# In-House Products
# vs.
# Cloud-Based Services

With the growth in cloud-based services, domestic violence and sexual assault advocacy agencies face the decision to either move to these low-cost and low-maintenance systems or to maintain their own IT equipment and software. The key considerations in this decision are survivor safety and privacy, and the agency's confidentiality obligations. This guide is intended to assist agencies in thinking through the benefits and risks of each approach.

## Cloud-Based Services

Cloud-based products can include data storage services, such as Dropbox, Google Drive, iDrive, Microsoft OneDrive; cloud-based databases, such as Client Track, Social Solutions, or Apricot; cloud-based communication tools, such as Gmail, Basecamp, or Google Chat; or cloud-based office products, such as Google Docs or Microsoft 365.

**Benefits:**

***Cost**:* In most cases, cloud-based services are less expensive than purchasing an in-house server, database, and software. Depending on the type of cloud-based service, advocacy agencies may be able to use it for free, pay a reduced non-profit rate, or pay only for what they need. This low-cost is attractive to agencies with limited budgets.

***Maintenance**:* With cloud-based services, the company is responsible for maintaining and updating the equipment and service.

***Security***: In general, cloud-based companies will have basic security in place to protect the data they are storing. The level of security will differ depending on the type of service; some services may have stronger security than others. Even major cloud-based companies have experienced breaches and hacks, however.

***Adaptability & Flexibility***: Depending on the service, an advocacy agency may be able to increase or decrease storage size, number of users, or add or remove features based on changing needs.

**Drawbacks:**

***Access by the Cloud-based Company**:* Cloud-based companies store data created by the agency and most can also access that information. This can be extremely problematic, particularly when the data contains survivors' personally identifying information (PII). Advocacy agencies must look at the degree to which the cloud-based service is secure, how the company might purposely or

inadvertently share data, and how much control the agency has over access to and retention of its own data.

Many cloud-bases companies don't actually own the servers where the data is being stored, but rather contract with yet another company for the data storage and that company may have different policies and practices around security and access. These companies may state that their employees are *not allowed* to access customer data, but that doesn't mean that they *can't* access it. While this access could be necessary as part of their business practices or for maintenance purposes, the ability of a third-party such as the cloud-based company or its employees to access any PII about survivors would be a violation of federal confidentiality laws.

As an added protection, some cloud-based companies, such as EmpowerDB, offer what is called "Zero Knowledge Encryption," which means that the company has zero knowledge of or access to the agency's data. With zero knowledge systems, the agency retains complete control over the data by maintaining the encryption key to its own data.

Even if they can't access the sensitive data itself, cloud-based companies may collect information such as usage, user accounts, and IP addresses and share this information with affiliates and other third parties, such as advertisers. Advocacy agencies that are considering using cloud-based services need to be aware of all the ways in which cloud-based companies may access and share their data.

***Agency Access:*** In addition, the advocacy agency must still manage access in-house by staff, volunteers and any IT consultants. The ability to access data from anywhere is one of the often-touted features of cloud-based services. This is also one of its major drawbacks when prioritizing the confidentiality and security of survivor and agency information. The more access points to the data, the more vulnerable that data is, and the more opportunities exist for that data to be disclosed. Agencies will need to develop policies and best practices on the security of agency devices and networks (including wi-fi) and staff access to cloud-based services from personal devices (which is not recommended).

Another drawback with cloud-based products is that they rely on the internet to access the data or service. If there is power or technological failure – on the agency side or the company side – the agency might not be able to access their information. In an emergency situation, this lack of access may pose a risk to safety.

***Data Disclosures***: Most cloud-based services that have the ability to see the data being stored with them will disclose their clients' data under certain circumstances, such as when responding to a

subpoena or search warrant. Agencies should review the company's terms of use, privacy policies, and security policies to learn exactly when the company will disclose their data and under what circumstances. If the company would not fight a subpoena to the same extent that an agency would, that is a significant concern.

Even in the absence of a subpoena or other external request for data, the mere fact that a company can see the data in the first place may violate federal confidentiality obligations.

Agencies should also be aware of what happens to their data if the company closes or changes ownership. Will the agency be informed and given the opportunity to remove their data? Agencies should clarify the process of how they would get their data back, and how long they would have to remove their data.

***Security:*** Although most cloud-based services will have security measures in place, no company is immune to security failures or data breaches. Agencies should know how and when they will be informed if any of their data has been breached and what steps the company will take to address the breach.

Additionally, many cloud-based services may say that their service is "encrypted," but this can mean different things. Usually cloud-based products only encrypt the communications sent between the user and the cloud service (encryption in transit). But the system may not also encrypt the data while on the company's servers (encryption at rest), leaving it vulnerable. It's also important to note that data encrypted at rest can still be fully visible to employees at the company if the company retains control of the key used to encrypt the data.

No form of encryption can protect an agency if one of their own computers becomes infected by a virus or is otherwise controlled by an outside party. Agencies will still have to ensure that their devices are secure.

***Retention and Destruction Policies:*** One of the benefits of cloud-based services is that they automatically back up their client's data to ensure against loss. However, this also means that an agency's data could be in multiple places and accessible even after the agency has "deleted" it. Agencies should ask how the company handles retention and destruction of data.

***Limitations to Customization:*** Many cloud services sell a specific product, and agencies don't have the ability to customize the product to fit their needs. Even if customization is available, it's often

limited. If agencies are looking for very specific features or have unique needs, cloud-based services may not meet those needs.

**In-House Equipment & Software**

In-house equipment and software can include a dedicated server, agency email software such as Microsoft Outlook, and office software products such as Microsoft Office.

**Benefits:**

***Control:*** For the most part, if the agency owns the equipment and the software, they have full control over the data, from determining who gets access to when the data gets deleted.

***Flexibility:*** Agencies may be able to make changes without having to wait on an external company, to the extent that technology is maintained by well-trained, on-site staff. Agencies may also have more flexibility over customizing certain features.

***Confidentiality & Privacy****:* Since both equipment and software are in-house, the agency can determine who has access, when information can be disclosed, and how to adjust security and privacy policies based on what they are doing.

**Drawbacks**

***Cost:*** Purchasing and maintaining equipment and software may be much more expensive than using cloud-based services. Agencies should take into account the "total cost of ownership" including upgrades to equipment and software, on-going training for front-line and administrative staff, as well as IT staffing and security (see below).

***Staffing:*** Agencies will need to hire IT staff or an external IT consultant to maintain and update equipment and software including servers, networks, databases and back-up devices. If an outside vendor, consultant or volunteer maintains these systems, policies and procedures should be in place to protect sensitive data, clearly communicate expectations and spell out consequences for data breach.

***Security:*** Agencies still need to ensure that they have policies and infrastructure in place to secure sensitive data. Policies should include access levels, user passwords, and retention and destruction guidelines. Infrastructure includes servers, networks, back-up devices, and software updates to maintain databases and protection against breaches and malware.

# In-House Products
# vs.
# Cloud-Based Services

**Concluding Recommendations – What Type of Data Is Being Stored?**

The first and foremost factor when considering whether to use a cloud-based service is the extent that the privacy and security of sensitive data can be maintained. This is particularly important for domestic violence and sexual assault agencies that have to meet federal confidentiality obligations. The following are options for maintaining the highest level of control and confidentiality over agency data.

**Option A:** Choose a cloud-based provider that can effectively minimize the inadvertent disclosure of sensitive, identifying and/or confidential information, either internally or externally.

**Option B:** Keep equipment and software in-house, and have policies and infrastructure in place to minimize inadvertent disclosure of sensitive, identifying and/or confidential information.

**Option C:** Use cloud-based services for non-survivor data and using in-house systems for sensitive, identifying and/or confidential information.

This project was supported by Grant No. 2013-TA-AX-K006 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/ exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.