CAPLAW enews brief

10 Data Security Tips to Protect Your CAA

By Christine Park and Veronica Zhang, Esq.
February 2018

Community Action Agencies (CAAs) constantly collect and store information relating to clients, employees, donors, and other stakeholders. This information often includes sensitive and confidential data that is subject to a variety of federal and state privacy protections. In light of recurring high-profile data breaches and inadvertent disclosures of confidential information, CAAs should take steps to evaluate and mitigate their data security risks.

The following are some recommended practices to help avoid data breaches and the accidental disclosure or release of confidential information. Rather than address the myriad of privacy requirements that could possibly apply to each individual CAA, the recommendations provide a general framework within which a CAA can begin building/customizing its data privacy protections. A CAA should work with local counsel to identify and ensure compliance with state-specific data privacy requirements as well as other requirements that may apply to a CAA because of the state, federal, and private funding it receives.

1. **Identify sensitive data and restrict access to it.** Determine which data contains sensitive or confidential information, such as employee, client, and financial information, and who has (or could have) access to it. The best way to protect personal information is to understand what information is collected and how it flows through the organization. Minimize the number of employees and/or vendors who have the keys, codes, or passwords to access that data, and keep a detailed inventory of who has access, granting it on a need-to-know basis only. When an employee leaves the organization, make sure to immediately change the codes and passwords to ensure that the information remains secure.

2. **Encrypting and regularly backing up data** are two of the easiest and most effective data security methods available. Encrypting data will translate data into another form, making it unreadable, and ensures that only the person with the decryption key can read the data. While encryption is not invulnerable against hackers, it does provide an extra layer of security if a strong password (see Tip #9) is used. Note, however, that if you forget the password that you used, you may never be able to recover the data. After encrypting the data, back it up regularly to an offsite location. All it can take is one small accident, virus, or hard drive failure for data to become lost or destroyed. It is essential that you back up your information and have a plan for recovering from a system failure. If you are

using an outside vendor, such as a cloud storage service, ensure that the contract with the vendor contains a provision stipulating the vendor's responsibilities regarding the data.

3 **Deleting unnecessary data and wiping data** minimizes the amount of confidential information that may be released if your security is compromised. Note that simply deleting data on a computing device rarely means that it is permanently removed. Ensure that the data no longer exists on a computer hard drive by overwriting and wiping the hard drive so that it cannot be recovered. If recordkeeping retention periods have passed such that your organization is no longer required to keep the confidential information, consider deleting it. Also be sure to clear or overwrite the memory of your organization's copiers, scanners, printers, and fax machines at the end of any lease, as these machines retain information that may include confidential data stored during use. Make sure to check all applicable federal, state or local recordkeeping retention laws to be sure that there are no continuing obligations to store the data.

Note that simply deleting data on a computing device rarely means that it is permanently removed.

4 **Installing malware detection software** can prevent, detect and remove malicious software. Malware is malicious software that is intended to harm data, devices, or people. Malware includes spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer. Malware detection software scans files to check if it is a "legitimate" file. If the software identifies the file as malware, the access operation will be stopped, the file will be dealt with by the scan in a pre-defined way (based on how you configure the anti-virus program), and the user will be notified.

5 **Make sure to use secure internet connections**. Public Wi-Fi connections (e.g., coffee shop, airport, and hotel free Wi-Fi) are typically not secure because they require little or no authentication to establish a network connection. Unsecured connections provide opportunities for hackers to obtain access to data on the device that you are using during that time. If you need to work outside the office, try to limit the use of confidential information when connected to a public unsecured Wi-Fi network. Also, using a Virtual Private Network (VPN), which encrypts traffic between a device and the VPN server, makes it more difficult for an outside intruder to look at data on an unsecured connection. Both free and paid VPN services are available.

6 **Check and say YES to updates**. Although it may not always seem necessary to update programs as soon as an update becomes available, it is an easy way to keep data more secure. Software companies often develop updates to patch identified security vulnerabilities. However, this also alerts potential outside intruders that there are vulnerabilities in the software, which can lead to targeted data breaches on systems that have not installed the update. For example, the WannaCry ransomware attack in May 2017 was a worldwide cyberattack that targeted computers running Microsoft Windows operating systems. The attack essentially held the targeted computer's data for ransom, and would not allow the computer owner to access to data without payment. Systems that had not installed Microsoft's latest security updates were particularly vulnerable to and affected by the attack.

7 **Using strong passwords** is a basic yet important way to secure data. In 2016, the most common password was "123456", followed by "123456789".[1] An easy way to create a secure password is to put together four random common words that are easy to remember. For example, putting the words "correct," "horse," "battery," and "staple" together creates an easy to remember 25-character password that is difficult to guess

through attacks that use every possible combination of letters, digits, and special symbols to determine the password. Using a password manager that will automatically create and store secure passwords is another method to keep track of passwords for various applications. Other password protection measures include policies that prohibit employees from sharing passwords, password-activated screens that lock computers after a period of inactivity or a certain number of login attempts, and system protocols that require users to change their passwords on a regular basis.

8 **Watch out for phishes**. Phishes are attempts to obtain financial or other confidential information from Internet users, typically through an e-mail that looks as if it is from a legitimate organization (often one that the user trusts or recognizes), but contains a link to a fake website that replicates the real one. These scams pose as banks, credit card companies, tax software providers, or government agencies and attempt to bait users to provide money, passwords, Social Security numbers, and other information that can lead to identity theft. The IRS reported a significant uptick in phishing scams during the 2016 tax season.[2] While e-mails from less sophisticated phishing schemes are often riddled with spelling and grammatical errors, there are also more sophisticated “spear phishing” attacks that directly target an individual using personal information that may also be publicly available (e.g., the individual’s name, school, location, etc.). For example, in an incident in 2017, a law firm was duped into wiring over a half million dollars to e-mail scammers after receiving phishing e-mails that the firm thought were from a well-known company administrating a class action settlement fund, for which the funds were intended. The e-mails, which appeared to come from a trusted source, instructed the firm to wire money to a particular address, and the funds then promptly disappeared.

9 **Training staff on the importance of data security** is essential and perhaps the best way to protect against data breaches. All it takes is for one staff member to fall for a phishing scam or download malware onto the organization’s computer for a security breach to occur. Or, a staff member may store confidential information onto a personal device that is lost, stolen, or hacked into. Train employees to be aware of potential security issues when using an organizational device such as a laptop or phone outside the office. Ask every employee to sign an agreement to follow your organization’s confidentiality policy and security standards for handling sensitive data.

10 **Have a plan for responding to data breaches**. A security breach can happen in spite of the best safeguards. To reduce the impact of a data breach, develop a plan to respond to these incidents and designate a senior staff member to coordinate and implement the plan. The plan should include investigating security breaches immediately and taking necessary steps to mitigate the disclosure of confidential information (for example, disconnecting a compromised computer from the CAA’s network or triggering an auto-destroy function on a phone that is reported stolen). Consider the parties that you may need to notify in case of a breach, including the individuals whose information was breached, law enforcement, credit bureaus, and other state or federal regulatory agencies. Also be sure to consult with an attorney on how to respond to a data breach.

Footnotes:

1. “The world’s most popular password is depressingly easy to guess,” Business Insider (Jan. 16, 2017)
2. “Phishing Schemes Lead the IRS “Dirty Dozen” List of Tax Scams for 2017; Remain Tax-Time Threat,” IRS (Feb. 1, 2017),

This eNews brief is part of the Community Services Block Grant (CSBG) Legal Training and Technical Assistance (T/TA) Center. It was created by Community Action Program Legal Services, Inc. (CAPLAW) in the performance of the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Community Services Cooperative Agreement – Grant Award Number 90ET0467-01-00. Any opinion, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Health and Human Services, Administration for Children and Families.

The contents of this publication are intended to convey general information only and do not constitute legal advice. Any communication through this publication or through CAPLAW's website does not constitute or create an attorney-client relationship. If you need legal advice, please contact CAPLAW or another attorney directly.