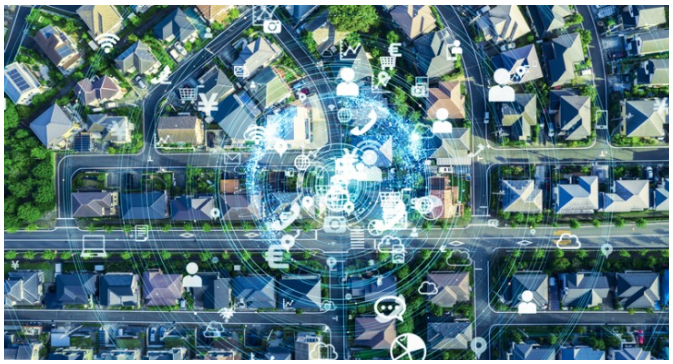
WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Privacy and Data Security for HOAs: What Your Community Association Needs to Know

Written By **Angela P. Doughty, CIPP/US** (apd@wardandsmith.com)
June 30, 2021



Privacy and Data Security is the body of law that addresses how an organization can collect, handle, and use personally identifiable information and how that information needs to be protected.

Community Associations quite often have and maintain the names, addresses, and financial information of their residents and homeowners. Many criminal groups find this kind of information valuable for identity theft. Such groups often encrypt the data so the Community Association cannot access it to gain leverage and force an organization to pay a "ransom" for its return. Because of this and in reaction to how much sensitive information is held on everyday people in the broader economy, all fifty states have laws on the books that require most organizations to disclose when an unauthorized party has accessed the information. Community Associations—just like any other North Carolina organization—always must act reasonably when the organization makes decisions to do something with personal information or risk negligence lawsuits and class actions.

Unfortunately, North Carolina does not provide statutory guidance on how Community Associations can act reasonably with respect to residents' personal data, but the federal government has provided frameworks that it recommends. The National Institute of Standards and Technology has published a Privacy Framework and a Cybersecurity Framework that, when followed, allow organizations to identify the data they have, protect that information, control and manage the data, govern the data with set rules within the organization, communicate the roles of each member of the organization, detect malicious or unauthorized activity, respond when an incident occurs, and recover from the incident.

There are a number of practical steps that organizations can take that can avoid or reduce the severity of common compliance pitfalls. The first is to review vendor contracts regularly—at least once a year—to make sure that they reflect an organization's risk tolerance. Often, a trusted service provider or another vendor can have a breach that impacts the privacy and security of the data entrusted to a Community Association. Without contractual protections, the organization might incur significant costs remediating the problem with little legal recourse to have those costs covered by the party at fault.

Additionally, encrypting data, which is a mathematical process to transform data from readable text to nonsense and back again when a code (called a key) is used, can be an important tool in the compliance

toolbox for Community Associations. Under North Carolina law—and the law of many other states—a breach only triggers reporting obligations when the information that was stolen was also unencrypted or when the encryption key was stolen with the data. This is not a silver bullet but, encryption is a practical technology that will be an important part of any compliance strategy.

Cyber insurance can also be an effective means of covering risk. However, insurance is not as simple as buying a policy and calling it a day. Insurers are increasingly raising premiums and lowering caps on organizations that do not take a proactive approach to mitigate privacy and security risks. So, while insurance can act as a hedge against devastating effects, it should not be seen as a substitute for a compliance strategy.

We also recommend getting community input on the Community Association's Privacy and Data Security efforts. Community Associations are necessarily accountable to their residents and homeowners, so understanding stakeholders' risk tolerance can inform the leadership on how to move forward with a compliance strategy. The laws at issue obviously do not change based on the community's sentiments, but discussing the matter at an annual meeting can be a good way to communicate what expectations the stakeholders in your community have of leadership.

Challenges and risks of liability and unmet stakeholder expectations are everywhere for Community Associations that do not take a proactive approach to the Privacy and Data Security of their residents' and homeowners' information. To better understand these challenges and risks and avoid them in the future, please contact us.

--