This article presents general guidelines for Georgia nonprofit organizations as of the date written, and should be not be construed as legal advice. Always consult an attorney to address your particular situation.

Protecting Confidential Information – Five Steps to Consider

By Michael Bertelson, Esq.[1]

Nonprofits, like all organizations, collect and create information that is valuable to the organization and important to maintain in confidence. Examples include client information (including personal and medical information), donor information, personal information (about board members, volunteers, or employees), as well as other business and financial information that needs to be protected. The following are steps organizations should consider in protecting confidential information.

(1) Identify what information needs to be maintained in confidence.

As a first step, identify what non-public information the organization is collecting or creating, and consider whether each type or category of information should be protected as confidential. Some information may warrant protection simply due to its value to the organization in not being known outside the organization. Other information may warrant protection based on an expectation of privacy by the persons disclosing that information (e.g. client or donor personal information), for public relations reasons, or because of laws or standards that require protection of the information, such as the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Payment Card Industry Data Security Standards (PCI DSS).[2]

For each type or category of information that warrants protection, consider:

- why that information is collected;
- how that information is used;
- where that information is maintained;
- who has access to that information;

[1] Michael Bertelson is a partner in the Atlanta office of Kilpatrick, Townsend, and Stockton LLP. His practice focuses on intellectual property law.

[2] Compliance with HIPAA, PCI DSS, and other privacy laws and data security standards is beyond this scope of this brief article. For more information, see for example "HIPAA Basics for Non-Profits" by Joseph E. Kennedy (https://www.pbpatl.org/wp-content/uploads/2014/05/HIPAA.pdf) and "Data Security Is Important for All Organizations, including Nonprofits" by Kevin Coy (https://www.pbpatl.org/wp-content/uploads/2015/09/Data-Security.pdf).

Dated: 2/27/2018
www.pbpatl.org
© 2018 Pro Bono Partnership of Atlanta, Inc. All rights reserved.

- how that information is currently protected, if at all; and
- whether there are laws, regulations, or standards governing what steps must be taken to protect that information (e.g. HIPAA or PCI DSS).

(2) Develop and implement a written policy on confidential information.

The organization should have a written policy on confidential information. The policy should specify what information should be maintained in confidence, how that information will be protected, who will have access to that information, and in what, if any, circumstances that information can be disclosed or used outside of the organization.

Obviously, the best written policy is not worth much if it is not implemented. Implementation should include providing and explaining the policy to everyone in the organization, so that everyone can understand what information is confidential and the importance of maintaining the confidentiality of that information.

(3) Include confidentiality provisions in employment agreements, and consider non-disclosure agreements for directors, volunteers, vendors, and others.

It is critical to obtain enforceable agreements from employees and others who work within the organization requiring them to maintain the organization's confidential information in confidence. The reason these agreements are necessary is because, in many instances, there is no legal protection for confidential information without a contractual obligation. One exception is trade secrets, which are legally protectable even without confidentiality agreements; however, much of the organization's confidential information will likely not qualify as "trade secret" under the applicable laws.

The confidentiality provisions of the agreement should specify exactly what types of information of the organization are confidential and what the restrictions are on the use and disclosure of that information. The agreement should make clear that these restrictions apply both during employment and after employment.

Confidentiality or non-disclosure agreements should also be considered for anyone else who works with the organization and comes into contact with confidential information, which may include directors, volunteers, consultants, and vendors. While many consultants and vendors will have form service agreements, those agreements often will not include confidentiality provisions protecting the organization.

While there are numerous form confidentiality and non-disclosure agreements available on the internet, there is usually not a form agreement that will be perfect for your organization.

© 2018 Pro Bono Partnership of Atlanta, Inc. All rights reserved.

Care should be taken to customize or develop a confidentiality agreement that works for your particular organization.

(4) Label Confidential Information As Confidential, and Restrict Access

People will not know to take steps to protect information as confidential if they do not know it is confidential in the first place. The confidentiality of information will not necessarily be obvious to everyone who comes in contact with it. A simple, but important, step in protecting the organization's confidential information is to clearly label or mark confidential information as "confidential – do not distribute" or in a similar manner.

The organization should also limit as much as possible the places where confidential information is stored and maintained. Access to confidential information should be restricted to only people who need to access it. Physically locked cabinets, passwords, and encryption are all effective mechanisms for limiting access. Particular care should be taken if confidential information can be remotely accessed (e.g. through network or website connectivity) or if it will be physically taken outside of the organization (e.g. on a laptop or USB drive). Consider working with an IT security vendor to make sure the appropriate encryption software, firewalls, anti-virus software, remote drive wiping software, etc. is in place.

(5) Train employees on how to protect confidential information, and periodically revisit confidentiality provisions and policies.

Periodic training to remind employees and others at the organization of what information is confidential and how it must be handled is important. It is also important to periodically revisit and update confidentiality policies and provisions to ensure that they remain relevant to what confidential information the organization is collecting and generating, how it is using that information, and what restrictions need to be in place on the use of that information.

If you have questions about the protection or use of confidential information, or if you need assistance drafting appropriate agreements, please seek legal counsel.

Dated: 2/27/2018
www.pbpatl.org
© 2018 Pro Bono Partnership of Atlanta, Inc. All rights reserved.