

IN THE CIRCUIT COURT OF THE STATE OF OREGON  
FOR MULTNOMAH COUNTY

FILED  
22 NOV 10 AM 12:18  
JUDICIAL DIST.

In The Matter of Establishing	)	Presiding Judge Order
James Bell Associates Access	)	No. 2201-00008
to Juvenile Court Records under	)	
ORS 419A.255(15)	)	ORDER ALLOWING JAMES BELL
	)	ASSOCIATES ACCESS TO
	)	JUVENILE COURT RECORDS FOR THE
	)	PURPOSE OF A RESEARCH STUDY

ORS 419A.255(15) authorizes the Presiding Judge of a Court to permit access to confidential juvenile records for research purposes. Chief Justice Order No. 22-030, signed November 3, 2022, establishes standards and guidelines for the release of juvenile records. This Presiding Judge Order grants James Bell Associates access to Multnomah County juvenile court records for research on what factors influence judges' reasonable efforts finding and how reasonable efforts findings relate to case outcomes.

I HEREBY FIND the following:

1. ORS 419A.255(15) permits the release of juvenile records for research purposes. Chief Justice Order (CJO) 22-030 establishes standards and guidelines for the release of records pursuant to ORS 419A.255(15).
2. The CJO Standards and Guidelines require a review of the research plan, information about the researchers, a written confidentiality plan, and a copy of the Institutional Review Board (IRB) approval. Additionally, the CJO requires the research study to meet certain criteria, including the anticipated results and benefits of the proposed research.
3. Oregon Judicial Department entered a detailed Data Use and Security Agreement on November 8, 2022 with James Bell Associates. James Bell Associates are conducting the Reasonable Efforts Findings Study (REFS). REFS is a national research study to understand what factors influence judges' reasonable efforts findings and how reasonable efforts findings relate to case outcomes.
4. The Data Use and Security Agreement includes sufficient protections regarding access, use, maintenance, disclosure, and destruction of juvenile court records.
5. The "REFS information Sheet" details the project's purpose and is attached to the Data Use and Security Agreement as Exhibit A. The primary researcher is Alicia Summers, Ph.D.
6. On November 7, 2022, study number 1322534, "Understanding Judicial Decision-Making and Hearing Quality in Child Welfare," received IRB approval. The approval is attached to the Data

Use and Security Agreement as Exhibit B.

7. The anticipated results and benefits of the study is a better understanding of best practices in child welfare proceedings.

I HEREBY ORDER, pursuant to ORS 419A.255(15):

1. Access to Juvenile Court Records

James Bell Associates may have access to the Multnomah County juvenile court records pursuant to the terms in the Data Use and Security Agreement signed on November 8, 2022, for the purpose of conducting a research study on reasonable efforts findings in child welfare hearings.

2. Duration of Access

This PJO will be in effect so long as the data share agreements listed above are in effect. James Bell Associates' access to Multnomah County Juvenile Court records will end if the data share agreement is terminated

This order takes effect 11-9-22



Judith Matarazzo  
Presiding Judge  
Multnomah County

## DATA USE AND SECURITY AGREEMENT

This Data Use and Security Agreement (“**Agreement**”) effective as of <sup>November 7th</sup>, 2022 (“**Effective Data**”), is made by and between Oregon Judicial Department (“**Data Provider**”) and James Bell Associates Inc. (“**Data Recipient**”) pursuant to the U.S. Department of Health & Human Services (“HHS”) Office of Planning, Research, and Evaluation (“OPRE”) and the HHS Administration for Children and Families (“ACF”) Children’s Bureau (“CB”) (“**Client**”) *Reasonable Efforts Findings Study (“REFS”)* as more particularly set forth on **Attachment A (“Project”)**. Data Provider and the Data Recipient are collectively referred to as the “**Parties**” or individually as a “**Party.**”

As part of the Project, Data Recipient will receive access to recorded child welfare hearings, court case files, and administrative data that will be reviewed for the Project using structured observation instruments. Specifically, Data Recipient will collect indicators of hearing quality (e.g., judicial engagement of parties present at hearings) and judicial decisions (e.g., reasonable efforts to prevent removal) solely for the purpose of understanding (such collected and provided information collectively, “**Data**”) factors influencing judicial decision-making and hearing quality during the life of a child welfare case, which must solely to be used for the Project (collectively, “**Purpose**”).

This Agreement sets forth the terms and conditions under which the Data Provider will disclose the Data to the Data Recipient and the terms in which the Data Recipient may use the Data for the Project.

Data Recipient shall comply with all federal and state regulations and laws, as well as contractual obligations set forth in this Agreement and shall be solely responsible and accountable for information confidentiality, integrity, and security of the Data. Additionally, Data Recipient shall ensure that its employees and agents, individual consultants, and vendors used by Data Recipient and their Subcontractors (defined in Section 3 below) shall be solely responsible and accountable for information confidentiality, integrity, and security of the Data.

The Data Recipient shall protect the Data in accordance with the requirements of this Agreement and all applicable laws and regulations, which may include, but are not limited to, the following and which are listed in a descending order of precedence below:

- This Agreement
- The Privacy Act of 1974, 5 U.S.C. 552a.
- The Federal Information Security Management Act of 2014.
- Federal Trade Secrets Act (18 USC 1905).
- The following State laws and rules: ORS 419A.252 through 419A.258 and ORS 646A.600 through 646A - 628.

Data Recipient shall protect and secure the Data and ensure that any of Data Recipient’s Authorized Users of the Data create, receive, maintain, or transmit Data with the same restrictions, conditions, and requirements that apply to the Data Recipient under this Agreement and in accordance with Data Recipient’s data security plan (**Attachment E**) and in accordance with the WIRB Copernicus Group, Inc (“WCG”) Institutional Review Board (“IRB”) attached as **Attachment B**.

Specific requirements:

**1) Data to be Accessed:**

- a) Data Provider will provide Data Recipient and Authorized Users with “read only” access to read, listen to, and view the Data while Data Recipient is on-site at Data Provider’s location. Data Recipient will have access to:
  - Audio or video recordings of court hearings
  - Court case files
  - Demographic data from administrative files

Data Recipient will review key portions of the Data into Data Recipient’s systems using structured observation instruments. The instruments will contain a project assigned identifier to represent the state, judge, and case number to link with other project Data collection. At no point will the Data Recipient download any Data from Data Provider. The project plan is provided in Attachment C.

Data Recipient shall not collect personally identifying information (“PII”) about the child, parents or other family member, however, Data Recipient will have access to PII that is included in the above information such as images of faces, names stated during the hearing and other PII that is said or viewed during the hearing or appears in the Data.

- b) Data Provider hereby grants Data Recipient and the Authorized Users, as identified in **Exhibit D**, limited, fully paid up, royalty free, revocable, nontransferable, non-exclusive, license to use the Data only for the Purpose. Data Recipient shall remain responsible and liable to Data Provider for Others’ access to and use of the Data. Data Recipient and the Authorized Users do not obtain any right, title, or interest in any of the Data except as expressly set forth herein.
- c) Data Recipient represents and warrants that the Data will be used Data Recipient solely for the Purposes.
- d) Data Recipient shall not attempt to contact individuals contained in the Data. Additionally, Data Recipient shall not attempt to identify individuals contained in the Data when the Data Recipient is provided with de-identified Data and the scope of work does not require further identification.
- e) Data Recipient may link or merge Data records with Data Recipient own survey data and with other records it has created or obtained related to study participants for the Purposes of this Project.

**2) Data Custodian & Point of Contact & Funding Agency Contact:**

- a) The Parties mutually agree that the following named individual is designated as the “**Custodian**” of the Data on behalf of the Data Recipient. Data Recipient shall be responsible for observing the security and privacy arrangements specified in this Agreement and for training Authorized Users and shall ensure that the Custodian and the Authorized Users will also comply with and observe the security and privacy arrangements specified in this Agreement .

- b) The Parties mutually agree that the following named individual will be designated as the point-of-contact for this Agreement on behalf of Data Provider.

Custodian for Data Recipient		Point of Contact for Data Provider	
<b>Name</b>	Anne Fromknecht	<b>Name</b>	Heidi Strauch
<b>Title</b>	Project Director	<b>Title</b>	
<b>Company/ Organization</b>	James Bell Associates	<b>Company/ Organization</b>	Oregon Judicial Department
<b>Street Address</b>	2000 15th Street, North Suite 1003033	<b>Street Address</b>	
<b>City/ State/ Zip Code</b>	Arlington, VA 22201	<b>City/ State/ Zip Code</b>	Salem, OR 97301
<b>Phone Number</b>	703-247-2631	<b>Phone Number</b>	
<b>E-Mail Address</b>	fromknecht@jbassoc.com	<b>E-Mail Address</b>	Heidi.O.Strauch@ojd.state.or.us

- c) Data Recipient acknowledges that the U.S. Department of Health & Human Services (“HHS”) Office of Planning, Research, and Evaluation (“OPRE”) and the HHS Administration for Children and Families (“ACF”) Children’s Bureau (“CB”) are providing Data Recipient with funding for this Project. The following is the contact information for the funding agencies:

OPRE and ACF CB	
<b>Name</b>	Alysia Blandon
<b>Title</b>	Senior Social Science Research Analyst
<b>Street Address</b>	330 C Street SW
<b>City/ State/ Zip Code</b>	Washington, D.C. 20201
<b>Phone Number</b>	202-205-8366
<b>E-Mail Address</b>	<a href="mailto:Alysia.blandon@acf.hhs.gov">Alysia.blandon@acf.hhs.gov</a>

**3) Authorized Users of the Data:**

- a) Data Recipient agrees that access to the Data provided under this Agreement will be limited to the minimum number of individuals necessary to perform the work within the purpose of the Project. With the exception of Data Recipient’s Subcontractors (where “**Subcontractors**” means: (i) the American Bar Association Center on Children and the Law; (ii) Systems Change Solutions; (iii) Data Savvy Consulting; along with (iii) such other contractors mutually agreed to in writing by the Parties), Data Recipient shall not share or make available the Data to any personnel not listed on the **Attachment D** or to any other third party. Further, the sensitivity of the Data requires Data Recipient to limit access to the Data to the roster of individuals listed on **Attachment D**. If any other

individuals need access to the Data, Data Recipient shall provide Data Provider with an updated roster and obtain Data Provider's written approval of the updated roster (email acceptable) prior to allowing such additional individuals access to the Data.

- b) The Data Recipient shall ensure that any Data Recipient personnel or Subcontractor's personnel, that will have access to the Data agree to the obligations, restrictions and conditions at least as strong as those that apply to the Data Recipient under this Agreement.
- c) Data Recipient shall not provide to the Client any personal identifiable information ("PII") that would allow for identification of the study participant's identity.
- d) Data Provider represents and warrants that: (i) it has obtained all consent, rights, interests and other authorizations needed by Data Provider under this Agreement; and (ii) the Data is free from viruses and other contaminants.

**4) Term of Agreement:**

This Agreement will commence on the Effective Date noted above and will expire on **September 22, 2023**. This Agreement may be terminated by either Party before the expiration of the stated term upon written notice (Email acceptable) of such Party. Any use of the Data beyond such termination or expiration shall require both Parties to execute a new agreement.

**5) Data Destruction:**

- a) Identified Data. At the expiration or termination of this Agreement, the Data Recipient shall destroy any Data that contains identifying information including, without limitation, PII.
- b) De-Identified Data. At the end of this Agreement, the Data Recipient will prepare de-identified data files for submission to a data archive and transfer to the Client. De-identified study data must be maintained on an encrypted cloud drive for 3 years after the project end date (September 22, 2023) and then destroyed.

**6) Data Security:**

- a) Data Recipient shall use appropriate administrative, technical and physical safeguards to protect the Data. Data Recipient shall provide authorizations to access Data on a need to know basis, least privilege and separation of duties. Data recipient maintains and shall continue to maintain an organizational System Security Plan compliant with NIST SP 800-53, Rev. 4 security controls. Data shall be handled in accordance with Data Recipient project-specific security plan for as long as the Data or De-identified Data is in Data Recipient's possession.
- b) Data Recipient shall notify Data Provider in writing promptly but no later than within 24 hours in the event of any unauthorized disclosure of the Data.

**7) Scope of Relationship:**

This Agreement will not constitute a partnership, agency or joint venture, and neither party may bind the other to any contract, arrangement or understanding except as specifically stated herein or otherwise mutually agreed to in writing by the parties.

**8) Publication and Use of Name:**

- a) Data Provider agrees that Data Recipient may publish reports discussing its research and findings arising from this Agreement. In such reports, Data Recipient may disclose and publish aggregated statistics based on the Data. Under no circumstances shall Data Recipient discuss or publish the raw or PII portions of the Data in such reports or publish any information, statistics or analysis that may identify any individual involved in any of the proceedings contained in the Data.
- b) Data Provider agrees that Data Recipient may use Data Provider's name as the source of the Data provided in this Agreement in any future public presentation(s) or report(s).

**9) Limitation of Liability, Insurance and Indemnification:**

- a) EXCEPT FOR BREACHES OF PRIVACY, CONSENT, CONFIDENTIALITY, INTELLECTUAL PROPERTY AND INDEMNITY OBLIGATIONS IN THIS AGREEMENT, NEITHER PARTY SHALL BE LIABLE UNDER ANY PROVISION OF THIS AGREEMENT FOR SPECIAL, INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS, REVENUE, TIME, GOODWILL, COMPUTER TIME, DESTRUCTION, DAMAGE OR LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGE WHICH MAY ARISE FROM THE USE, OPERATION, OR MODIFICATION OF DATA PROVIDED UNDER THIS AGREEMENT).
- b) EXCEPT FOR DATA RECIPIENT'S LIABILITY ARISING OUT OF OR RELATED TO SECTION 9)e) OR AN UNAUTHORIZED DISCLOSURE OF DATA, UNDER NO CIRCUMSTANCE SHALL EITHER PARTY HAVE ANY LIABILITY WHATSOEVER FOR ANY CLAIM ARISING FROM OR RELATING TO THIS AGREEMENT OR ITS PERFORMANCE OR NONPERFORMANCE FOR AN AGGREGATE AMOUNT IN EXCESS OF \$1,000,000.
- c) Data Recipient shall obtain and maintain during and for three (3) years after this Agreement the following insurance covering the other Party as an additional insured: (i) Commercial General Liability or Public Liability Insurance with a limit of \$1,000,000 per occurrence and \$5,000,000 in the aggregate including coverage for bodily injury and property damage; (ii) Workers' Compensation and Employer's Liability insurance where required by local statute; (iii) Cyber Breach, Special Perils or All Risk Property Insurance with limits of \$2,000,000 per claim; and (iv) Professional Liability or Errors & Omissions insurance with limits of \$2,000,000 per claim covering liabilities arising from this Agreement related to intellectual property infringement, trade secret misappropriation, privacy and data security breach.
- d) Data Provider is insured with respect to tort liability by the State of Oregon Insurance Fund, a statutory system of self-insurance established by ORS Chapter 278, and subject to the Oregon Tort Claims Act, ORS 30.260 through 30.300.
- e) Data Recipient shall pay, defend, indemnify and make Data Provider whole from and against any claim or liability arising from Data Recipient's breach of any represents or warrants under this Agreement.
- f) **Defense of Claims.** To the extent Data Recipient is required under this Agreement to defend Data Provider against claims, including under Section 9)e) above, Data Provider shall reasonably cooperate in good faith, at Data Recipient's expense, in the defense of the claim, Data Recipient shall select counsel reasonably acceptable to Data Provider and the Oregon Attorney General to defend the claim, and Data Recipient shall bear all costs of counsel. The Data Provider's and the Oregon Attorney General's acceptance of counsel may not be unreasonably withheld.

Counsel must accept appointment as a Special Assistant Attorney General under ORS Chapter 180 before counsel may act in the name of, or represent the interests of, the State of Oregon, Data Provider, its officers, employees or agents. Data Provider may elect to assume its own defense with an attorney of its own choice and at its own expense any time Data Provider determines important governmental interests are at stake. Subject to these limitations, Data Recipient may defend a claim with counsel of its own choosing, on the condition that no settlement or compromise of any claim may occur without the consent of Data Provider, which consent must not be unreasonably withheld.

- g) Subject to the limitations of Article XI, section 7 of the Oregon Constitution and the Oregon Tort Claims Act ORS 30.260 through 30.300, Data Provider shall pay, indemnify and make Data Recipient whole from and against any claim or liability (including attorney fees and legal cost) arising from Data Provider's breach of any represents or warrants under this Agreement. Data Provider has no obligation to defend Data Recipient.

10) **Governing Law; Jurisdiction; Venue.** This Agreement is governed by, construed, and enforced in accordance with the laws of the State of Oregon, without giving effect to its conflict of law principles, and applicable federal law. Any action or suit brought by the parties relating to this Agreement must be brought and conducted exclusively in the Circuit Court of Marion County for the State of Oregon in Salem, Oregon; provided, however, if a claim must be brought in a federal forum, then it must be brought and conducted solely and exclusively within the United States District Court for the District of Oregon. LICENSOR HEREBY CONSENTS TO THE PERSONAL JURISDICTION OF THESE COURTS, WAIVES ANY OBJECTION TO VENUE IN THESE COURTS, AND WAIVES ANY CLAIM THAT THESE COURTS ARE INCONVENIENT FORUMS. In no way may this section or any other term of this Agreement be construed as (i) a waiver by the State of Oregon of any form of defense or immunity, whether it is sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States, or otherwise, or (ii) consent by the State of Oregon to the jurisdiction of any court.

11) **Attorneys' Fees.** Neither Party to this Agreement is entitled to obtain judgment from the other party for attorneys' fees incurred in any litigation between the Parties. Except as allowable under Section 9 above, neither party may obtain judgment from the other party for attorneys' fees incurred in the defense of any claim asserted by a third party.

**12) Compliance:**

Each Party agrees to comply with applicable regulations and laws, including but not limited to the Privacy Act of 1974 (5 U.S.C. 552a et seq.), , the Sarbanes-Oxley Act and the Gramm-Leach-Bliley Act of 1999. Each Party acknowledges that there are administrative, civil, or criminal penalties for disclosure or misuse of these data.

**13) Data Recipient's Legal Status:**

Data Recipient represents and warrants that Data Recipient is a legally recognized, nonprofit organization, as defined by the Internal Revenue Service, and is registered legal entity within the United States. Data Recipient further warrants that Data Recipient will maintain its



nonprofit status and will remain a legally registered business entity within the United States for the duration of this agreement.

**14) Miscellaneous:**


Attachments A, B, C, D, and E are hereby incorporated into this Agreement by this reference. This Agreement supersedes all agreements between the Parties with respect to the subject matter hereof. The terms of this Agreement can be changed only by written modification to this Agreement or by the Parties adopting a new Agreement.

*The signatories below hereby attest that he or she is authorized to commit to this Agreement on behalf of their respective organization and further agrees to abide by all the terms specified in this Agreement.*

**DATA RECIPIENT: James Bell Associates, Inc.**

<u>Lina Gong</u>	Vice President of Finance and Admin
Name	Title
<u>Lina Gong</u> <small>Digitally signed by Lina Gong Date: 2022.11.07 15:29:06 -05'00'</small>	
Signature	Date

**DATA PROVIDER: Oregon Judicial Department**

<u>Nancy J. Cozine</u>	State Court Administrator
Name	Title
<u></u>	November 8, 2022
Signature	Date

# Reasonable Efforts Findings Study (REFS) Information Sheet

IRB Approved at the  
Study Level

Dec 01, 2021

## What is the REFS?

The REFS is a research study to understand what factors influence judges' **reasonable efforts findings** and how reasonable efforts findings relate to **case outcomes**.

Factors we will examine include:

- Pre- and between hearing communication (e.g., depth of information in reports)
- Hearing quality components (e.g., depth of discussion and parent engagement)
- Case characteristics (e.g., age, race, and gender of child, presenting problems)
- Judicial characteristics (e.g., race and ethnicity of judge, years of experience, case assignment type)
- Timing and frequency of review hearings

The study will include observation of recorded court hearings, review of court case files, and surveys with judges.

### Research Team

This study is funded by the Office of Planning, Research, and Evaluation (OPRE) and the Children's Bureau and conducted by James Bell Associates, the American Bar Association Center on Children and the Law, and Co-Principal Investigators Drs. Alicia Summers and Sophie Gatowski.



# What are the research questions?

1. How are hearing quality components (e.g., discussion during the hearing, how judges engage parents), information provided to the court before the hearing, case characteristics, judicial characteristics, and timing of the initial hearing **related to judges' findings of reasonable efforts to prevent removal?**
2. How are the breadth and depth of information provided to the court, case characteristics, judicial characteristics, and frequency and timing of the review hearings **related to the judges' findings of reasonable efforts to achieve permanency at review hearings?**
3. How are judges' findings of reasonable efforts to prevent removal and the detail documented in findings related to **the likelihood of reunification?**
4. How are judges' findings of reasonable efforts and the detail documented in findings related to **the time for cases to achieve permanency?**
5. Is there evidence of bias in the language used in child welfare court cases?

# Who will participate?

We are inviting up to 4 CIPs and up to 8 judges to participate. The total sample will include 440 cases (55 cases from 8 judges each).

# What is required for your site to participate?

Our goal is to require minimal time and effort from you and your staff. Study sites will be asked to:

1. Identify 2 judges who:
  - Presided over child welfare cases in 2019
  - Work in jurisdictions with an ethnically diverse caseload
  - Mostly follow a one family, one judge model
  - Do not preside over cases in a problem-solving court model (e.g., family treatment drug court, mental health court or a "0-3" young children's court cases)
  - Are willing to complete a brief web survey about their demographics and judicial experience
  - Allow the study team to review 55 cases they closed in 2019 as part of the study sample.

2. Grant remote access to recordings of 55 initial hearings of cases closed in 2019 from each participating judge. For a total of 110 cases from your state.
3. Grant remote access to the associated court case file of the 110 initial hearings reviewed.

## How will your data be protected?

We are committed to protecting all data collected for the study. We will sign a data sharing agreement with each site that explains how data will be shared, stored, accessed, and disposed. Data will be stored and maintained in accordance with Administration for Children and Families and FISMA requirements. Data access will be password protected and restricted to the study team. All team members are trained on data security procedures and human subjects protections. Child welfare cases and judges will be given unique identifiers so that final datasets will not have any personally identifying information. All data will be analyzed and reported in the aggregate, so that no families, judges, or sites are identified.

## What is the timeline?

We want to collect data between March and June 2022. That means we'd like to get access to the data from sites by March 1, 2022.

## How can your state benefit?

This is one of the first research studies to explore reasonable efforts in depth. The information your CIP provides will contribute to a growing body of evidence about what works best in child welfare hearings. Findings from this study will be shared widely and used to inform practice, policy, and court improvement efforts. Additionally, we will give you an Excel file that includes all deidentified data collected from hearing observation and court case file review in your state. This will allow you to conduct your own analyses on the 110 closed cases sampled from your state.

## How can you learn more?

Contact Project Director Anne Fromknecht to learn more:

[Fromknecht@jbassoc.com](mailto:Fromknecht@jbassoc.com) 703-247-2631

<b>Investigator Name:</b> Alicia Summers, PhD, MS Sophia Gatowski, PhD	<b>Board Action Date:</b> 11/07/2022
<b>Investigator Address:</b> 682 Talus Way Reno, NV 89503, United States	<b>Approval Expires:</b> 12/01/2023 <b>Continuing Review Frequency:</b> No CR Required
<b>Sponsor:</b> Office of Planning, Research, and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services <b>Institution Tracking Number:</b>	<b>Sponsor Protocol Number:</b> None <b>Amended Sponsor Protocol Number:</b> None
<b>Study Number:</b> 1322534	<b>IRB Tracking Number:</b> 20216278
<b>Work Order Number:</b> 1-1591729-1	
<b>Protocol Title:</b> Understanding Judicial Decision-Making and Hearing Quality in Child Welfare	

**THE FOLLOWING ITEMS ARE ACCEPTED OR ACKNOWLEDGED:**

Study and Investigator for an additional continuing review period. This approval expires on the date noted above.

**Please note the following information:**

This certificate documents that the IRB will continue oversight for an additional year.

Under the revised common rule (effective 1-21-2019), continuing review by the Board of the above referenced research is not required; however, the IRB will maintain our records and continue responsibility for exercising administrative and regulatory oversight of this research. The IRB will automatically charge an Ongoing Oversight fee for this administrative effort unless we are notified the research is closing. To avoid unnecessary fees due to closure, a closure form must be submitted for each site 30 days prior to expiration.

**THE IRB HAS APPROVED THE FOLLOWING LOCATIONS TO BE USED IN THE RESEARCH:**

James Bell Associates, 2000 15th St., North, Suite 100, Arlington, Virginia 22201

**ALL IRB APPROVED INVESTIGATORS MUST COMPLY WITH THE FOLLOWING:**

As a requirement of IRB approval, the investigators conducting this research will:

- Comply with all requirements and determinations of the IRB.
- Protect the rights, safety, and welfare of subjects involved in the research.
- Personally conduct or supervise the research.
- Conduct the research in accordance with the relevant current protocol approved by the IRB.
- Ensure that there are adequate resources to carry out the research safely.
- Ensure that research staff are qualified to perform procedures and duties assigned to them during the research.
- Submit proposed modifications to the IRB prior to their implementation.
  - Not make modifications to the research without prior IRB review and approval unless necessary to eliminate apparent immediate hazards to subjects.
- For research subject to continuing review, submit continuing review reports when requested by the IRB.
- Submit a closure form to close research (end the IRB's oversight) when:
  - The protocol is permanently closed to enrollment
  - All subjects have completed all protocol related interventions and interactions
  - For research subject to federal oversight other than FDA:
    - No additional identifiable private information about the subjects is being obtained
    - Analysis of private identifiable information is completed

This is to certify that the information contained herein is true and correct as reflected in the records of WCG IRB. WE CERTIFY THAT WCG IRB IS IN FULL COMPLIANCE WITH GOOD CLINICAL PRACTICES AS DEFINED UNDER THE U.S. FOOD AND DRUG ADMINISTRATION (FDA) REGULATIONS, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) REGULATIONS, AND THE INTERNATIONAL CONFERENCE ON HARMONISATION (ICH) GUIDELINES.



## Attachment B to REFS\_Data Use Agreement

- For research subject to continuing review, if research approval expires, stop all research activities and immediately contact the IRB.
- Promptly (within 5 days) report to the IRB the information items listed in the IRB's "Prompt Reporting Requirements" available on the IRB's Web site.
- Not accept or provide payments to professionals in exchange for referrals of potential subjects ("finder's fees.")
- Not accept payments designed to accelerate recruitment that are tied to the rate or timing of enrollment ("bonus payments") without prior IRB approval.
- When required by the IRB ensure that consent, permission, and assent are obtained and documented in accordance with the relevant current protocol as approved by the IRB.
- Promptly notify the IRB of any change to information provided on your initial submission form.

Consistent with AAHRPP's requirements in connection with its accreditation of IRBs, the individual and/or organization shall promptly communicate or provide, the following information relevant to the protection of human subjects to the IRB in a timely manner:

- Upon request of the IRB, a copy of the written plan between sponsor or CRO and site that addresses whether expenses for medical care incurred by human subject research subjects who experience research related injury will be reimbursed, and if so, who is responsible in order to determine consistency with the language in the consent document.
- Any site monitoring report that directly and materially affects subject safety or their willingness to continue participation. Such reports will be provided to the IRB within 5 days.
- Any findings from a closed research when those findings materially affect the safety and medical care of past subjects. Findings will be reported for 2 years after the closure of the research.

For Investigator's Brochures, an approval action indicates that the IRB has the document on file for the research.

If the IRB approved an e-consent process that involves uploading the approved consent form to an e-consent platform, please ensure that the consent form(s) approved for your site is the version of the consent form that gets uploaded to the platform.

If the board approves a change of Principal Investigator - Once approved, the new Principal Investigator is authorized by WCG IRB to carry out the study as previously approved for the prior Principal Investigator (unless the Board provides alternate instructions to the new Principal Investigator). This includes continued use of the previously approved study materials. The IRB considers the approval of the new PI a continuation of the original approval, so the identifying information about the study remains the same.

If your research site is a HIPAA covered entity, the HIPAA Privacy Rule requires you to obtain written authorization from each research subject for any use or disclosure of protected health information for research. If your IRB-approved consent form does not include such HIPAA authorization language, the HIPAA Privacy Rule requires you to have each research subject sign a separate authorization agreement.

If this study includes data monitoring committee/data safety monitoring board, please note that the reports of all meetings of this committee should be submitted to the IRB even if the outcome of the meeting results in no changes to the study.

**For research subject to continuing review, you will receive Continuing Review Report forms from WCG IRB when the expiration date is approaching.**

Thank you for using this WCG IRB to provide oversight for your research project.

### **DISTRIBUTION OF COPIES:**

#### **Contact, Company**

Alysia Blandon, Office of Planning, Research, and Evaluation ACF DHHS

Alicia Summers, PhD, MS, Data Savvy Consulting, LLC

Sophia Gatowski, PhD, Systems Change Solutions Inc.

Anne Fromknecht, James Bell Associates

Sarah Blankenship, Office of Planning, Research, and Evaluation, ACF DHHS

## ATTACHMENT C

### Project Plan

Court data shall only be accessed in-person using state-owned computers. The study team will be given “read-only” log-in access to the study states’ court data systems. This is needed to access the sample of hearing recordings and related court case files. The study team shall not download any data from the system.

Upon log-in, audio or video recordings from a sample of initial court hearings and their associated case files will be reviewed and coded using the structured observation instruments. The structured observation instruments are designed to document dimensions of hearing quality with a focus on judicial engagement of parents, reasonable efforts discussion, reasonable efforts findings, detail of findings, removal and placement decisions, and case outcomes. A project assigned identifier will be used to associate the hearing with its court file, judge, and state.

When viewing the recorded hearings and case files, study team members will complete a hardcopy of the observation instruments. After the hardcopy instruments are completed, the study team members will enter the data into Qualtrics using a survey link. JBA has an enterprise license for the version of Qualtrics which has FedRAMP certification and an HHS ATO. This ensures that the product used for data collection already complies with all FISMA requirements. Like all such software, Qualtrics contains a user responsibility component and JBA has drafted policies around the use of Qualtrics to ensure compliance. This limits access to Qualtrics surveys, ensuring all projects utilize restricted access licenses. Every employee at JBA has their own Qualtrics license and are limited to the projects they can access in Qualtrics. This allows all users within a project to gain access to the survey, while ensuring all unauthorized users cannot. Qualtrics is centrally managed and routinely audited to ensure correct access rights are maintained. In addition, Qualtrics system activity is regularly monitored to ensure that all survey data collection conforms to expectations and all unusual behavior is immediately investigated as a potential security incident.

Completed hardcopies of the observation instruments will be stored in locked file cabinets by all Authorized Users as identified in **Attachment D** who are doing the coding. At the end of the project, each study team member shall shred all hardcopy instruments in their possession and shall sign a form confirming that all hardcopy hearing observation instruments have been destroyed.

Observation instrument data entered into Qualtrics must be pulled into secured folders within OneDrive. The OneDrive folder must be managed by a policy which limits access only to authorized personnel and must be audited for appropriate access rights on a quarterly basis. The project-assigned ID must be retained for each entry. The resulting analytic data sets will be used in additional analysis, likely conducted in SAS that exists outside of the OneDrive environment. All analysis and results files (i.e., those not containing PII) must be stored on OneDrive after completion of the analysis and reporting. The data files must be securely retained until project completion at which time they will be copied to an encrypted hard disk for JBA post-study secure storage, prepared for transfer to a data archive, and deleted from OneDrive.



**ATTACHMENT D**

Authorized Users: Roster of Individuals with Access to Data

Individuals named in this Attachment D are designated as Authorized Users. Subject to terms and conditions of the Agreement, Data Recipient may only share the Data with the Authorized Users. Any changes to the list of Authorized Users shall be approved in writing (email acceptable) by the Data Provider. Data Recipient shall not share the Data with anyone that is not an Authorized User. Staff that have access to project data must be trained in the project data handling procedures and approved by the data security officer in accordance with the company system security plan. Staff roles and whether they have access to case level personally identifiable information (“PII”) are indicated below.

NAME & ROLE	EMPLOYER	ADDRESS	PHONE & EMAIL	ACCESS TO CASE PII
Anne Fromknecht, MPH  Project Director; Data Collection Team	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 247-2631  Fromknecht@jbassoc.com	Yes
Alicia Summers, PhD  Co-Principal Investigator; Data Collection Team	Data Savvy Consulting	682 Talus Way Reno, NV 89503	(775) 686-8545  Alicia.d.summers@gmail.com	Yes
Sophia Gatowski, PhD  Co-Principal Investigator; Data Collection Team	Systems Change Solutions	2-6988 177th Street Surrey, B.C., CANADA V3S 2K1	(778) 575-5779  sgatowski@ymail.com	Yes
Eva Klain, JD  Data Collection Team	ABA Center on Children and the Law	1050 Connecticut Avenue, NW, Suite 400 Washington, DC 20036	(202) 662-1681  Eva.Klain@americanbar.org	Yes
Julie Murphy, MSW	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA	(703) 528-3230  Murphy@jbassoc.com	Yes

Data Collection Team		22201		
Loren Masters, MPH Data Analyst	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Masters@jbassoc.com	No
Nichole Sturfels, MPH Data Security Officer	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Sturfels@jbassoc.com	No
Timothy Pitsch IT Coordinator	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Pitsch@jbassoc.com	No
Yuan Wang, MS Data Analyst	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Wang@jbassoc.com	No
Tammy Richards, MEd Writing Team	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Richards@jbassoc.com	No
Susan Higman, PhD Writing Team	James Bell Associates	2000 15th Street, North Suite 100 Arlington, VA 22201	(703) 528-3230 Higman@jbassoc.com	No

REPORT | Updated August 2022

# Data Security Plan

Understanding Judicial Decision-Making and Hearing Quality in Child Welfare

# Data Security Plan

## Understanding Judicial Decision-Making and Hearing Quality in Child Welfare

### Authors

Anne Fromknecht and Matthew Poes, James Bell Associates

### Submitted to

Christine K. Fortunato, Ph.D., Contract Officer's Representative  
Alysia Y. Blandon, Ph.D., Contract Officer's Representative  
Sarah Blankenship, Ph.D., Project Specialist  
Office of Planning, Research, and Evaluation  
Administration for Children and Families  
U.S. Department of Health and Human Services  
Contract Number: HHSP233201500133I  
Task Order Number: HHSP23337010T

### Prepared by

James Bell Associates  
3033 Wilson Boulevard, Suite 650  
Arlington, VA 22201  
(703) 528-3230  
[www.jbassoc.com](http://www.jbassoc.com)

Anne Fromknecht, M.P.H.  
Project Director



# Contents

---

Project Information .....	1
Contract Information .....	1
Description .....	1
Data Types, Access, Collection, Storage, Encryption, and Transmission .....	4
Online Survey of Judges .....	4
Hearing Observation Instrument .....	6
Court Case File Review Instrument.....	8
Child Welfare Agency Administrative Data .....	11
Contact Tracking Matrix 2 .....	12
Site Specific Datafiles .....	13
Data Environment.....	15
JBA Laptops .....	15
JBA Microsoft Office 365 SharePoint Online and OneDrive .....	17
Qualtrics.....	19
Dedoose .....	22
Chorus Call .....	23
Reporting Data Breaches/Incident Response .....	25
Training Procedures for Data Security .....	26
Data Disposition .....	27
Data Archive by JBA.....	27
Transfer to Data Archive.....	27
Annual Data Security Report.....	29
 <b>Exhibits</b>	
Exhibit 1. Key Roles .....	2

Exhibit 6. Data Lifecycle of Online Survey of Judges ..... 6

Exhibit 7. Data Lifecycle of Hearing Observation Instrument ..... 7

Exhibit 8. Data Lifecycle of Court Case File Instrument ..... 9

Exhibit 9. Data Lifecycle of Child Welfare Agency Administrative Data..... 12

Exhibit 10. Data Lifecycle of the Contract Tracking Matrix 2 ..... 13

Exhibit 11. Site Specific Datafiles ..... 14

# Project Information

---

## Contract Information

- Contract name: Understanding Judicial Decision-Making and Hearing Quality in Child Welfare
- Contract number: HHSP233201500133I
- Task order number: HHSP23337010T
- Start date: September 26, 2018
- End date: September 22, 2023
- Contract Officer's Representatives:
  - Alysia Blandon, Ph.D.
- Co-Principal Investigators:
  - Alicia Summers, Ph.D.; Data Savvy Consulting
  - Sophie Gatowski, Ph.D.; Systems Change Solutions
- Project Director:
  - Anne Fromknecht, M.P.H.; James Bell Associates

## Description

This is the Data Security Plan (DSP) for the Understanding Judicial Decision-Making and Hearing Quality project operating under the Office of Planning, Research, and Evaluation (OPRE) within the Administration for Children and Families (ACF). The purpose of this project is to deepen the understanding of judicial decision-making and hearings during the life of a child welfare case. The project includes a review of the knowledge base, proposed design options for the study of judicial decision-making and hearing quality in child welfare, a pre-testing and feasibility study, and full implementation of a selected study or studies.

The goal of the study is to better understand how individual and contextual factors influence judges' decisions about whether child welfare agencies made reasonable efforts to prevent child removals from the home and to reunify children who have been removed. These factors include pre- and between hearing communication (such as depth of information in reports), hearing quality components (such as depth of discussion and how judges engage parents during hearings), case characteristics, judicial characteristics, timing of the initial hearing, and the timing and frequency of review hearings. Additionally, the study explores how judges' reasonable efforts decisions relate to the likelihood of reunification and the time for children to achieve permanency. Planned data

collection includes a web survey of judges, observation of recorded child welfare hearings, and review of court case files. If relevant information is not available in court case files (e.g., child's race/ethnicity), we will request the data from the child welfare agency's case management information system.

This DSP will be updated annually, or as new information collection is planned for future phases of the project.

## Key Roles

Key roles on the project are listed in exhibit 1. All employees, consultants, subcontractors (at all tiers), and employees of each subcontractor, who perform work under this contract/subcontract, are trained on data privacy issues. Initial and annual refresher trainings are provided in the following ways: 1. incident response training provided by the JBA Chief Risk Officer; 2. PII and IT security training provided by JBA IT contractor Business Engineering Inc. (BEI); and 3. project specific data handling and security training provided by the JBA Chief Risk Officer. Study team members are required to read and sign a confidentiality pledge.

### Exhibit 1. Key Roles

Organization	Name	Role
James Bell Associates	Anne Fromknecht	Project Director
Systems Change Solutions	Sophie Gatowski	Co-Principal Investigator
Data Savvy Consulting	Alicia Summers	Co-Principal Investigator
American Bar Association Center on Children and the Law	Eva Klain	Stakeholder and Expert Consultant Task Lead

## Personnel Screening

JBA has aligned its policies around personnel screening with the control requirements in NIST 800-53 rev. 4. Personnel screening has a baseline requirement that is modified based on project specific requirements. All personnel are required to be able to pass any necessary background checks required to obtain a PIV card or gain access to any federal data systems if needed for a project. The baseline requirements, beyond the above-mentioned hiring requirement, are as follows:

- All staff assigned to work on a project will have completed all necessary security trainings before accessing any project data.
- All staff assigned will recertify annually.



- All staff with access to project data will be fully indoctrinated to the data they are accessing and recertified annually.

The training and data indoctrination process involves both general IT security training and project specific data security training to ensure all staff with access to the data are aware of the expected acceptable access and protection requirements of said data.

## **Personnel Termination or Reassignment**

JBA has in place standard policies and procedures to address data system security and project level security in the event of a staff termination or reassignment. This process is consistent with all relevant controls and is designed to ensure that staff with access to sensitive data can do no harm. The process quality is controlled via a set of associated checklists to ensure all steps are completed and to document the appropriate termination process. Upon termination or reassignment, the following procedures are followed:

- The IT manager disables information system access within 1 hr.; this is coordinated ahead of time.
- The IT manager terminates/revokes any IT authenticators/credentials associated with the individual.
- In the event of a termination, HR department conducts exit interviews that include a discussion of all data security issues such as turning over all data and hardware, requirement to not obtain, store, or remove any project data, and to not attempt access to any data systems.
- The IT manager retrieves all security-related organizational information system-related property within 5 days.
- IT manager retains access to organizational information and information systems formerly controlled by terminated individual; and
- The IT manager notifies the Vice President of Finance and Administration, the Executive Vice President, and the data system security managers immediately upon completion of the above steps.
- The project director will inform the COR by email within 2 business days that a given employee is no longer part of the project research team and all access rights have been revoked.

# Data Types, Access, Collection, Storage, Encryption, and Transmission

---

The JBA team will ensure that all data, including all sensitive and personally identifiable information (PII) in its possession, is stored and maintained in accordance with the JBA SSP. All PII whether sensitive or not will be protected from inappropriate access, use, and disclosure. Electronic PII data for the full study will be collected or viewed in the following formats: online survey files, raw audio recordings, raw video recordings, court case files, child welfare case files, and a Microsoft Excel contact tracking matrix.

The remainder of this section will detail the lifecycle of the data collected as part of the full study from its creation to the eventual desensitization of the information and the decommissioning of any underlying storage devices.

## Online Survey of Judges

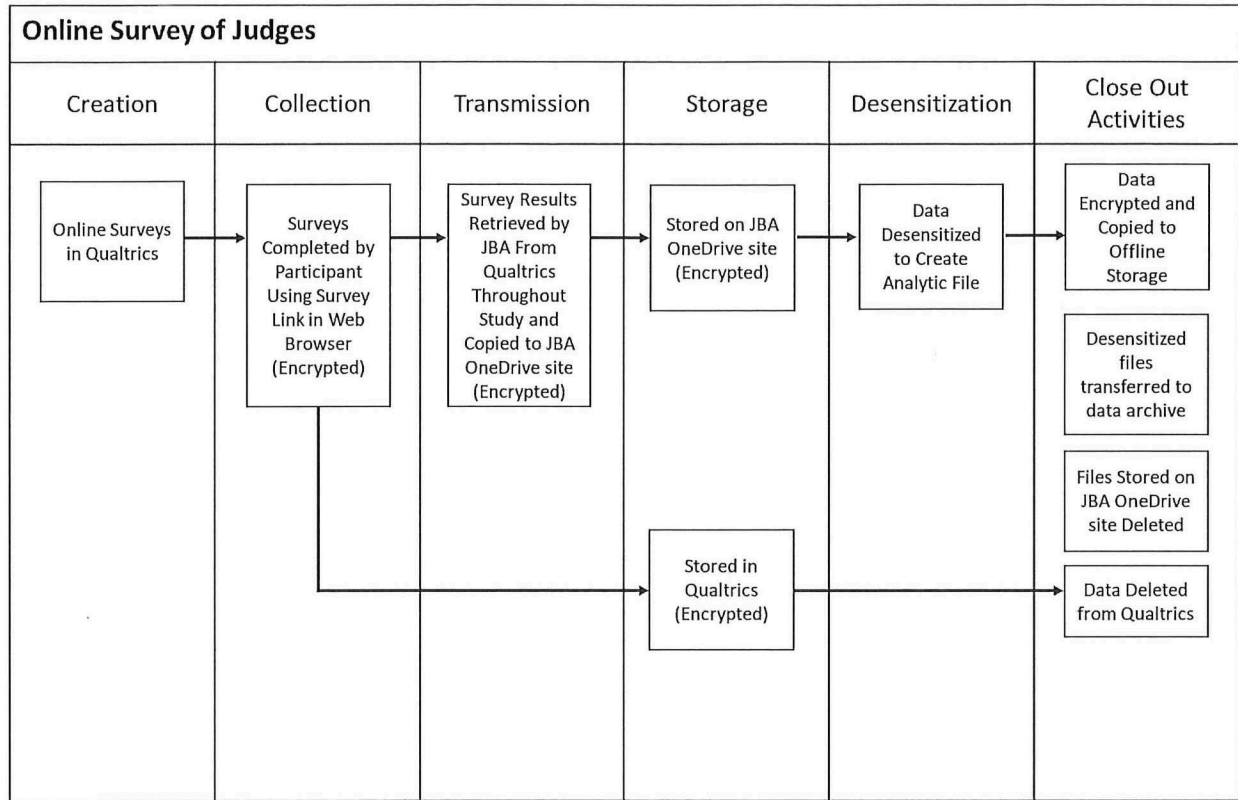
To gather information about the judges in selected study sites, we will administer a short, online survey to the 8 study judges. CIP Directors at each study site will provide contact information for the judges overseeing child welfare cases in that court. Two judges will be surveyed per study state for a total of 8 judges. Judges will share (1) demographic information, (2) the number of years the judge(s) have been hearing child welfare cases in their jurisdiction, (3) whether or not the judges hear only child welfare cases or a variety of case types (e.g., such as general jurisdiction judges who can hear child welfare, juvenile justice, civil and criminal matters), (4) their perceptions about their role in reasonable efforts findings, (5) what informs their reasonable efforts decisions, and (6) training they've received on reasonable efforts findings. The questions can be quickly answered using multiple choice items and short open-ended response fields. The information collection is not subject to the Privacy Act. Information will not be maintained in a paper or electronic system from which data are actually or directly retrieved by an individuals' personal identifier.

Survey data collection will happen using Qualtrics. JBA has an enterprise license for the version of Qualtrics which has FedRAMP certification and an HHS ATO. This ensures that the product used for data collection already complies with all FISMA requirements. Like all such software, Qualtrics contains a user responsibility component and JBA has drafted policies around the use of Qualtrics to ensure compliance. This limits access to Qualtrics surveys, ensuring all projects utilize restricted access licenses. Every employee at JBA has their own Qualtrics license and projects utilize a sharing process to create Qualtrics project surveys. This allows all users within a project to gain access to the survey, while ensuring all unauthorized users cannot. Qualtrics is centrally managed

and routinely audited to ensure correct access rights are maintained. In addition, Qualtrics system activity is regularly monitored to ensure that all survey data collection conforms to expectations and all unusual behavior is immediately investigated as a potential security incident. Note that for this information collection, data is not expected to be highly sensitive, though the same precautions will be taken regardless.

Survey data collected via Qualtrics will be pulled into secured folders within OneDrive. The OneDrive folder will be managed by a policy which limits access only to authorized personnel and will be audited for appropriate access rights on a quarterly basis. The data within OneDrive will then be desensitized by JBA staff to create the analytic file. Desensitizing the data will involve removing any participant names and IP addresses and redacting (coding) any references to PII in the qualitative responses in the surveys. A second team member will review the file to ensure the file is completely desensitized. The state name associated with data will be retained. The resulting analytic data sets will be used in additional analysis, likely conducted in SAS that exists outside of the OneDrive environment. A cross-walk document that links participant PII to the project-assigned identifier used in the desensitized data file will be maintained separately (as part of the Contact Tracking Matrix described below) in a secure file location. All analysis and results files (i.e., those not containing PII) will be transferred and stored on OneDrive after completion of the analysis and reporting. The data files will be securely retained until project completion at which time they will be copied to an encrypted hard disk for JBA post-study secure storage (see Data Disposition section below for more details), prepared for transfer to a data archive, and deleted from OneDrive. Exhibit 6 displays the lifecycle of survey data.

**Exhibit 6. Data Lifecycle of Online Survey of Judges**



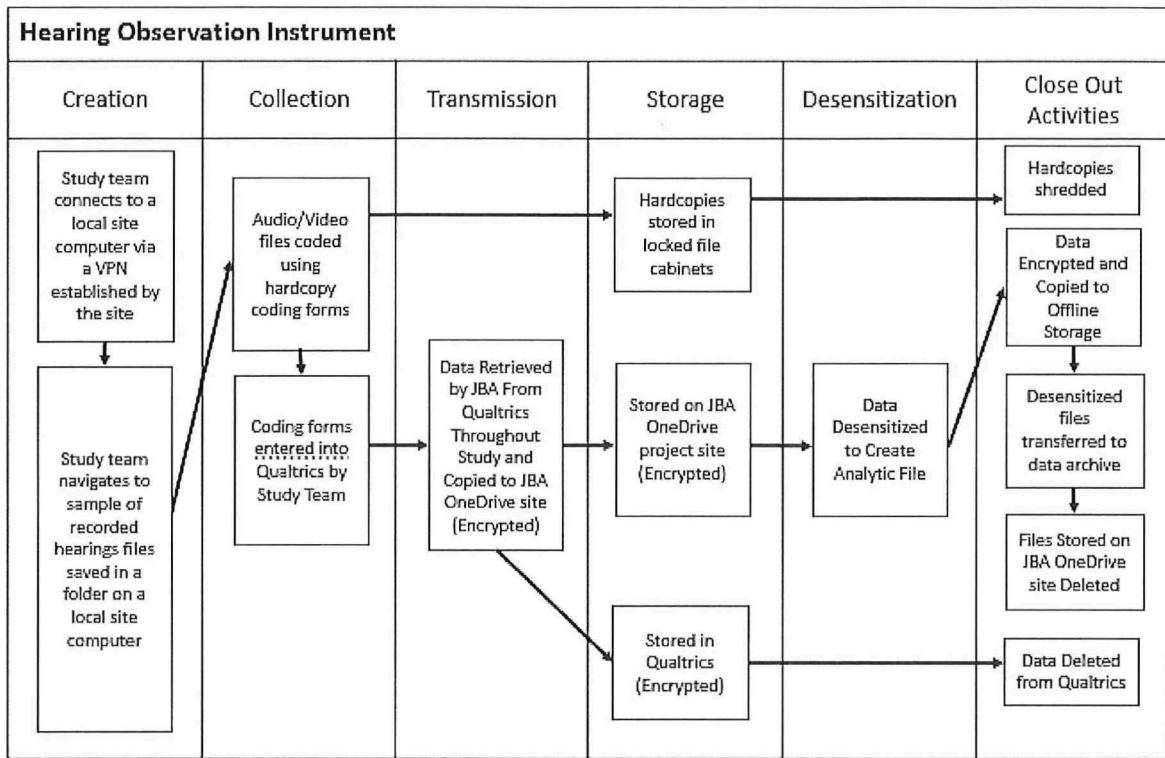
## Hearing Observation Instrument

Audio or video recordings from a sample of initial court hearings will be reviewed and coded using the hearing observation instrument. The structured observation instrument is designed to assess dimensions of hearing quality with a focus on judicial engagement of parents, reasonable efforts discussion, reasonable efforts findings, detail of findings, and removal and placement decisions.

A project assigned identifier will be documented on the hearing observation instrument to represent the state, judge, and case number. This is needed to link the observed hearing with its court file and to information about judicial characteristics obtained via the online survey of judges. Coders' names will be collected to facilitate reliability testing. The instrument will also collect the date the hearing was held and its length. No PII about the child, parents, or other family members will be collected on the hearing observation instrument, however, the study team will have access to PII that is included on the recording. This includes images of faces, names stated during the hearing, and other PII that may be said during the hearing.

Per guidance from the OPRE Data Security Team, the study team will either access court data via a VPN connection setup by each study site or in-person using a state-owned computer. JBA will never save or be in possession of the recorded hearing files. The study team will request that access to files be set to “read only.” Exhibit 7 shows the data lifecycle for audio/video recording files.

### Exhibit 7. Data Lifecycle of Hearing Observation Instrument



The Project Director will coordinate with each state CIP’s IT team to establish a VPN connection for team members. Once connected to a local site computer through the VPN, study team members will view and code the audio or video recordings for the sample of initial hearings. The Project Director will work with each court site to put in place a data use agreement that would be signed by each of the study team members and specify which files the team will need to access. Access and connection details for each site are provided below.

- Oregon:** The study team will conduct data collection in-person using a state-owned computer in a private setting (e.g., no one else can view the screen, not using public wi-fi) to view the files.

When viewing the recorded hearings, study team members will complete a hardcopy (pen and paper) of the hearing observation instrument. After the hardcopy instrument is completed, the study team members will enter the data into Qualtrics using a survey link. As noted above, JBA has an enterprise license for the version of Qualtrics which has FedRAMP certification and an HHS ATO.

This ensures that the product used for data collection already complies with all FISMA requirements. Like all such software, Qualtrics contains a user responsibility component and JBA has drafted policies around the use of Qualtrics to ensure compliance. This limits access to Qualtrics surveys, ensuring all projects utilize restricted access licenses. Every employee at JBA has their own Qualtrics license and projects utilize a sharing process to create Qualtrics project surveys. This allows all users within a project to gain access to the survey, while ensuring all unauthorized users cannot. Qualtrics is centrally managed and routinely audited to ensure correct access rights are maintained. In addition, the JBA Qualtrics Administrator manually monitors accounts on a monthly basis to ensure only approved users have access to the survey data. All unusual behavior is immediately investigated as a potential security incident as part of JBA Incident Response.

Completed hardcopies of the hearing observation instruments will be stored in locked file cabinets by all study team members that are participating in data collection. At the end of the project, each study team member will shred all hardcopy instruments in their possession and will sign a form confirming that all hardcopy hearing observation instruments have been destroyed.

Hearing observation instrument data entered into Qualtrics will be pulled into secured folders within OneDrive within one month of the end of data collection. The OneDrive folder will be managed by a policy which limits access only to authorized personnel and will be audited for appropriate access rights on a quarterly basis. The data within OneDrive will then be desensitized by JBA staff to create the analytic file. Desensitizing the data will involve replacing the state and judges' names with the project-assigned ID. The project-assigned ID will be retained for each entry. The resulting analytic data sets will be used in additional analysis, likely conducted in SAS that exists outside of the OneDrive environment. A cross-walk document that links study state and judge to the project-assigned ID used in the desensitized data file will be maintained separately (as part of the Contact Tracking Matrix 2 described below). All analysis and results files (i.e., those not containing PII) will be transferred and stored on OneDrive after completion of the analysis and reporting. The data files will be securely retained until project completion at which time they will be copied to an encrypted hard disk for JBA post-study secure storage (see Data Disposition section below for more details), prepared for transfer to a data archive, and deleted from OneDrive.

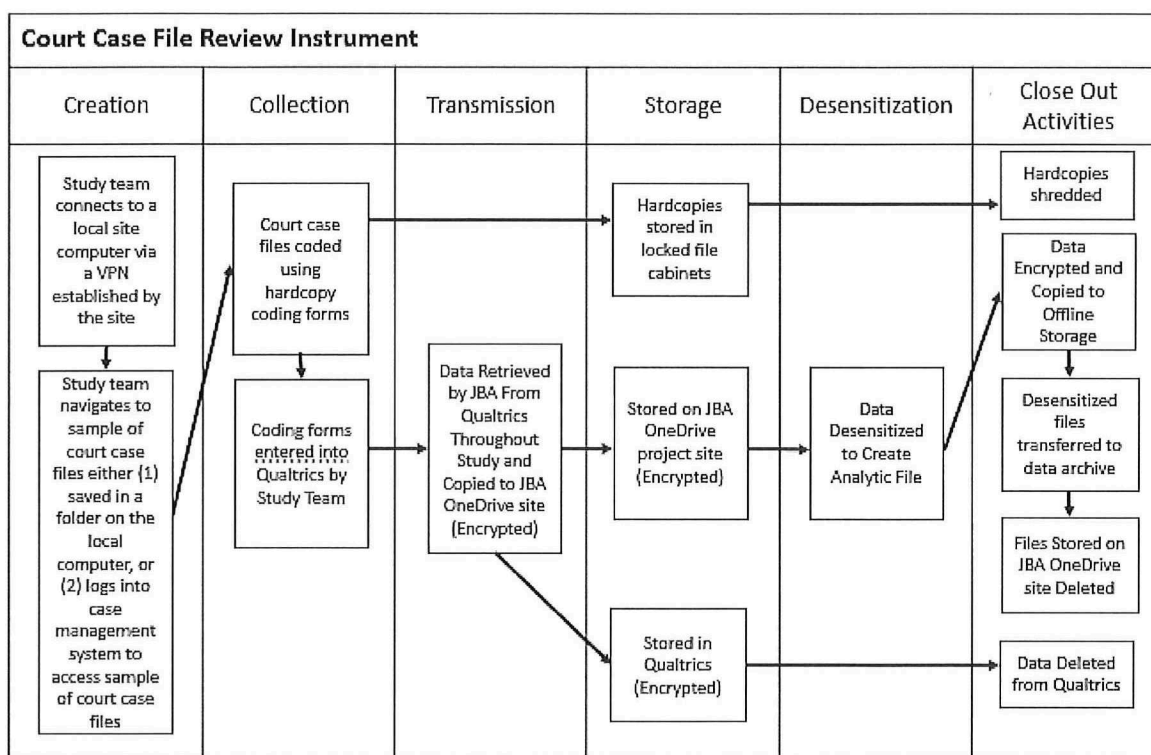
## Court Case File Review Instrument

Court case files from the sample of observed initial hearings will be coded by study team members using the structured court case file review instrument. This instrument is designed to collect information about judicial reasonable efforts findings, the breadth and depth of reasonable efforts topics included in child welfare agency reports submitted to the court at review hearings, and case outcomes.

As with the hearing observation instrument, a project assigned identifier will also be documented on the instrument to represent the state, judge, and case number. This is needed to link the case file to its observed hearing and information about judicial characteristics obtained via the online survey of judges. Coders' names will be collected to facilitate reliability testing. The instrument will also collect the date the hearing was held and its start and end times. No PII about the child, parents, or other family members will be collected.

Per guidance from the OPRE Data Security Team, the study team will access court data via a VPN connection setup by each study site or in-person using a state-owned computer. JBA will never save or be in possession of the court case files. Exhibit 8 shows the data lifecycle for court case files.

### Exhibit 8. Data Lifecycle of Court Case File Instrument



The Project Director will coordinate with each state CIP's IT team to establish a VPN connection for team members. Once connected to a local site computer through the VPN, study team members will view and code the sample of court case files. The Project Director will work with each court site to put in place a data use agreement that would be signed by each of the study team members and specify which files the team will need to access. Access and connection details for each site are provided below.

- **Oregon:** The study team will conduct data collection in-person using a state-owned computer in a private setting (e.g., no one else can view the screen, not using public wi-fi) to view the files.

When viewing the court case files, study team members will complete a hardcopy of the court case file review instrument. After the hardcopy instrument is completed, the study team members will enter the data into Qualtrics using a survey link. As noted above, JBA has an enterprise license for the version of Qualtrics which has FedRAMP certification and an HHS ATO. This ensures that the product used for data collection already complies with all FISMA requirements. Like all such software, Qualtrics contains a user responsibility component and JBA has drafted policies around the use of Qualtrics to ensure compliance. This limits access to Qualtrics surveys, ensuring all projects utilize restricted access licenses. Every employee at JBA has their own Qualtrics license and projects utilize a sharing process to create Qualtrics project surveys. This allows all users within a project to gain access to the survey, while ensuring all unauthorized users cannot. Qualtrics is centrally managed and routinely audited to ensure correct access rights are maintained. In addition, Qualtrics system activity is regularly monitored to ensure that all survey data collection conforms to expectations and all unusual behavior is immediately investigated as a potential security incident.

Completed hardcopies of the court case file review instruments will be stored in locked file cabinets by all study team members that are participating in data collection. At the end of the project, each study team member will shred all hardcopy instruments in their possession and will sign a form confirming that all hardcopy court case file instruments have been destroyed.

Court case file instrument data entered into Qualtrics will be pulled into secured folders within OneDrive. The OneDrive folder will be managed by a policy which limits access only to authorized personnel and will be audited for appropriate access rights on a quarterly basis. The data within OneDrive will then be desensitized by JBA staff to create the analytic file. Desensitizing the data will involve replacing the state and judges' names with the project-assigned ID. The project-assigned ID will be retained for each entry. The resulting analytic data sets will be used in additional analysis, likely conducted in SAS that exists outside of the OneDrive environment. A cross-walk document that links study state and judge to the project-assigned identifier used in the desensitized data file will be maintained separately (as part of the Contact Tracking Matrix 2 described below) in a secure file location. All analysis and results files (i.e., those not containing PII) will be transferred and stored on OneDrive after completion of the analysis and reporting. The data files will be securely retained until project completion at which time they will be copied to an encrypted hard disk for JBA post-study secure storage (see Data Disposition section below for more details), prepared for transfer to a data archive, and deleted from OneDrive.



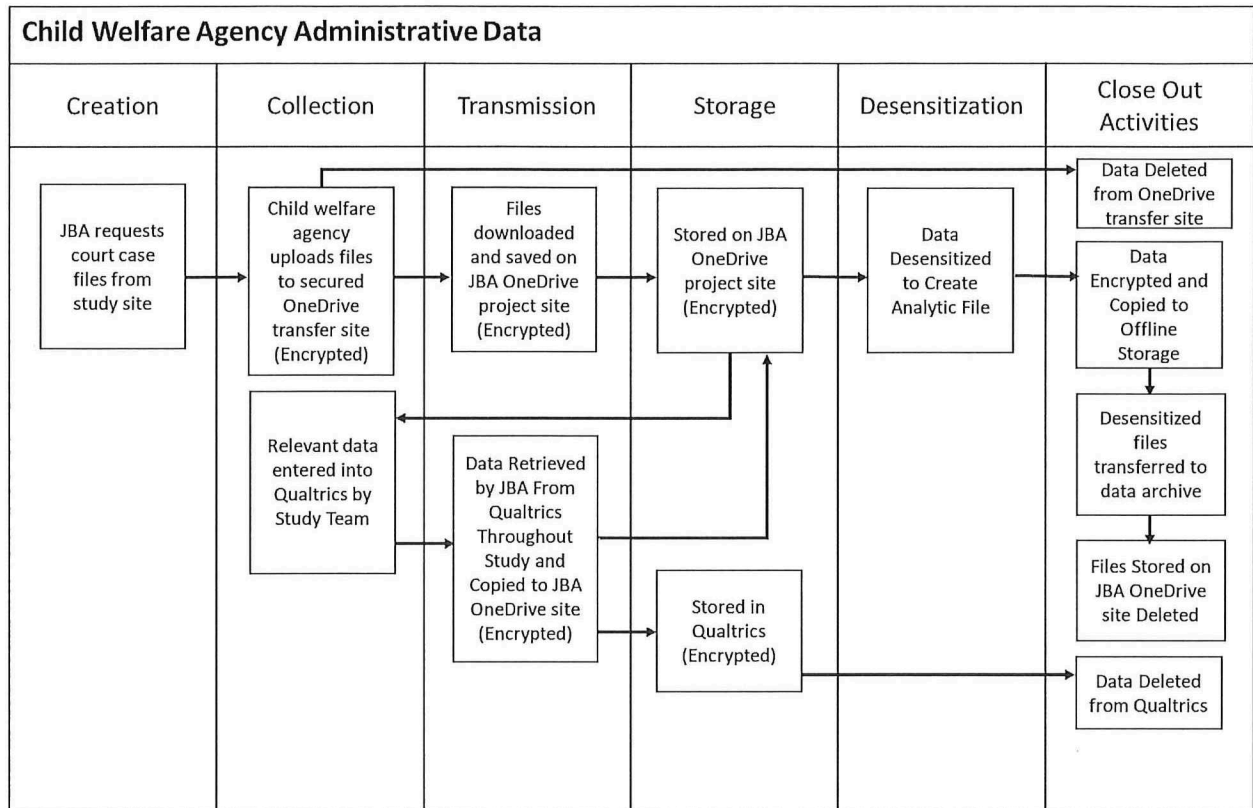
## Child Welfare Agency Administrative Data

If relevant demographic information for the child is not available in the court case files, we will work with data system staff from the child welfare agency to collect this data. Examples may include the child's race and ethnicity, which are often not available in court case files. The case file number will be used to identify cases where data is missing. In these cases, we will request that the child welfare agency securely transfer a file with demographic or other case information relevant to the study and not available from the court case files. File types may include a pdf report from their data system or an excel file. The child welfare agency would securely transfer the files to JBA using a secured OneDrive folder with limited access created by JBA. The folder will be accessible to the child welfare agency only until the transfer is complete. After the transfer, the OneDrive transfer folder will be cleansed. The project director will save the files to the OneDrive project folder. The OneDrive project folder will be managed by a policy which limits access only to authorized personnel and will be audited for appropriate access rights on a quarterly basis. These files will contain PII, however, no PII will be documented by the study team.

When viewing the child welfare agency administrative data, study team members will enter relevant data into Qualtrics using a survey link. The project-assigned ID will also be entered to allow data to be linked to the court case file and hearing observation data. As noted above, JBA has an enterprise license for the version of Qualtrics which has FedRAMP certification and an HHS ATO. This ensures that the product used for data collection already complies with all FISMA requirements. Like all such software, Qualtrics contains a user responsibility component and JBA has drafted policies around the use of Qualtrics to ensure compliance. This limits access to Qualtrics surveys, ensuring all projects utilize restricted access licenses. Every employee at JBA has their own Qualtrics license and projects utilize a sharing process to create Qualtrics project surveys. This allows all users within a project to gain access to the survey, while ensuring all unauthorized users cannot. Qualtrics is centrally managed and routinely audited to ensure correct access rights are maintained. In addition, Qualtrics system activity is regularly monitored to ensure that all survey data collection conforms to expectations and all unusual behavior is immediately investigated as a potential security incident.

All analysis and results files (i.e., those not containing PII) will be transferred and stored on OneDrive after completion of the analysis and reporting. The data files will be securely retained until project completion at which time they will be copied to an encrypted hard disk for JBA post-study secure storage (see Data Disposition section below for more details), prepared for transfer to a data archive, and deleted from OneDrive. Exhibit 9 displays the lifecycle of child welfare agency administrative data.

## Exhibit 9. Data Lifecycle of Child Welfare Agency Administrative Data

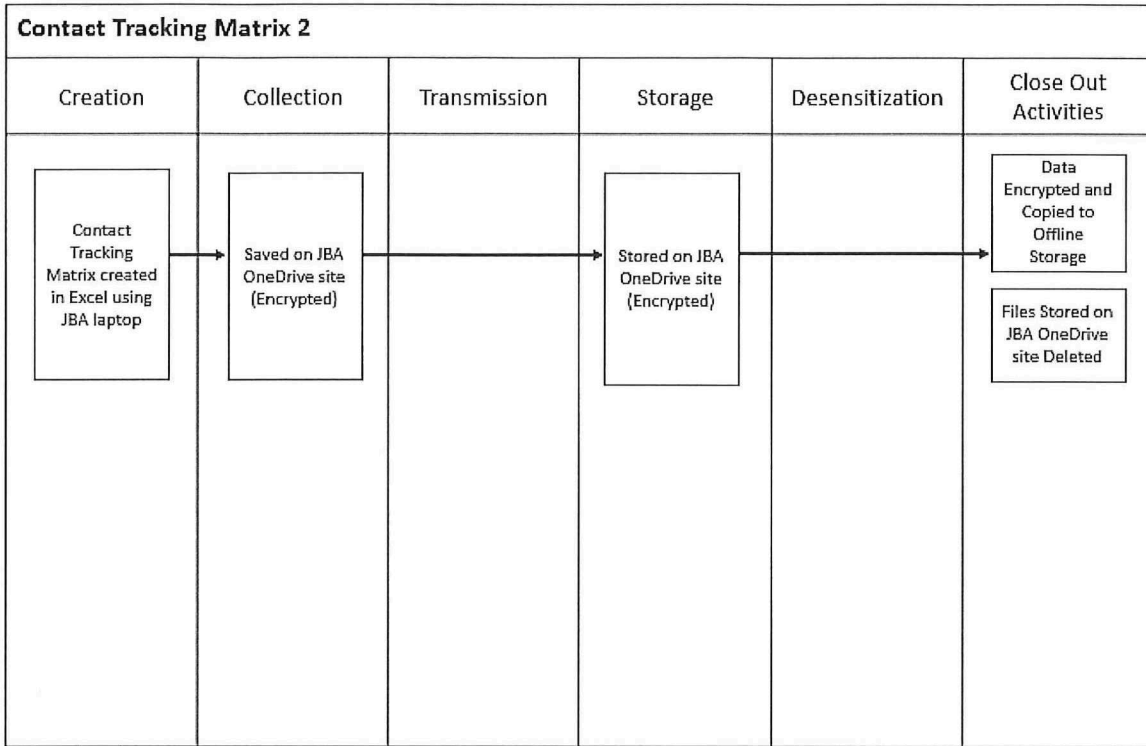


## Contact Tracking Matrix 2

The Contact Tracking Matrix 2 is a password protected Microsoft Excel file saved on OneDrive. The Project Director manages the password and is made available to all individuals work on this aspect of the project. The document is stored in OneDrive which has limited, least privilege access to staff approved to work on the project. The Contact Tracking Matrix 2 will include the names, email addresses, and states for participating CIP Administrators and judges and will track when initial study invitation emails are sent to selected CIP Administrators and when introductory calls are scheduled and held. The matrix will also designate a JBA issued ID number for each study state, each judge, and each case number in the study sample, The names and email addresses for judges will be provided by the CIP contact from each study state. Project staff involved in desensitizing datasets will update the Contact Tracking Matrix 2 throughout the data collection phases of the project to (1) link the observed hearing with its court file and to information about judicial characteristics obtained via the online survey of judges, and (2) to track administration and completion of the online survey of judges and coding for each case. At project completion, the Contract Tracking Matrix 2 will be copied to an encrypted hard disk for JBA post-study secure

storage (see Data Disposition section below for more details) and deleted from OneDrive. Exhibit 10 displays the lifecycle of Contract Tracking Matrix 2 data.

**Exhibit 10. Data Lifecycle of the Contract Tracking Matrix 2**

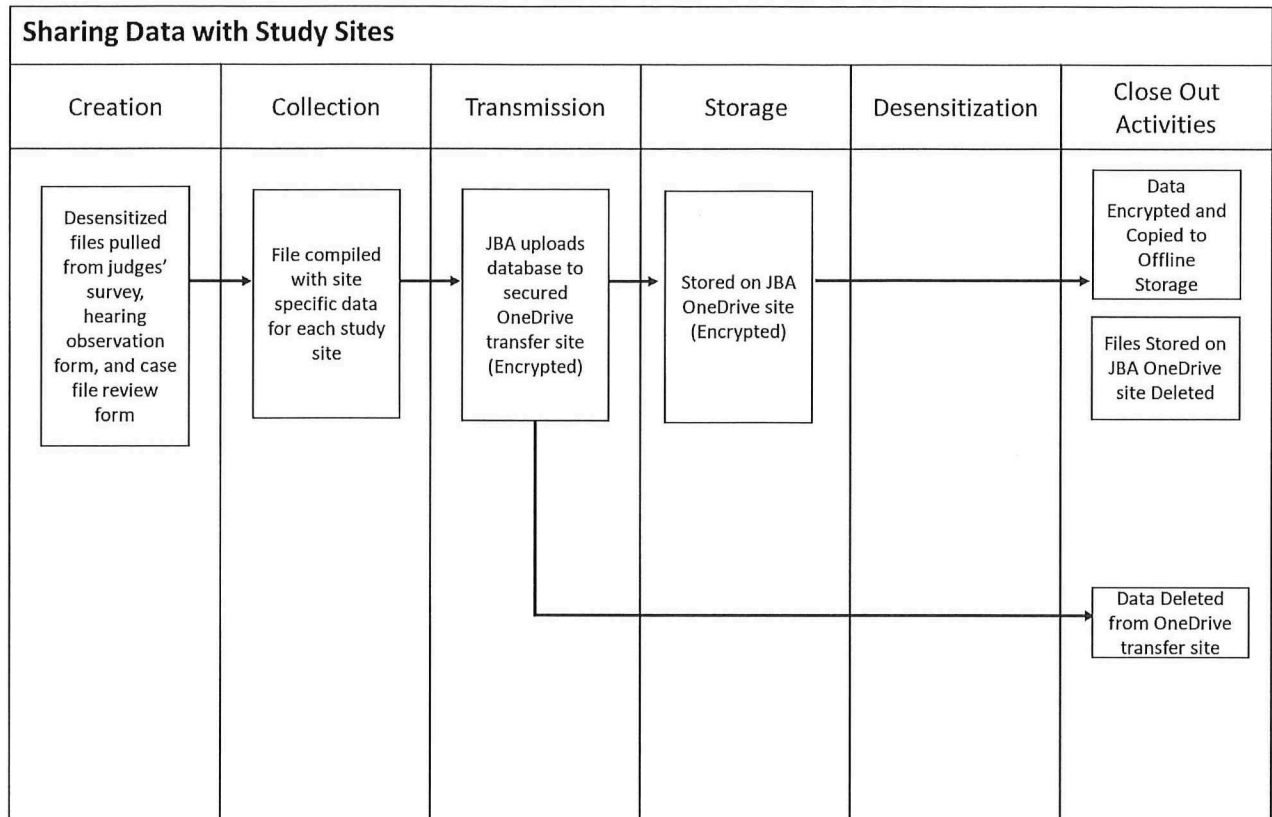


**Site Specific Datafiles**

A password protected Excel file will be compiled for each study site that includes all desensitized data collected from the judges' survey, hearing observation form, and court case file review form. This will be shared with the study site at the end of data collection. Sharing data back in this way is a sign of gratitude for participation and will serve as an incentive for CIPs to participate. Many CIPs lack data collection capacity so having this data file will enable them to analyze data for their own purposes. To ensure a safe transfer of data from JBA to each study site, secured OneDrive folders will be created with limited access. The folder will be accessible to a study site until the transfer has been confirmed. Study sites will only have access to data from their state. Following the completion of the transfer, the OneDrive transfer folder will be cleansed by the Project Director and confirmed by the IT coordinator. The Project Director will notify the COR once files have been deleted. At project completion, each site specific datafile will be copied to an encrypted hard disk for JBA post-study

secure storage (see Data Disposition section below for more details) and deleted from OneDrive. Exhibit 11 displays the lifecycle of the site specific datafiles.

### Exhibit 11. Site Specific Datafiles



# Data Environment

---

## JBA Laptops

JBA Laptops are corporate resources maintained within the standards for industry best practices for protecting the confidentiality and integrity of company and customer data. All laptops are configured with a software firewall, anti-virus software, anti-malware software, and are enrolled with an enterprise patch management system to provide the operating system with the latest security patches from Microsoft. For this project, all sub-contractors accessing sensitive data will utilize JBA corporate laptops in order to ensure that all necessary controls can be maintained. No sensitive project data will be accessed by non-JBA devices.

## Access Controls

- JBA Laptops require username and password authentication. All computer accounts require the use of a password. Default guest accounts are disabled by group policy, meaning that no guest login is permitted, as would be the case in a default windows profile.
- JBA Laptops utilize separate user and administrator roles. Administrators are members of the Administrator group. Users are members of the users group.
- Non-Administrators are not provided administrative access to the Windows OS and do not have the capability to add or remove software, change audit settings, or adjust security settings configured by group policy.
- Permissions granted to a user account are based on the principal of least privilege so that users are not afforded access to the system greater than their minimum requirements.
- Passwords used by user and administrative accounts require a minimum of 8 characters and must be complex, meaning that they must contain at least one number, one capital letter, and one symbol.

## Remote Access

Remote Access to JBA laptops is restricted to the Administrators group for remote system administration. All other remote access into a JBA laptop is not permitted and managed through security and firewall policies.

## Mobile Device Management

- JBA laptops are managed remotely using suites from Trend Micro, WebRoot, and DUO. Our mobile device management infrastructure allows complete remote management and security of all JBA laptops.

- As part of the mobile device management policies and procedures, JBA ensures that all required patches are implemented across all JBA laptops in a timely manner, typically within 24 hours of release.
- In the event that a JBA laptop is compromised, missing, or broken, it can be remotely locked, preventing unauthorized access to any JBA systems. Note that this process is only possible if the device has an internet connection, but JBA laptops are setup such that no local sensitive data can be stored. Any attempt to access remotely stored data would lead to the device being locked.

## **Identification and Authentication**

All accounts on JBA laptops are issued to an individual and the sharing of account information is prohibited by policy and reinforced through mandatory training. All accounts have unique passwords only known by the account owners.

## **Auditing and Monitoring**

The following events are logged by systems that store or process sensitive information related to this project. These requirements are based on the FedRAMP baseline and when recorded will allow for after-the-fact investigations of security incidents.

- Successful and unsuccessful account logon events
- Account management events
- Object Access
- Policy Change
- Privilege Functions
- Process Tracking
- System Events

## **System and Communication Protection**

- Data at Rest - To protect the integrity and confidentiality of data at rest, JBA laptops have an encrypted H drive for storage of project data files. Staff have customized browser settings that download directly to the encrypted H drive.
- Data in Transit - JBA will only transfer sensitive information to either the JBA OneDrive Online site or the JBA SharePoint Online site (for staff data) for the storage of sensitive information. The Microsoft Office 365 OneDrive and SharePoint Online system is a FedRAMP accredited system with documented controls that protect both the confidentiality and the integrity of data being transferred into and out of the OneDrive and SharePoint Online system. Additional details about the Microsoft protections can be found in the Microsoft Office 365 FedRAMP package.

# JBA Microsoft Office 365 SharePoint Online and OneDrive

JBA is a subscriber to the FedRAMP ATO-holding Microsoft Online 365 Service with both Business and Enterprise licenses. JBA operates multiple SharePoint Online sites to separate data between projects and access requirements within those projects. In addition to operating with Microsoft best practices for security, SharePoint Online sites that will be used to store sensitive data will use the following additional controls that fall within JBA responsibilities for management. Additional documentation pertaining to the security of SharePoint Online can be found within their approved FedRAMP package.

## Access Controls

- JBA SharePoint Online and OneDrive requires users to authenticate using multi-factor authentication for all users who participate in groups with access to sensitive information.
- JBA SharePoint and OneDrive Online uses role-based access permissions to limit access to sensitive data and separate access based on assigned roles.
- Non-Administrators do not have access to modify the security policies, sharing permissions or role-based access permissions.
- Permissions granted to a user account are based on the principal of least privilege so that users are not afforded access to the system greater than their minimum requirements.
- Passwords used by user and administrative accounts require a minimum of 16 characters and must be complex, meaning that they must contain at least one number, one capital letter, and one symbol.

## Remote Access

JBA only permits users with a valid account to access to the JBA operated SharePoint sites. Anonymous or guest access is prohibited. JBA SharePoint Online is hosted on the FedRAMP approved Microsoft Office 365 SharePoint online service. Microsoft controls remote access to the SharePoint Platform. JBA controls user access into the JBA owned and operated sites. Security related to the transmission to and from SharePoint online is documented in the Microsoft FedRAMP package available to the government at <https://www.FedRAMP.gov>.

## Identification and Authorization

All accounts on a JBA SharePoint Online are issued to an individual and the sharing of account information is prohibited by policy and reinforced through mandatory training. All accounts have unique passwords only known by the account owners.

## **System and Communication Description**

JBA follows a set of policies and procures around system and communication controls to ensure all project data are maintained in a secure fashion as required by the project. The following controls are in place to ensure that all project data stored on Sharepoint and OneDrive are properly maintained for both security and integrity.

- JBA maintains an inventory of all project sensitive information for all projects.
- Every project is assigned its own Sharepoint site and associated OneDrive folder system. This ensures complete isolation of project data from other JBA assets and projects
- Microsoft monitors and guards against data loss and exposure.
- JBA relies on personnel controls to prevent the unauthorized transfer or exposure of data from Sharepoint or OneDrive. All employees are trained on appropriate use of project assets and are expected to follow protocols for the storing and sharing of data.
- SharePoint and Azure rely on TLS 1.2 or greater encryption for all data in transit. All project data uploaded to Sharepoint or OneDrive is transferred through a secure encrypted transfer meeting the TLS 1.2 or greater requirements. To avoid non-secure transfer of data, no project data is transferred directly to laptops or devices, through emails, or onto non-secure storage assets.
- Role Based Controls are put in place for all folders to ensure the least required access is granted to all users. These controls are routinely monitored to ensure appropriate access at all times.
- As standard, Microsoft Office 365 cloud products incorporate a robust encryption protocol for all data at rest and in transit. The encryption at rest protocol include BitLocker at all data centers and on JBA client machines.

## **Auditing and Monitoring**

The following events are required by JBA to be logged by all systems that store or process sensitive information related to this project. The systems must be capable of and configured to log the listed event types. These requirements are based on the FedRAMP requirements and will allow for after-the-fact investigations of security incidents.

- Successful and unsuccessful account logon events
- Account management events
- Object Access
- Policy Change
- Privilege Functions



- Process Tracking
- System Events

Additionally, SharePoint online will be configured to log the following additional events. The capability to log audit events of the SharePoint platform is documented in the SharePoint FedRAMP package.

- All Administrator Activity
- Authorization Checks
- Data Deletions
- Data Access
- Data Changes
- Permission Changes

All required audit activity will be recorded and reviewed by JBA staff on a monthly basis during active data collection, and monthly during analysis and follow-up periods, via the audit logs provided by Office 365 Console. Unusual activity defined by the list below will be immediately reported to the Project Director.

- Multiple and continuous failed login attempts
- Failed attempts to modify folder or object permissions
- Failed attempts followed by successful attempts to access data or objects
- Failed attempts to execute privileged functions to perform the following
  - Modify Groups or Roles
  - Modify Permissions
  - Create or Modify administrative accounts

## Qualtrics

JBA is a subscriber to the FedRAMP ATO-holding Qualtrics Service with Enterprise licenses. JBA operates multiple Qualtrics user accounts to separate data between projects and access requirements within those projects. In addition to operating with Qualtrics' best practices for security, Qualtrics Online services that will be used to store sensitive data will use the following additional controls that fall within JBA responsibilities for management. Additional documentation pertaining to the security of Qualtrics Online can be found within their approved FedRAMP package. Qualtrics customer responsibility requirements are fully followed by JBA in the setup of the Qualtrics online cloud service.

## Access Controls

- JBA Qualtrics online require login authentication with access to sensitive information through a token.
- JBA Qualtrics uses role-based access permissions to limit access to sensitive data and separate access based on assigned roles.
- JBA Qualtrics Cloud administration is managed at limited access, with user accounts only able to access their associated surveys.
- Non-Administrators do not have access to modify the security policies, sharing permissions or role-based access permissions. Monitoring of security controls is managed by the JBA Configuration Management Plan protocols and overseen by the Data Security Manager. The Configuration Management Plan is provided as an attachment.
- Permissions granted to a user account are based on the principal of least privilege so that users are not afforded access to the system greater than their minimum requirements.
- Passwords used by user and administrative accounts require 8 numbers and must be complex, meaning that they must appear random. All numeric based passcodes were derived from a random number generator and checked for common use.
- Passwords are updated based on routine checking of password breach, breached passwords are prohibited.

## Remote Access

- JBA only permits users with a valid account to access the JBA operated Qualtrics site. Anonymous or guest access is prohibited.
- JBA Qualtrics Online is hosted on the FedRAMP approved Qualtrics servers. Qualtrics controls remote access to the Qualtrics Platform. JBA controls user access into the JBA owned and operated sites. Security related to the transmission to and from Qualtrics online is documented in the Qualtrics package available to the government at <https://www.FedRAMP.gov>.

## Mobile Device Management

JBA laptops are the only mobile devices authorized to connect to the Qualtrics online system for the purpose of accessing sensitive information. This is included in the JBA Acceptable Use Policy, which is reviewed and signed by all JBA staff granted access to sensitive information.

## Identification and Authorization

All accounts on JBA's Qualtrics are issued to an individual and the sharing of account information is prohibited by policy and reinforced through mandatory training and auditing. All accounts have unique passwords only known by the account owners. The JBA Qualtrics Administrator provides accounts and ensures only staff approved to work on the project have access to the JDMHQ

surveys. In the event that a staff member leaves their access will be revoked in accordance with Personnel Termination or Reassignment Policy. Routine changes in credentials could create significant disruptions in the routine collection of data, while security will always be maintained at the highest level, routine credential changes will not be made if it is deemed to provide no benefit to the data integrity and security.

## **Auditing and Monitoring**

The following events are required by JBA to be logged by all systems that store or process sensitive information related to this project. The systems must be capable of and configured to log the listed event types. These requirements are based on the FedRAMP requirements and will allow for after-the-fact investigations of security incidents.

- Successful and unsuccessful account logon events
- Account management events
- Object Access
- Policy Change
- Privilege Functions
- Process Tracking
- System Events

All required audit activity will be recorded and reviewed by JBA staff on a monthly basis during active data collection, and analysis and follow-up periods, via the audit logs provided by Qualtrics. Unusual activity defined by the list below will be immediately reported to the Project Director. In addition, the Qualtrics accounts will be shut down after data collection to avoid errant data collection problems.

- Multiple and continuous failed login attempts
- Failed attempts to modify folder or object permissions
- Failed attempts followed by successful attempts to access data or objects
- Failed attempts to execute privileged functions to perform the following
  - Modify groups or roles
  - Modify permissions
  - Create or modify administrative accounts
- New IP address data activity
- New device activation

## **System and Communication Protection**

Qualtrics software is fully FedRAMP compliant.

- Data at Rest - Qualtrics is a FEDRamp certified application using cloud-based data systems managed by Qualtrics. Data is stored using an AES-256 bit encrypted system that meets FIPS 140-2 requirements. In addition, all data is stored behind a Qualtrics Key. No Qualtrics data is stored on local computers, ensuring robust availability and security.
- Data in Transit – Qualtrics is fully FedRAMP compliant and uses a Transport Layer Security encryption method for all data in transit, ensuring a secure upload from the JBA laptops or remote site to the Qualtrics servers. Response data is transmitted over HTTPS using the device's highest supported TLS version.

## **Dedoose**

Dedoose is a cross-platform application for analyzing qualitative and mixed methods research data. Dedoose was designed with security as a central component of its design, using the FedRAMP compliant cloud server service of Microsoft Azure. Dedoose was setup as a client on Azure to ensure it inherits the majority of security controls and numerous security certifications.

## **Access Controls**

- JBA's Dedoose account requires password authenticated login.
- JBA staff do not share Dedoose accounts; access to Dedoose is restricted within projects.
- Dedoose allows automatic account lockout after a specified number of login attempts. Our accounts provide for five failed login attempts before temporary lockout.
- Dedoose is set to timeout after 15 minutes idle.
- Dedoose makes use of 2-factor authentication.

## **Remote Access**

Dedoose is a cloud-based data analysis application and is exclusively accessed remotely. JBA only permits users with a valid account to access to the JBA operated Dedoose App. JBA Dedoose Online is hosted on the FedRAMP approved Azure servers. Dedoose controls remote access to the Dedoose Platform. JBA controls user access into the JBA owned and operated license. Security related to the transmission to and from Dedoose online is documented in the Microsoft Azure package available to the government at <https://www.FedRAMP.gov>.

## Identification and Authorization

The following events are required by JBA to be logged by all systems that store or process sensitive information related to this project. The systems must be capable of and configured to log the listed event types. These requirements are based on the FedRAMP requirements and will allow for after-the-fact investigations of security incidents.

- Successful and unsuccessful account logon events
- Account management events
- Object Access
- Policy Change
- Privilege Functions
- Process Tracking
- System Events

## System and Communication Protection

All data communication through Dedoose occurs through a 2-lock system. First Dedoose sets up an AES-256 CBC Encrypted SSL/TLS tunnel using premium SSL/TLS-EV certificate. The Servers then provide Dedoose client with a one way write key using RSA encryption. Dedoose client then applies a per user salt hashing algorithm (SHA-256) and encrypts this result with the one-way write key, RSA, to verify user password.

## Chorus Call

Chorus Call is a global audio-conferencing service allowing remote meeting collaboration and call hosting. Chorus Call will be used to host and record interviews with participants. Recordings are stored on secured and decentralized servers in an encrypted format. The audio files are transmitted, encrypted, to the call host only.

## Access Controls

JBA's Chorus Call account requires password authenticated login for hosts. Chorus Call conferences require passcode for entry and announce each entrant

## Identification and Authorization

The following events are required by JBA to be logged by all systems that store or process sensitive information related to this project. The systems must be capable of and configured to log the listed

event types. These requirements are based on the FedRAMP requirements and will allow for after-the-fact investigations of security incidents. Chorus Call is not a data system, however the company can provide this information based on their backend servers.

- Successful and unsuccessful account logon events
- Account management events
- Object access
- Policy change
- Privilege functions
- Process tracking
- System events

# Reporting Data Breaches/Incident Response

---

JBA maintains an annually updated incident response plan and provides annual training and tabletop exercises. All JDMHQ project staff will be trained annually to recognize data breaches within the project and report them to the team within one hour of the incident. Both the general JBA plan and the specific articulation of the plan within the JDMHQ project are designed to be in compliance with all FISMA and HHS reporting and monitoring requirements.

JBA's approach to incident response takes a strict stance in defining incidents as both any breach of the systems or breach of protocol. We treat all project data and products as sensitive due to their proprietary nature and do not limit security controls to PII. If a violation of any of the security controls for maintaining sensitive information occurs, JBA support staff will begin an assessment of the incident. Using risk-based analysis the assessors will determine which actions will be taken as a result of the incident, determine if there is evidence of harm, and determine if sensitive information is at risk of being compromised. If JBA support staff identify a risk to sensitive information they will notify senior staff immediately for escalation.

All reported violations will lead JBA to immediately notify the COR, and if PII is involved, the OPRE email box at [CyberICU@acf.hhs.gov](mailto:CyberICU@acf.hhs.gov) within one hour of reported violation. JBA will work with the COR to complete a HHS Computer Security Incident Response Center (CSIRC) incident report form that includes details of the risk, a description of the information that may be at risk, and a list of activities made during the assessment in accordance with HHS-OCIO-2008-0001.003 (November 17, 2008). JBA's complete Incident Response Plan is provided as an attachment.

# Training Procedures for Data Security

---

JBA staff members are required to have current certification in protection of human subjects and take a course on protecting PII approximately annually. The PII training covers the following topics:

1. Identifying PII
2. Reporting PII Breaches
3. Threats to PII including hackers, physical theft, employee mistakes, and mobile devices
4. Properly securing non-digital PII in the office and in the field
5. Properly accessing, transmitting, and storing of digital PII
6. Additional security requirements included in this security plan

JBA staff members are required to satisfactorily complete the training. JBA IT support staff maintain the training records for seven years. Before access to sensitive information is granted to a staff member, JBA IT Support staff review the training records to ensure that the required training has been completed.

JBA updates our Incident Response Plan annually. The Incident Response Plan is managed by our Incident Response Team, who carries out routine tabletop exercises to ensure preparedness for any real events. Training and tabletops are carried for individual projects as needed.

In addition, JBA staff members are required to read and pledge compliance with an assurance of confidentiality (i.e., Data Privacy Agreement). JBA staff sign and pledge compliance with our acceptable use policy.



# Data Disposition

---

Digital media involved with this project is to be returned to the JBA IT support staff for proper sanitization. This includes JBA Laptops. JBA support staff use a commercial product that meets the NIST 800-88 standards for sanitizing media. JBA Server hard drives are disposed of in accordance with NIST 800-88 standards. A standard wiping process is used between projects (empty sectors are overwritten) and wiping, degaussing, and physical destruction at end of life.

Non-digital media is to be turned into the JBA administration support staff where it will be shredded and disposed of in accordance with government requirements.

For information regarding the sanitation or destruction of media used by Microsoft SharePoint Online and OneDrive please see the Microsoft Office 365 SharePoint Online and OneDrive FedRAMP package. For media sanitization information pertaining to Qualtrics, please see the Qualtrics FedRAMP package. For media sanitization information pertaining to Dedoose, please see the Microsoft Azure FedRAMP package.

## Data Archive by JBA

JBA will create a project archive and save it to an encrypted hard drive. The project archive will include a copy of all desensitized data collected or created during the scope of the project, as well as key analysis and reporting documents. The encrypted hard drive will then be stored in a limited access locked cabinet in the JBA office located in Arlington, Virginia. The encrypted hard drive will be kept for three years post contract, in line with guidance from the project officer at the Administration for Children and Families, Office of Planning Research and Evaluation, after which the data will be purged in accordance with NIST guidelines. In addition to the internal archive, data will be prepared and transferred to a national archive as indicated below.

## Transfer to Data Archive

In accordance with the requirements of the contract, JBA will prepare copies of the data sets requested by OPRE for submission and transfer to the identified archive group, including National Data Archive on Child Abuse and Neglect, Inter-University Consortium for Political and Social Research, or the National Archives and Records Administration. In addition to the necessary data sets, data dictionaries and data use materials will be developed to aid future researchers in accessing and making use of the data. Data will be submitted in accordance with all requirements determined by the COR, best practices, and as outlined by the respective archive group. Once an

archive destination has been identified, a more detailed plan will be developed specific to that archive and all documentation will be specific to their requirements.

# Annual Data Security Report

---

Each year, in addition to annual updates to the DSP, an Annual Data Security Report (DSR) will be generated. The DSR will validate any updates to the DSP have been implemented, including changes to processes, personnel, compliance dates for security awareness training, and reports about data incidents that occurred during the reporting year and how they were remediated. Additionally, the DSR will describe changes and updates to the system environment (e.g., boundary changes, interconnections, data sharing/usage agreements, and Plans of Action and Milestones) and any changes or updates to data collection plans or approaches.

# Reasonable Efforts Findings Study (REFS) Information Sheet

IRB Approved at the  
Study Level

Dec 01, 2021

## What is the REFS?

The REFS is a research study to understand what factors influence judges' **reasonable efforts findings** and how reasonable efforts findings relate to **case outcomes**.

Factors we will examine include:

- Pre- and between hearing communication (e.g., depth of information in reports)
- Hearing quality components (e.g., depth of discussion and parent engagement)
- Case characteristics (e.g., age, race, and gender of child, presenting problems)
- Judicial characteristics (e.g., race and ethnicity of judge, years of experience, case assignment type)
- Timing and frequency of review hearings

The study will include observation of recorded court hearings, review of court case files, and surveys with judges.

### Research Team

This study is funded by the Office of Planning, Research, and Evaluation (OPRE) and the Children's Bureau and conducted by James Bell Associates, the American Bar Association Center on Children and the Law, and Co-Principal Investigators Drs. Alicia Summers and Sophie Gatowski.

# What are the research questions?

1. How are hearing quality components (e.g., discussion during the hearing, how judges engage parents), information provided to the court before the hearing, case characteristics, judicial characteristics, and timing of the initial hearing **related to judges' findings of reasonable efforts to prevent removal?**
2. How are the breadth and depth of information provided to the court, case characteristics, judicial characteristics, and frequency and timing of the review hearings **related to the judges' findings of reasonable efforts to achieve permanency at review hearings?**
3. How are judges' findings of reasonable efforts to prevent removal and the detail documented in findings related to **the likelihood of reunification?**
4. How are judges' findings of reasonable efforts and the detail documented in findings related to **the time for cases to achieve permanency?**
5. Is there evidence of bias in the language used in child welfare court cases?

# Who will participate?

We are inviting up to 4 CIPs and up to 8 judges to participate. The total sample will include 440 cases (55 cases from 8 judges each).

# What is required for your site to participate?

Our goal is to require minimal time and effort from you and your staff. Study sites will be asked to:

1. Identify 2 judges who:
  - Presided over child welfare cases in 2019
  - Work in jurisdictions with an ethnically diverse caseload
  - Mostly follow a one family, one judge model
  - Do not preside over cases in a problem-solving court model (e.g., family treatment drug court, mental health court or a "0-3" young children's court cases)
  - Are willing to complete a brief web survey about their demographics and judicial experience
  - Allow the study team to review 55 cases they closed in 2019 as part of the study sample.

2. Grant remote access to recordings of 55 initial hearings of cases closed in 2019 from each participating judge. For a total of 110 cases from your state.
3. Grant remote access to the associated court case file of the 110 initial hearings reviewed.

## How will your data be protected?

We are committed to protecting all data collected for the study. We will sign a data sharing agreement with each site that explains how data will be shared, stored, accessed, and disposed. Data will be stored and maintained in accordance with Administration for Children and Families and FISMA requirements. Data access will be password protected and restricted to the study team. All team members are trained on data security procedures and human subjects protections. Child welfare cases and judges will be given unique identifiers so that final datasets will not have any personally identifying information. All data will be analyzed and reported in the aggregate, so that no families, judges, or sites are identified.

## What is the timeline?

We want to collect data between March and June 2022. That means we'd like to get access to the data from sites by March 1, 2022.

## How can your state benefit?

This is one of the first research studies to explore reasonable efforts in depth. The information your CIP provides will contribute to a growing body of evidence about what works best in child welfare hearings. Findings from this study will be shared widely and used to inform practice, policy, and court improvement efforts. Additionally, we will give you an Excel file that includes all deidentified data collected from hearing observation and court case file review in your state. This will allow you to conduct your own analyses on the 110 closed cases sampled from your state.

## How can you learn more?

Contact Project Director Anne Fromknecht to learn more:

[Fromknecht@jbassoc.com](mailto:Fromknecht@jbassoc.com) 703-247-2631