Many domestic violence and sexual assault agencies are struggling with deciding whether they should purchase or keep their own equipment and software or move to cloud-based services and products (or do a combination of each). There are significant considerations that agencies must take into account when making their decisions, which most importantly include survivor privacy and safety and the agency’s confidentiality obligation.

**Cloud-Based Services & Products**

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 may be less expensive than purchasing an in-house server, database, and software. Depending on the type of cloud service, agencies can use it for free, pay a reduced non-profit rate, or pay only for what they need. This flexibility may be helpful for agencies with limited budgets.

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

**Security:** In general, cloud-based companies will have basic security in place over 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 agency may be able to increase or decrease storage size, number of users, or add or remove features based on the agency’s needs.
**Drawbacks**

All cloud-based products will store some type of data created by the agency and most can also access that information. This can be extremely problematic, particularly when an agency wants to store sensitive data, such as survivor information. Agencies must look at whether the service is secure, how it could purposely or inadvertently share data, and how much control the agency actually has over its own data.

**Access:** Because the agency’s data is being stored on a third-party server, the company could have access to the data. Many providers may state that their employees are not *allowed* to access customer data, but that doesn’t mean that they *can’t* access it. This access could be necessary as part of their business practices or for maintenance purposes. Regardless, the ability for a cloud-based company to access any personally identifying information about survivors would be a violation of federal confidentiality laws.

Some cloud-based providers, such as EmpowerDB, offer what is called “Zero Knowledge Encryption,” which means that the provider 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.

Even if they can’t access the data itself, companies may collect some type of information, such as monitoring usage, user accounts, and IP addresses and share this information with affiliates and other third parties, such as advertisers. Agencies that are contemplating using third-party cloud services need to ask and know all the different ways cloud services may access their data.

Access also needs to be managed on your agency end. One of the features of cloud services is the ability to access the data from anywhere, as long as the user has internet access. This is also one of its major drawbacks. The more access there is to the data, the more vulnerable that data can become, and the more opportunities exists for that data to be disclosed. Agencies will need to develop policies and best practices on device security, WiFi access security, and whether staff can access these cloud-based services from personal devices (which is not recommended).
Another drawback with cloud-based products is that it relies 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.

**Data Disclosures:** Most cloud services 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 disclose information with a subpoena that the agency is prohibited from sharing without a court order, that is a significant concern. As stated above, if the company can see the data in order to share it in the first place, this would already be a concern since it would violate federal confidentiality obligations.

Agencies should also be aware of what happens to their data if the company closes or is merged with or bought out by another company. Will the agency be informed and given the opportunity to remove their data? Agencies should clarify the process, how they would get their data back, and how long they have to remove their data.

**Security:** Although most cloud services will have some kind of security, they are not immune to security failures or data breaches. Agencies should know if they will be informed if any of their data has been breached and what steps the company is taking to address the breach.

Additionally, many cloud-based services may say that their service is “encrypted,” but this can mean different things. Most of the time, encryption only means during the communication process: when the client logs into the account and accesses the cloud service. The encryption may not include encrypting the data while on the company’s servers (while at rest), and it certainly doesn’t include encryption on the agency side. Agencies will still have to ensure that their devices and internet access are secure.

**Retention and Destruction Policies:** One of the benefits of cloud services is that they will 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 using software such as Microsoft Outlook, or 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 can quickly make changes without having to wait on an external company. Agencies might also have more flexibility over customizing certain features.

**Confidentiality & Privacy:** Since everything is 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**

**Staffing:** Because everything is in house, agencies will need to hire IT staff or an IT consultant to maintain and update equipment and software.

**Cost:** Purchasing and maintaining equipment and software may be much more expensive than using cloud-based services.
**Security:** Agencies still need to ensure that they have policies in place to address security, including security software and policies on access levels, user passwords, and retention and destruction guidelines.

**Decision Factor – What Type of Data Is Being Stored?**
Although there are many factors to consider, such as cost, ease of use, security and privacy options, long-term management needs, and whether it has the adaptability and features the agency needs, agencies need to first and foremost consider whether the cloud service gives the agency the ability to maintain privacy and security over the data. This is particularly important for domestic violence and sexual assault programs that have to meet federal confidentiality obligations.

A cloud-based service may not be the best option if agencies are going to use create, store, or communicate personal information about survivors of domestic violence, sexual assault, or stalking. Even if the cloud service doesn’t share any information, if there is a chance that they could see the data (during regular maintenance, for example), which could violate the agency’s federal confidentiality obligations if they knowingly use a system that allows other individuals access to survivor data. Using cloud services for non-survivor data and using in-house systems for sensitive, identifying data may be the best combination.

© 2016 National Network to End Domestic Violence, Safety Net Project. Supported by US DOJ-OVW Grant# 2013-TA-AX-K006. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.