CAPLAW enews brief

Is Your Head in the Cloud? Contemplating Cloud Computing for Community Action Agencies

By Emily Center and Veronica Zhang, Esq.
August 2019

Cloud computing is rapidly increasing as one of the most cost effective and efficient ways to conduct business. A Community Action Agency (CAA) looking to add, renew, or upgrade its existing software platform is likely, now more than ever, to consider cloud-based solutions. As of 2012, 90% of nonprofits across the world were using some type of cloud technology, with the most frequently used services being email (55%), social networking/internet (47%), file storage/sharing (26%), web conferencing (24%), and office productivity (23%).[1]

To help CAAs better understand the benefits and risks of cloud computing, this article highlights the key differences between cloud-based applications and traditional hosted software, with a focus on the potential impact that cloud software may have on a CAA's operations and data security. It discusses reasons your CAA may decide to adopt a cloud model. Finally, the article provides a checklist of issues for your CAA to consider negotiating in its agreement with a cloud provider, to ensure your CAA and its data are sufficiently protected.

What is Cloud Computing and How is it Different from Traditional Software?

Cloud computing is any application or service offered over the internet. Examples of cloud services range from Gmail to Dropbox, Facebook, and Skype. These services are hosted at data centers all over the world, which are collectively called "the cloud". The cloud is a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources that can be quickly deployed and used with minimal management.

With traditional software, the CAA buys a specific number of licenses for each product, such as Microsoft Office, and each license typically entitles the user to physically install the software on a single computer (for example, an employee's work computer). The employee is not able to access Microsoft Office from his or her home computer or laptop, because the software is only accessible via the work computer's physical hardware.

With cloud computing, one employee with one login can access cloud-based software from anywhere with an internet connection. The cloud allows for this flexibility because the software is kept on a remote server and managed by the cloud provider, off premises, and is simply accessed by CAA employees via the internet.

Other key differences between traditional hosted software and cloud services include:

	Cloud Services	Traditional Hosted Software
Installation	Immediately available for use after registration and login	Requires on-site installation of software license on a physical computer
Access	Via the internet to software hosted on an off-site server	Via the software installed on the physical computer or an internal server
Software Compatibility	Option to sync data with other cloud software	More limited capability to sync with other software programs
Collaboration	Different users can access the same data at the same time	Shared access is limited
Mobility	Mobile software	Immobile software
Protection	Protected data in off-site locations	Data stored in-house and subject to organization's security systems
Power	Eliminates hardware and saves power	Requires server room that consumes power

Is Moving to the Cloud the Right Decision for My Organization?

In determining if a cloud services model is right for your organization, it is helpful to understand and weigh the key advantages and disadvantages experienced by others. We've identified ones that are likely most relevant to CAAs.

Key Advantages

Administration	Cost	Partnership	Data
+ Increases efficiency and access to software (e.g., all files stored in a central, accessible location) + Deploys rapidly + Enables easier disaster recovery + Reduces system administration/ easier to manage (cloud provider has team of on-staff professionals) + Bypasses risk of buying software that may soon be obsolete	+ Reduces operational costs (CAA no longer pays for in-house server and may reduce IT personnel) + Shifts IT expenditure to a pay-as-you-go model + Increases investment in more innovative digital services (i.e., spending fewer resources to maintain current systems) + Reduces carbon footprint (by aggregating data in efficient data centers, less equipment and energy is used)	+ Increases employee collaboration (e.g., multiple users often able to access project or file simultaneously) + Provides mobility and off-site access (employees can work from any location) + Enhances ability to partner with other organizations	+ Improves data security (if laptop stolen, data still in cloud) + Increases focus on data security (cloud provider's business model devotes resources to protecting data) + Enables better data organization

Key Disadvantages

Lack of Knowledge	Cost	Data Security	Lack of Trust	Noncontrollable Externalities
- Organization may not be technical enough to fully understand pros and cons - No management support for adopting cloud services - No funder support for adopting cloud services	- Ongoing monthly costs - Migration costs (initial cost to move to cloud, and additional cost if switching cloud providers) - Increased internet costs (need reliable connection)	- Subject to service provider's capability and technology - Vulnerable to possible cyber incident/data breach - Sensitive business information given to third-party provider	- Cloud not yet fully dependable - Lack of in-house control (i.e., no server) - Service continuity contingent on third-party (down time may occur during workday or important times)	- Lack of consistent Internet connectivity affects performance - Need bandwidth for increased online traffic - Integration issues (existing system may not integrate well with the cloud system) - Funding source and government data protections

Considering these advantages and disadvantages, a CAA that is likely ready to move to the cloud is one:

- With a reliable internet connection and bandwidth
- Ready for a software update
- With employees willing to adapt to new technologies
- Concerned about upgrading hardware to keep up with software installations
- Seeking to reduce its carbon footprint
- Able to be flexible so it can respond to fluctuations in services and software needs

Conversely, for a CAA that needs customized software and uses and stores data subject to strict privacy or confidentiality requirements, a complete move to the cloud may not be the right decision. Rather, the CAA may consider a more incremental move such as adopting a cloud services model that is used for storing non-sensitive data and maintaining in-house servers for sensitive data.

What Steps Can CAAs Take to Help Mitigate Risk When Moving to Cloud Computing?

CAAs can take a number of key steps when moving to a cloud-based software model to help mitigate the risks associated with cloud computing.

Select the right cloud provider

When selecting a cloud provider, include those members of your team who will be most impacted by the decision as they likely know best the needs of the organization and the issues that a cloud-based model would address. The team would weigh the advantages and

disadvantages of the options within the context of your organization's operations and create a list of services it is seeking, as well as address topics such as the:

- degree of configurability, i.e., how much you can customize the services?
- scalability, i.e., how many users?
- collaboration, i.e., can multiple users collaborate on a single project?
- required integrations and systems compatibility, i.e., are there data, software, or applications that need to link to the cloud, and how seamlessly will they integrate with the cloud application's functions?

The team should consider using the Key Provisions and Issues Checklist below to identify initial screening questions, and send all questions/requirements to the different cloud providers. Most software companies offer trial periods or demos, and, while not customized, they will likely give your team an idea of a particular software's capabilities and functionality.

Negotiate the terms of the contract with the cloud provider

Even though cloud providers mostly use templates or form agreements, your team should still attempt to negotiate for provisions important to your organization, especially those providing additional protections. Again, the team could begin identifying issues using the Key Provisions and Issues Checklist as well as the Data Privacy and Security overview below. In particular, the termination options in the Checklist and the data restrictions in the overview are often dictated by the different funding a CAA receives and need to be reflected in either the contract provisions or addendum.

Maintain the proper internal controls

Proactively adjusting your CAA's approach to risk mitigation to account for the challenges associated with cloud computing is another key way to successfully transition to a new system. Employees should receive training on the features and functions of the software to ensure they understand the risks of cloud applications and are knowledgeable about the best practices for keeping data secure.

Other steps a CAA can take include:

- Updating its data security policy for the use of cloud services and reviewing the policy annually, as well as any time the data environment changes, e.g., different data is obtained or new requirements apply;
- Tracking purchased licenses and actual usage to monitor whether the CAA is maximizing its cloud subscription and making adjustments as necessary; and
- Backing up data, storing it in multiple places and including these approaches in policies to ensure that data is available and accessible.

What Key Provisions Should CAAs Focus on When Negotiating a Cloud Computing Contract?

Most providers will provide you with a form agreement that your CAA should approach as a starting point. Look at the form and identify any key issues, based on your CAA's discussions of its needs and concerns. The following checklist is intended to help your CAA identify and think through areas of concern and priority that will guide your negotiation strategy.

Key Provisions and Issues Checklist:

- [ ] License model: How many users are entitled to use each license? Are your subcontractors authorized to use the application? Some applications are licensed on a per-user basis, while others are per-device, and still others offer certain levels (standard, gold, platinum, etc.). Determine which model best fits the way your CAA intends to use the software.

- [ ] Fee structure: Are fees based on the number of users or devices? Does your CAA have the ability to adjust the number of users on a regular basis to reflect its actual use? Are there any caps on future price increases?

- [ ] Service levels and uptime: What is the amount of time the cloud service will be up and running and available to use? Ensure that these levels align with your CAA's expectations and what you need to conduct your operations. The provider should agree to a minimum uptime, or percentage availability measured over an agreed-upon period. What are the consequences if this uptime is not met? This typically takes the form of credits towards the CAA's bill for the next service period.

- [ ] Service availability and business continuity: Will the software continue to be available in the event of a disaster, power outage, or loss of the provider's server? Include disaster recovery and business continuity provisions requiring the provider to continue making the cloud services available through a secondary server or data center, as appropriate.

- [ ] Response time when service problems occur: Is the cloud provider required to respond and begin working on your CAA's reported service problem within a certain period of time? Is the cloud provider required to actually resolve the problem, or come up with an alternate solution, within a specified period of time?

- [ ] Data ownership: The contract should clearly state that the CAA is the sole and exclusive owner of the data uploaded, submitted, transferred, or otherwise provided by the CAA to the cloud software.

- [ ] Data sharing and use rights: Because the CAA's data is stored on the cloud provider's server, the agreement should specifically cover the rights of the cloud service provider to use, aggregate, manipulate, or share customer data for other purposes, including for marketing purposes. Generally speaking, the agreement should state that the provider must maintain the confidentiality of the CAA's information and limit the provider's use of the information to that which is necessary for the provider to perform its obligations under the cloud computing agreement. The CAA should also ask where its data will be stored (in the U.S. or overseas, and if outside the U.S., which country). Certain sensitive data may be subject to stricter security requirements if stored outside the U.S., and the data privacy rules of those countries may apply.

- [ ] Data privacy and security: How will the cloud service provider protect the security and confidentiality of your CAA's data? The contract should specify a schedule for the cloud provider to perform and test backups. For more information about specific data privacy and security requirements that may apply to CAAs, see the Data Privacy and Security overview below.

- [ ] Security audit rights: Can your CAA have independent third party auditors audit the cloud provider against the CAA's internal controls? Audits can be done based on certain standards, such as the International Standards Organization (ISO), which certifies that the cloud provider meets quality, safety and efficiency measures set by the ISO.

- [ ] Data breach: What is the definition of a data breach? When is the provider required to notify your CAA of a data breach? If the provider is at fault for the breach, is it required to reimburse your CAA for its reasonable out-of-pocket costs for notifying any employees, donors, clients, or volunteers whose personal information may have been disclosed during the breach?

- [ ] Software updates: What is the frequency of software updates? Are those updates mandatory, or do your users have to opt-in to install the updates? Does the provider need to give your CAA notice of software changes?

- [ ] Insurance: The cloud contract should address the insurance carried by each party. Since your CAA will likely be liable for a security breach, even if the provider was at fault, your CAA should consider obtaining a cyber-liability insurance policy. Such insurance protects the CAA from a range of losses such as a data breach, theft or destruction of data, and potentially privacy breaches related to theft of personal information. The CAA should also consider requiring the cloud provider to maintain insurance, such as technology errors and omissions liability insurance and coverage against electronic and computer crime or unauthorized computer access. Consider asking the cloud provider to add the CAA as an additional insured party.

- [ ] Limitation of liability: A limitation of liability clause limits the amount of exposure a cloud provider will have if a lawsuit or other claim is filed against the cloud provider. Will there be a cap on the amount of damages the cloud provider will have to pay if your CAA sues for breach of the cloud services contract? Typically, a cloud provider will limit their liability to a certain amount (e.g., the fees paid by the CAA over the last 12 months). Will the limitation of liability apply both ways, limiting the amount of money your CAA may have to expend if sued? Are there any circumstances in which the limitation of liability does not apply? CAAs should push to exclude certain breaches by the cloud provider from this liability cap such as breach of confidentiality and security obligations.

- [ ] Indemnification: The cloud provider should agree to defend your CAA from claims or lawsuits by third parties that result from a breach of the cloud provider's obligations. Your CAA should be fully protected from any claim resulting from an intentional confidentiality or data security breach. If the breach is unintentional, the cloud provider may require a cap on how much money it will expend to defend your CAA from third party lawsuits. The cloud provider should also defend your CAA if it is sued by a third party claiming that the provider's software, and your subsequent use of it, infringes the third party's intellectual property rights.

- [ ] Termination rights: Can either or both the CAA and the cloud provider terminate for convenience? Are there any cancellation penalties? The CAA should ensure that it can terminate the agreement if its funding is reduced or terminated, as well as for breach of the contract by the cloud provider.

- ☐ Term: Does the CAA get any discounts for committing to a longer initial term? Does the license automatically renew?
- ☐ Fee disputes: Will the cloud provider guarantee that it will not withhold cloud services to your CAA (e.g., in the case of a pending dispute over fees)?
- ☐ Transfer of data: Confirm whether and how your CAA's existing data can be imported into the provider's services at the beginning of the agreement, as well as how the CAA's data will be returned at the end of the agreement. What role will the cloud provider play in data transfer? How will your CAA interact with your previous cloud provider when transferring data to another cloud provider? How can your CAA extract its data, and in what format will the data come? After the transfer, will the cloud provider delete the data? Will your CAA have the continued right to use deliverables, such as reports, after your relationship with a previous cloud provider comes to an end?
- ☐ Publicity and use of the CAA's name and logo: The cloud provider should be prohibited from making any public announcements relating to your CAA's decision to enter into a cloud services agreement. Your CAA should also require that the cloud provider obtain your CAA's written consent before using its name and logo.
- ☐ Training: Does the cloud provider offer any training on the software, including when updates are issued?

What are the Data Privacy and Security Concerns Generally Facing a CAA?

Because cloud-based services store data in a server hosted by a third-party, a CAA must understand the requirements applicable to the types of data the cloud provider has access to and whether sufficient levels of security exist. In the event of a breach, a CAA is ultimately the party responsible for complying with applicable rules.

Generally, federal or state data privacy law will define what is often referred to as personally identifiable information (PII), but generally speaking, PII is information that can, either on its own or in combination with other specified pieces of data, identify an individual. For example, the definition of "personal information" under the Massachusetts data protection law, M.G.L. ch. 93H, and implementing regulations, 201 C.M.R. 17.00, is a person's first name and last name, or first initial and last name in combination with any of the following for that person: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number.

Two strategies for managing data security are encryption and de-identification. First, data can be stored on the cloud in encrypted form. The methods used to decrypt and access data must be kept within the CAA's control (i.e., not in the cloud), since encrypted data is not secure if both the data and the keys used to decrypt that data are both stored in the cloud. Second, the CAA can use de-identification by anonymizing the data in the cloud using some type of referencing system. While all of the data would be stored in the cloud, personal information would be stored only as reference values.

Below is a brief overview of some of the federal and state data privacy rules that could apply to CAAs. Please note that your CAA should consult with local counsel knowledgeable about these requirements to determine whether the organization is subject to these and potentially other data security rules and to assist with your compliance approach.

Health Insurance Portability and Accountability Act (HIPAA)

Some CAAs obtain health information when providing services to clients. Just because the CAA handles medical information, however, does not mean that it is subject to HIPAA. HIPAA establishes protections for protected health information (PHI) that is created, received, maintained, or transmitted by a HIPAA "covered entity" or "business associate." "Covered entities" include certain health care providers, health plans, and health care clearinghouses. More specifically, only health care providers who bill for their services using an electronic transaction are covered. For example, a CAA that provides health care services using grant funds but does not bill the client's insurers is not a HIPAA covered entity. Further, a CAA that uses email to communicate PHI but does not conduct electronic billing transactions also is not a HIPAA covered entity.

If your CAA is a covered entity, it must comply with HIPAA privacy and security regulations with respect to the CAA's use of PHI. PHI is defined as information that singly or in combination identifies a person and relates to the past, present, or future: (1) physical or mental health or condition of that person; (2) provision of health care to that person; or (3) payment for provision of health care to that person.

Further, when a covered CAA engages the services of a cloud provider, the provider becomes a "business associate" under HIPAA. A covered CAA must enter into a HIPAA-compliant business associate agreement with the cloud service provider. HHS has issued guidance on Business Associate Agreements, including providing sample provisions to include in these agreements.

Data Privacy Rules under the Head Start Program Performance Standards (Part 1303, Subpart C)

The Head Start Program Performance Standards (HSPPS) that were updated in 2016 included new rules on a Head Start and Early Head Start grantee's obligation to safeguard the privacy of personally identifiable information in child records. When entering into a cloud computing contract, a CAA with a Head Start program must ensure that the cloud provider is familiar with the procedures established by the CAA to protect the confidentiality of any such data in child records. The HSPPS rules explicitly require programs that use a web-based data system to maintain the child records to ensure that the system adequately protects and maintains such records according to current industry security standards.[2]

Further, HSPPS rules require Head Start grantees who establish written agreements with third parties relating to the disclosure of PII from child records to conduct an annual review of the agreement and if necessary, update the agreement. If the third party (i.e., the cloud provider) violates the agreement, then the grantee may: (1) allow the third party an opportunity to self-correct; or (2) prohibit the third party from accessing the records for a time period established by the program's governing body and policy council.[3] Parents of Head Start children have the right to review any written agreements with third parties addressing the PII of their child's record.[4] CAAs with Head Start programs should ensure that contracts with cloud providers for software used in connection with the Head Start program do not have restrictions on who the CAA can share the agreement with, or at least explicitly permit Head Start parents to view the agreement.

Other Federal Data Protection Laws

No single, comprehensive federal statute protecting PII or governing privacy exists. Instead, a patchwork of laws primarily regulates certain industries and types of data. The ones that are most likely applicable to CAAs include:

- Children's Online Privacy Protection Act (15 U.S.C. § 6501 *et seq.*): Protects the privacy of children under 13 on the internet.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act, 15 U.S.C. § 7701 *et seq.*): Regulates email marketing.
- Fair Credit Reporting Act (15 U.S.C. § 1681): Regulates the collection and use of credit information and access to credit information.
- Federal Trade Commission (FTC) Telemarketing Sales Rules (15 U.S.C. § 6101 *et seq.*): Applies to interstate calls made by for-profit telemarketers to solicit charitable contributions, requiring telemarketers to disclose that the purpose of the call is to ask for a donation, maintain internal do-not-call lists, and prohibit calls before 8 am or after 9 pm.
- PCI Data Security Standard (PCI DSS v3.2.1): Requires organizations processing credit card payments to put in place certain technical and operational systems, including firewalls, access controls, monitoring, and encryption of cardholder data during transmission and storage.
- Telephone Consumer Protection Act (TCPA, 47 U.S.C. § 227 *et seq.*): Generally requires prior express consent for calls made using automated technology or with an artificial or prerecorded voice.

State Data Security Law

State data security laws vary. Some states such as California have passed fairly restrictive rules[5], while other states have relatively little regulation. Many states have data security laws that require entities that own, license or maintain personal information about a resident of that state to implement and maintain reasonable security procedures and practices appropriate to the information they are collecting and processing. These laws may apply to nonprofit organizations and provide for monetary penalties for violations.

In light of recent high-profile data breaches, the trend is towards states passing more restrictive data privacy laws. Current state laws cover a number of issues, including giving consumers a right of action, access rights, the right to receive personal data they have provided, and the right to elect not to have their information sold.

The decision to move to the cloud is complex, and CAAs have to consider a host of issues — from negotiating for the right services and protections to ensuring the CAA has the necessary internal controls and policies to safeguard sensitive data when using cloud-based software. It is critical that your CAA engage an attorney when reviewing and entering into a new cloud-based software agreement. We encourage you to reach out to CAPLAW if you need assistance identifying a local attorney.

---

[1] *2012 Global Cloud Computing Survey Results*, TechSoup Global (Sept. 2012), available at https://www.techsoup.bg/sites/default/files/2012%20Global%20Cloud%20Survey%20Full%20Report_2.pdf.

[2] 45 C.F.R. § 1303.24.

[3] 45 C.F.R. § 1303.22(d).

[4] 45 C.F.R. § 1303.23(e).

[5] California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*