In Florida, if there is a breach in the security of a computerized system containing names and social security numbers, drivers' license numbers, or certain other information, individuals must be notified within 45 days. Failure to provide the required notice may result in administrative fines as high as $500,000. Consequently, time is of the essence.

CONCLUSION

Data privacy is a concern for secular and religious institutions alike and likely to become even more critical and complex with the progress of the digital revolution. Not all data privacy statutes are applicable to religious institutions, but the standards that they set are indirectly applicable under the common law. Parishioners of churches, no less than clients of businesses, have come to expect a certain level of data privacy. Consequently, it is more important than ever to adopt sound data privacy policies with the assistance of professionals and to take reasonable measures to ensure confidential information is protected.