NNEDV

Vendor Negotiation & Contract Checklist for a Secure & Survivor-Centered Database

Law and best practice require that victim service programs choose a database that protects the privacy and safety of victims and their information. Many vendors design and market their products with “convenient” or “easy to use” options for customers who may work with clients who have lower safety and privacy risks, and so they may emphasize these features over those that are necessary to maintain confidentiality and reflect a survivor-centered approach.

The following is a check-list of features and options to help guide your negotiations with database vendors so you can choose the product that best supports survivor safety and privacy. For every question, a vendor should be able to give you a clear, understandable answer or agree to follow-up with an answer.

This checklist is not meant as a stand-alone document. Please see the sections of the companion document, Client Information Databases and Confidentiality, that matches the headings below for important background information.

Client Files: Content & Retention

Content. To adhere to the best practice of only collecting the most minimal amount of identifying information necessary to provide services:

- Any data field can be hidden or removed from the data entry view.
- The language or wording of any data field can be changed.
- Each question can be changed to be required or optional.
- The order of the questions can be changed.
- If these changes must be made by the vendor, what is the cost?

Retention. To adhere to the best practice of keeping data only as long as absolutely necessary for services or according to applicable laws or regulations:

- The data can be purged (deleted and permanently removed) according to a routine schedule set by the program.
- The data to be purged can be part of a record or the entire record. For example, the narrative field could be purged while the rest remains.
- Any record can be manually deleted by a user with appropriate access level at any time.
- The vendor can describe how purged information would not remain as part of a back-up.

Selecting a Database Vendor

Ownership. The vendor must ensure that the program retains control, oversight, and ownership of survivor data.

- The program owns the data in the database.
- There is a clear procedure for the program to export all data out of the database at any time.
- The vendor should clearly explain what will happen if they change ownership or go out of business.

Access. Access to personally identifying survivor data in the database must able to be limited to appropriate people inside the victim services program.

- Each user can be assigned an individual password-protected account (versus one account and password that is shared by many).
- Access can be quickly and easily removed, for example if an employee or volunteer leaves the program.

- Security options are in place so that the database can be opened only on computers in the program’s network, or
- If the database can be opened on the web, there are options that allow for or ensure that:
    - The program can limit access to certain devices, for example, program-owned devices/computers.
    - The program has the ability to remotely wipe the device of all information.
- The database vendor and all sub-contractors commit to notifying and give the program an opportunity to resist subpoenas, warrants, and any other third party requests for survivor data.
- The vendor makes agreements in line with the programs’ confidentiality obligations, including, if necessary to be responsible for reasonable damages if the vendor’s staff or subcontractors misuse or mishandle survivor data.

Security. The vendor must take strong precautions against an accidental or malicious breach of the security of the database.

- Data is encrypted in transit and at rest.
- The program, not the vendor, holds the encryption key(s).
- The vendor states where the data is physically kept, including any back-ups.
- The vendor performs regular internal security audits.
- The vendor can clearly explain what happens when security flaws are discovered, including how flaws would be addressed and when the program would be notified.

- The vendor can clearly explain what would happen if there is a data breach, what records would exist documenting the breach, and how quickly the program would be notified.
- The vendor makes reasonable agreements to be responsible for damages if the vendor's staff or subcontractors misuse or mishandle survivor data.
- The program has the right to enforce the contract in a court close to the victim service program (as opposed to a contractual agreement to only bring a lawsuit where the database vendor is located).

Supported by US DOJ-OVW Grant # 2019-TA-AX-K003. 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.