Confidentiality INSTITUTE

NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Databases: The Intersection of Law & Best Practice

FVPSA State Administrators Webinar Series

Presenters:

Alicia Aiken, JD– Director, Confidentiality Institute
Corbin Streett, MSW – Technology Safety Specialist

Confidentiality Institute

- Empower people to protect privacy for violence survivors.
- Support non-profits and government agencies to implement services consistent confidentiality best practices.
- Assist everyone to understand the web of confidentiality, privilege and mandated disclosure laws.

Alicia L. Aiken, JD

- Since 2011, Director of Confidentiality Institute
- Principal at Danu Center for Strategic Advocacy
- Attorney with 15 years experience representing survivors of violence & people living in poverty

alicia@confidentialityinstitute.org

Confidentiality INSTITUTE

NNEDV

Safety Net Project

- Addresses **intersection** between technology and abuse.
- Provides **technical assistance and training** to advocates, law enforcement, legal services, social services providers, and survivors.
- **Advocates** with policymakers and technology companies.

SAFETY NET

Objective

- Take a deep dive into the practical realities of implementing a database that is consistent with the law on confidentiality for FVPSA grantees.
- Answer your questions about how best to support programs to implement best practices

Laying the Foundation

- We are talking about how to support local programs you are monitoring in selecting and maintaining a database
- The legal requirements and best practices related to a local program’s selection and use of a database are quite different than those related to databases used by state administrators

Different Systems, Different Purposes

Local Programs:

- Collect personally identifying information from survivors in order to help them on their path to safety

State & Territorial Administrators:

- Collect aggregate information from programs about the number of victims served

Federal Grant Requirements

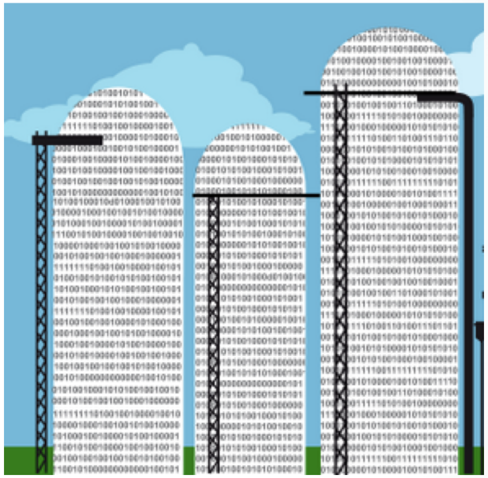
- FVPSA, VAWA, VOCA Grantees

- Shall NOT disclose, reveal or release any:
  - Personally identifying information (PII)
  - Collected in connection with program services that were requested, utilized, or denied

Keep the Data Separate

Identifiable Agency Data should be siloed.

- Each program should have their own database.
- No program should be able to access information collected by other programs.



- State/territorial administrators should not have access to the local program’s database.

A Database is Like a Cookie Jar

Who is allowed in the Cookie Jar?

FVPSA prohibits disclosure of PII to those outside the victim services unit

- Except when survivor requests it
- Or when court/ statute requires it

Inside/Outside the Circle

Inside the Circle

Survivor chooses
to share information
with staff of
victim services program

Outside the Circle

- Law Enforcement
- Child Welfare
- Other V.S.P's
- Non Victim Service Programs
- Funders
- Auditors
- Allies
- Vendors

Helping Local Programs Understand & Choose Databases

Assumptions that Vendors Make

1. Losing access to data is agency's biggest concern
2. If it's affordable to save data forever, it should be saved forever
3. Ease of sharing access to data is agency's primary goal
4. Vendors can be trusted to see everything
5. Potential misuse of data is a small & acceptable business risk

Grantee Values & Needs

1. Misuse of survivor data can result in permanent, serious harm
2. Best Practice: keep only the data needed to help the survivor
3. Best Practice: share internally only as needed to help the survivor
4. Data is and should be routinely destroyed on a set schedule

Routine data destruction is a healthy part of information management!

Heightened Risks for Survivors

1. Most abusers/stalkers and their allies would pass a background check
2. A data breach can’t be fixed by mere credit monitoring
3. Contacting a survivor to notify of a breach might increase danger
4. Even a small risk of misuse of data is not an acceptable business risk

Exposed on the Web!

211 LA County stored data on Amazon web:

- Mistakenly available for public download
- Cybersecurity firm found records of:
  - 33,000 Social Security numbers
  - Full names & addresses
  - 200,000 call logs with detailed notes
    - Describing elder abuse & mental health crises

May 2018 LA Times: https://www.latimes.com/local/lanow/la-me-ln-211-data-20180515-story.html

What Do Grantees Need?

- Detailed information management plan, including destruction policy
- Funds to hire qualified internal systems administrator/tech person
- Legal counsel when negotiating database contracts
- Awareness of the collateral costs of using this information management system

Ease of Access & Sharing…

- Creates training, supervision, and monitoring costs

- Web-access means
  - Controlling which devices have access
  - Encrypting devices that will be lost/stolen
  - Training staff not to use access carelessly
  - Controlling who has access to how much
  - Shutting off access promptly

Data Breach Notification…

- VAWA now requires grantees to have a data breach notification policy
- All states have data breach notification laws
- Existing law focusses on notifying people so can protect against identity theft
- Contacting survivors to notify them can be *dangerous to them*

WEBINAR & TA ARE COMING!

But…Everybody's Doing the Database Dance

“We’re HIPAA-Compliant”

Data Sharing: HIPAA vs. FVPSA

HIPAA

- Healthcare providers can choose to share Personal Health Information (PHI) as part of doing business
- Providers and their business associates are monitored by HHS Office of Civil Rights
- Business Associates can be fined if don’t protect PHI

FVPSA / VAWA

- Grantees can’t decide to share PII as part of doing business; only survivors can
- No OCR involvement in monitoring grantees or vendors
- No power to oversee, monitor or fine vendors

Databases & Their Sales Teams

What Can Vendors Do for Privacy? IDEAL STRATEGY

- Make it so vendor can’t READ the data
- “Zero Knowledge” or “No Knowledge” Encryption
  - Data is locked up, you have a key, vendor doesn’t
- Vendor can’t expose information if they can’t read it
- Thieves can’t read it either

What Can Vendors Do for Privacy? BACK-UP PLAN

- 1 – 2 named staff at vendor have access
- Named staff receives DV/SV privacy training
- DV/SV agency can veto named staff
- Vendor pays liquidated damages if breach
- Vendor will notify & forward subpoenas/orders
- **BUT - breaches can still happen!**
  - Thieves can still read what they steal

Conversations with Programs: Vendor Access & Program Control

- Can the vendor access the program’s information?
- Can programs get their data back at any time?
- Can the vendor move, release, or share the program’s data without its permission?
- What will the vendor do with a request from government, law enforcement, lawyers?
- Will they provide notice to the program if they release the program’s information to someone else?
- What is in their privacy policy?

Conversations with Programs: Data Ownership vs. Possession

- Where is the data, including back-ups?
- Will they purge information according to the program's data retention schedule?
- What happens to the data when the service agreement ends?
- What happens to the data if the company changes ownership or goes out of business?

Conversations with Programs: Security & Encryption

- Is data encrypted in transit? At rest?
- Is data zero knowledge / no knowledge?
- Who has the key?
- Does the vendor provide notice of requests for information, hacks, or breaches?
- Does the company perform security audits?

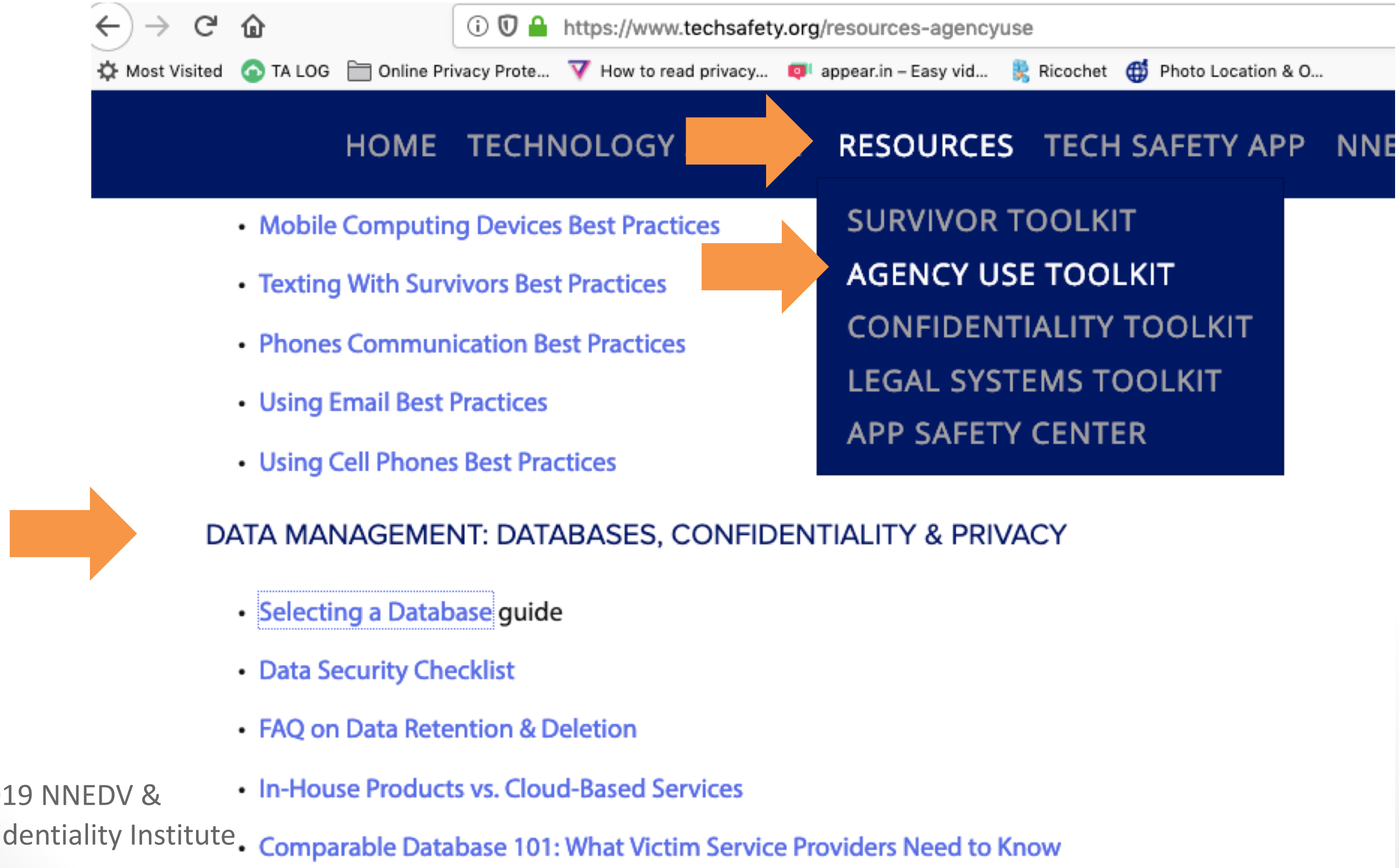
Poll Question

Given the information presented in this webinar, how confident do you feel now about talking to programs about databases?

- Very Confident
- Confident
- Somewhat Confident
- Not Very Confident
- Data*what*? 🤔

Resources? We've Got You Covered!

Check out our database TA materials at techsafety.org



- Mobile Computing Devices Best Practices
- Texting With Survivors Best Practices
- Phones Communication Best Practices
- Using Email Best Practices
- Using Cell Phones Best Practices

DATA MANAGEMENT: DATABASES, CONFIDENTIALITY & PRIVACY

- Selecting a Database guide
- Data Security Checklist
- FAQ on Data Retention & Deletion
- In-House Products vs. Cloud-Based Services
- Comparable Database 101: What Victim Service Providers Need to Know

Digital Services Webinar Series

Assessing Readiness, May 7

Choosing a Platform & Vendor, May 23

Best Practices, May 30

All webinars will be held from

3:00-4:30 PM ET

QUESTIONS?

Contact Information

Alicia Aiken
alicia@confidentialityinstitute.org

Corbin Streett
cstreett@nnedv.org

Safety Net Project
safetynet@nnedv.org

This webinar was made possible by Cooperative Agreement, Award Number 90EV0429-02-00, from the Administration on Children, Youth, and Families, Family and Youth Services Bureau, U.S. Department of Health and Human Services. Its contents are solely the responsibility of the author(s) and do not necessarily represent the official views of the U.S. Department of Health and Human Services.

Database Resources
https://www.techsafety.org/resources-agencyuse