

NNEDV

Databases



How the Technology Works

Databases are computer programs used to organize information in a way that makes information easy to locate, access, and update. Databases can be organized in a variety of ways (alphabetically, numerically) and can include text, words, and images. Databases can be searched using a “query” like a name, place, date, etc. To find information about groups of people, databases have a “report” function that allows the user to run a report on the number of new clients in the last month or the most popular resource accessed, etc.

Databases generally allow administrators to set usernames, passwords, access levels, and permissions. Additionally, well-designed databases incorporate audit trails to provide a detailed record of the queries and actions of each user. Databases can be designed at the outset to automatically purge certain data elements after a certain time period and only retain the elements necessary for reporting purposes.

Access levels: Access levels enable a few staff to see all the information in a database, and other users to only see the appropriate information relevant to the role of the user (volunteer, staff, attorney, etc). Before the database is put into place, it is important to determine who needs to have access to the data, what level of access is appropriate, and how access to the data will be limited to these authorized persons.

Data storage: Some databases are hosted locally while others are hosted off-site. A locally hosted database means that the data remains in the agency, on the agency’s server. A remotely hosted database is often a commercial package, whereby the agency pays a monthly fee and the database is hosted by a third-party, outside the agency.

Pre-packaged, commercial databases are often less expensive up front, but may not be adaptable or may require additional costs to modify the database or create a new type of report, etc. If agencies choose to contract with someone to have a database developed especially for the agency, a limited number of modifications can be written into the initial contract. The costs to develop, implement, and maintain a database can range widely from \$5,000 to over \$50,000.

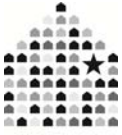
How Are Agencies and Partnerships Using It?

Some agencies use client or patient databases as the primary means of information storage, while others use them more as “card catalogs” to reference paper files. In the latter method, the data is entered with a non-identifying client code instead of a name. Paper files are labeled with the same code and this helps staff know which filing cabinet to go to in order to find the paper file.

Other agencies create resource databases to share training materials and articles. Sometimes, these are full-text, meaning they include the entire article. Other times, they include just a summary of the article. Regardless, resource databases make it easy to locate information on a specific subtopic, and usually offer a search function, allowing the user to search by topic, author, title, etc.

Benefits and Risks

- Databases allow agencies to easily analyze relationships between data and run reports on service usage
- Resource databases eliminate the need to recreate materials or resources and generally offer keyword searches to provide quick results.
- Any data kept on a computer that has Internet access is vulnerable to interception or breaches.



NNEDV

Databases



- Remember that any information entered into a database could exist for perpetuity. Even if the database owner promises to delete it after a certain number of days, data can be backed up, removed, exported, etc. So, it's important to carefully consider what is collected and what the future implications may be.
- Although it's highly unethical, there is always a risk that data collected for one purpose will be used for secondary purposes (such as client intake information being used by researchers for research studies). Additionally, there is a risk that current or former employees will purposely or accidentally share confidential information or take advantage of their access to the database to perform searches for personal use.
- Untrained users may accidentally delete or alter data.

Things To Consider

Necessity: What problem is the agency trying to solve? Is a database really the answer? For example, a community experiencing difficulties with protection orders being served may want to create a database thinking that will make the process more efficient. Creating a database doesn't address the problem of orders not being served because the problem is not having enough officers to serve the orders.

Functionality: Is it user-friendly? Has the agency allocated sufficient money, resources, and staffing to keep the database up to date and make it useful? Has the agency allocated sufficient resources for training existing and new staff (turnover) and providing ongoing technical support?

Privacy & Safety: What confidentiality and privilege laws/regulations/obligations apply? Who will have ultimate responsibility for ensuring that confidential data is protected? Is there a designated privacy officer within the organization? Do users sign documents acknowledging their responsibilities for protecting the confidentiality of data, such as a data confidentiality agreement or an employment agreement with data confidentiality provisions?

Client Information: What factors will agencies use in establishing collection, modification, use, and disclosure procedures for client-identifiable data? Are clients informed about the security and data sharing policy? What is the process for clients to opt-out, inspect, withdraw, or correct their data/records? How will agencies inform clients about this process?

Cost: Has the agency priced multiple options and received at least 2 bids for the project? Has the agency done a cost-benefit analysis to assess the balance between ongoing costs and ultimate benefits? Has the agency designated appropriate funds for the project? While modest expenses for outcomes measurements are part of any grant, a direct services grant should primarily fund services and not outcomes measurement.

Security: Best practice is to secure backups at the same level of security as the original source. Has the agency included plans for system backup and security? Consider contracting with a computer security professional to assess the penetrability/security of the system and to recommend improvements.



Specialized System Databases



How the Technology Works

Systems databases are unique in that they build upon the basic database architecture, but in order to be effective, require collaboration from multiple partners in the community. Examples include Criminal Justice Information Systems (CJIS), offender management systems, and victim notification systems. (See *the Databases factsheet for more information about the basic operation of databases.*)

How Are Agencies and Partnerships Using It?

“CJIS” is a category of criminal justice system databases that link with the FBI’s National Crime Information Center (NCIC). Typically, a CJIS is a state-level database under the oversight of the state’s Department of Justice. CJIS allows both export of data to NCIC and searching of NCIC. A state CJIS generally contains more information than NCIC and allows more specific searches and queries. Some CJIS automatically send regular updates to NCIC while others require NCIC to “pull” updates.

Offender management systems are used by specialized courts to keep track of incarcerated offenders and to monitor offender compliance with release/probation conditions. These systems may include a jail management system, a court case management system, an active and inactive arrest warrant list, a sex offender registry, a database of state statutes, and more. Offender management systems are generally accessible by relevant community agencies like probation, prosecution, etc. In some cases, a nonprofit agency providing drug and alcohol counseling, abuser intervention, or more may access and update the data.

Victim notification systems (VNS) are systems designed to notify crime victims about the release of the perpetrator. Typically, victims register for this service with their phone number and/or email address. The victim is automatically contacted every time a change in the offender’s custody status occurs. Some VNS also provide information on upcoming court hearings, scheduled court events, and their outcomes. The VNS will continue to try to contact the victim until the victim enters her/his personally selected 4 digit code to verify that she/he has received the message.

Benefits and Risks

CJIS: Systems that regularly push updates to NCIC ensure that NCIC is updated more regularly than systems that require NCIC to pull updates. Additionally, some CJIS are setup to actually query the source databases that feed into NCIC, thus ensuring that the most recent versions are queried.

If the CJIS contains an offender registry component, it is important to assess what information is being included in publicly searchable database, since the agency does not want to include information that would identify the victims. (For example, instead of saying that a sexual offender was charged with child molestation of twin six-year-old girls, it is less identifying to saying that the offender was charged with second degree sexual offense against minor children.) In some communities, detailed information may be too identifiable, and the victims’ identities may be revealed.

Offender Management: Since the purpose of this database is offender accountability, it is important to ensure that it is not used to share victim information.

Victim Notification Systems: If the database is not regularly updated, this can create a false sense of security for the victim. With victim notification systems, data must be input almost immediately to avoid the victim believing the offender is still in custody when he was actually released a day or two earlier.



Specialized System Databases



Things To Consider

- Specialized databases require all partners to regularly input and update data so that the database can be relied on as the most up-to-date source of information. Is the community prepared (have adequate resources, staffing, and training) to ensure that the database is updated regularly and audited for accuracy?
- How many different users will have access to the database and what security measures will be implemented to protect the database from unauthorized access, viruses, etc.?