1. Meeting Minutes

JISC DATA DISSEMINATION COMMITTEE
Friday August 26, 2016 (8:15 a.m. – 9:45 a.m.)
Administrative Office of the Courts
SeaTac Office Building
18000 International Blvd. Suite 1106, Conf Rm #2
SeaTac, WA 98188
Call-in Number: 1-877-820-7831, Passcode 797974

DRAFT - MEETING MINUTES

Members Present
Judge Thomas J. Wynne, Chair
Judge Jeannette Dalton
Judge J. Robert Leach
Judge G. Scott Marinella
Ms. Barbara Miner
Ms. Brooke Powell
Ms. Aimee Vance

Members Not Present
Judge David A. Svaren

Guests Present (telephonically)
Ms. Sonya Kraski, Snohomish Co. County Clerk
Mr. Mark Allen, Snohomish Co. Clerk's Office
Mr. Kevin Hurtado AIRS
Ms. Luu Nguyen, U of Cal, Berkeley
Ms. Gillian Slee, Harvard University

Staff Present
Stephanie Happold, Data Dissemination Administrator
Kathy Bowman, MSD Administrative Secretary
Keli Beck, Senior System Support Analyst
Charlotte Jensen, Court Business Information Coordinator
Michael Keeling, ISD Operations Manager
Lisa Lind, Business Process Engineer
Trina Wendel, Business Process Engineer
Paul Farrow, Tyler Technologies

1. Call to Order, Approval of Minutes

The August 26, 2016, JISC Data Dissemination Committee Meeting was called to order at 8:20 am by Judge Wynne. Judge Marinella moved to approve the Minutes of June 24, 2016, and Judge Dalton seconded. The minutes were unanimously approved as written.

Due to AOC Staff schedules, Judge Wynne called the review of the Data Dissemination Policy Draft next.

2. Review of Data Dissemination Policy Draft

Judge Wynne presented his proposed changes to Section III.G. Ms. Vance, Ms. Miner, Ms. Kraski and Mr. Allen all raised questions about how the changes to the policy, particularly Section III.G, would impact staff work and customer interaction within their offices, and about how confidential addresses could be protected. The Committee discussed various technical restraints between the case management systems and what can/should be driven by policy. Ms. Vance voiced concerns about prohibiting release of party addresses as it would hinder the

courts' ability to disseminate reports that are needed to efficiently conduct court business. This prohibition would exponentially increase staff counter time. She asked if exceptions could be made in the policy to allow address dissemination related to court work.

The Committee then discussed how addresses are entered into the case management systems. Questions were raised about the case source for addresses, and how a confidential address would display in JIS if the party was a defendant in a later criminal case. Committee members asked how addresses could be filtered between the case management systems and if they could be protected by case type. Mr. Farrow was asked to demonstrate how addresses are entered into the Odyssey case management system and then displayed. Mr. Farrow explained the Odyssey address screen and showed how addresses can be flagged as confidential. He also stated that if an Odyssey or Odyssey Portal user does not have certain access rights, the confidential address will not be seen.

Ms. Vance asked if there was a system-wide way to flag addresses by case type. Ms. Kraski responded that the cases of particular concern are not just confidential cases, but also those public cases with a confidential information form filled out. The document itself is confidential, but the information contained on it may possibly be entered into database to create the PER record. Committee members discussed how prior to Odyssey, documents were maintained in a separate database from the person case records. Now, documents and case management data are combined, creating difficulty. Also, once the address is added into the case management system, whether it is JIS or Odyssey, the source of the address (a confidential information form, DOL, etc.) is not linked to the information. Odyssey does provide the ability to add a source for the address, but there was confusion if source was case/court source or a code similar to the status code in the JIS ADH screen. Judge Leach asked what additional problems were created because of data transfers and/or new case data entries. Ms. Vance responded that because of not knowing the source of the address, problems would occur in both.

The Committee also discussed the relationship of the address of the person (defendant, victim, protected party) to the case type itself and that not all addresses are protected addresses.

Judge Leach asked how the systems handled data requests if multiple courts added different addresses for a party for various cases and if it could be controlled where those addresses came from, be displayed, or be disseminated. He asked if it was possible to display addresses only from non-confidential case types. Ms. Jensen explained that when running BOXI reports from JIS, the system pulls all records for the date, attaches names to it, and then the current address. The addresses would be used regardless of where it came from. The user could try to limit the addresses from confidential case types by filtering out by case types (removing adoption or juvenile dependency cases for instance.). However, if there is a protection order case and petitioner is a parent in a dependency case, the system would not report parents' name and address on dependency case, but the information would be in JIS for the protection order. Because the same party/person record is used, the report would have the name and address.

Ms. Kraski presented her concerns about allowing addresses to be displayed. Because of confidential addresses from public cases being displayed in Odyssey Portal during the Snohomish County Odyssey implementation, she had the AOC SC-CMS staff immediately shut down that access for Portal roles.

The Committee discussed splitting the policy to what can be viewed in the case management systems and what the courts could provide directly for a data dissemination request.

The Committee was concerned about making any decisions on the policy today, as not enough was known about the case management technology, how the systems interact with one another, and how addresses are entered into the systems. The Committee agreed that they should schedule an additional meeting specifically for this topic. DDA Happold will set up a meeting late September, early October for the Committee to discuss these issues further.

3. American Information Research Financial Data Request

Mr. Kevin Hurtado from American Information Research (AIRS) presented the request for an unlawful detainer report that would include financial data in judgement cases. However, after hearing the discussion about the draft data dissemination policy, Mr. Hurtado was concerned that the addresses would not be available in the system. DDA Happold had reported earlier to Mr. Hurtado that if there were any addresses associated with the case, they would belong to the parties and not the address where the unlawful detainer took place. However, respondent addresses would not even be available because the parties to unlawful detainers are not well identified parties and the addresses would not be in the system. There is a possibility that the address for a pro se would be in the system, but that was not assured either. DDA Happold advised that AIRS would need to research the address information by going to the individual county clerk's offices. Mr. Hurtado said without the address information, AIRS did not want the data. DDA Happold asked if it was beneficial to AIRS if AOC provide a list of unlawful detainer cases that AIRS could use to research the address information with the county clerk's offices. Mr. Hurtado responded that it was possible. DDA Happold suggested that Mr. Hurtado go through with requesting the financial data with the DDC just in case the list of unlawful detainer cases is helpful so he does not have to come back to the Committee. Mr. Hurtado agreed. DDA Happold asked the Committee for a motion to approve AIRS request for financial data, minus addresses. The motion was unanimously passed with the usual financial data request requirements that included the county clerk's office representative reviewing the reports for accuracy.

4. University of California – Berkeley Financial Data Request

Ms. Luu Nguyen presented University of California – Berkeley's request for debt collection cases including financial data. Ms. Miner asked if the request was for Superior Court and CLJ Court data; Ms. Nguyen confirmed it was for both.

It was discussed that causes of action are not always clear in the case management system and that there is no case type/specific cause code for debt collection. Debt collection could occur in numerous other causes of action and the docket coding would need to be used to draw out the information. It was asked and Ms. Nguyen confirmed that they are not looking for child support or maintenance. Judge Wynne called for a motion; Judge Svaren moved to approve the request, subject to usual requirements for financial data requests. Ms. Miner seconded and it was passed unanimously.

5. Harvard Financial Data Request

Ms. Slee presented the Harvard request for unlawful detainer case information, including financial data. Although they are looking at where evictions occur, they are prepared to do the additional research for address information as they understand it will not be available through AOC. Judge Leach made the motion to approve the request with the same requirements as previous financial data requests and Ms. Powell seconded it. The motion passed unanimously.

6. DCH Screen Recommendation Vote

DDA Happold updated the Committee on its July 22, 2016, decision to revise the DDC recommendation from removing the DCH screen from JIS to adding warning messages agreed upon by EDE Governance Committee as soon as possible. The Committee Members had held off voting on the recommendation change during the July meeting until more members were present. Ms. Vance moved and Judge Svaren seconded that the DDC revise its recommendation to AOC and the EDE Governance Committee from removing the DCH screen to instead adding warning messages, both temporary and permanent, to multiple JIS case compilation screens and reports as soon as possible. The motion passed unanimously.

7. Other Business

Dates of birth and addresses are still shut off for every Odyssey Portal Role. DDC will table this discussion for now.

Meeting adjourned 9:30 am.

WASHINGTON COURTS	**JISC DATA DISSEMINATION COMMITTEE** **Data Dissemination Policy Work Session** **Thursday, October 6, 2016 (1:00 p.m. – 3:00 p.m.)** **Administrative Office of the Courts** **SeaTac Office Building** **18000 International Blvd. Suite 1106, Conf Rm #2** **SeaTac, WA 98188** **Call-in Number: 1-877-820-7831, Passcode 797974**

DRAFT - MEETING MINUTES

Members Present	**AOC Staff Present**
Judge Thomas J. Wynne, Chair	Stephanie Happold, Data Dissemination Administrator
Judge J. Robert Leach	Keli Beck, Senior System Support Analyst
Judge G. Scott Marinella (telephonically)	Charlotte Jensen, Court Business Information Coordinator (telephonically)
Judge David A. Svaren (telephonically)	Michael Keeling, Operations Manager
Ms. Barbara Miner	Elaine McLaughlin, Court Records Access Coordinator
Ms. Brooke Powell	Dexter Mejia, Court Business Office Manager
Ms. Cynthia Marr, Pierce County District Court, appearing on behalf of Ms. Aimee Vance	Maribeth Sapinoso, SC-CMS Project Manager
	Trina Wendel, Business Process Engineer
Members Not Present	
Judge Jeannette Dalton	**Guests Present**
Ms. Aimee Vance	Ms. Sonya Kraski, Snohomish County Clerk
	Mr. Mark Allen, Snohomish County Clerk's Office
	Mr. Paul Farrow, Senior Project Manager Tyler Technologies
	Ms. Dena Marley, Snohomish County Clerk's Office

1. Call to Order, Purpose of Work Session:

The October 6, 2016, Data Dissemination Committee (DDC) work session was called to order at 1:00 pm by Committee Chair Judge Wynne.

Judge Wynne informed attendees the purpose of the work session was to come to a consensus regarding the following issues so the Data Dissemination Policy (DD Policy) could be completed:

- Understand how party addresses are entered and displayed in the case management systems; and
- How confidential address information is used in the JIS and Odyssey systems.

Ms. Miner inquired if the Confidential Information Form (CIF) would be discussed during the meeting as well. DDA Happold indicated the Law Enforcement Information (LEI) was one of the forms Judge Wynne asked her to provide for the meeting and that she also had an answer to Judge Wynne's question he posed to her before the meeting as to why there were two different CIF forms being used. She suggested she provide a summary of the documentation contained

in the work session binders prior to discussing individual documents so the Committee members knew what they had before them

2. Background from DDA Happold

Prior to the work session, Judge Wynne requested DDA Happold collect specific documentation and case screen shot examples from the different case management systems for the Committee members to review. He also requested that certain subject matter experts attend the meeting to answer any questions necessary to finalize proposed amendments to the current DD Policy.

DDA Happold commented that the decisions today needed to include not only JIS and Odyssey and how the data is displayed between the two systems, but also how the data is transferred into the AOC data warehouse and in BOXI reports that are also used by the courts.

3. Review of Binders

DDA Happold reviewed the contents of each binder tab, explaining why Judge Wynne asked for each item.

Tab 1. Draft DD Policy Amendments, with tracked changes.

Tab 2. Draft DD Policy Amendments, clean version.

Tab 3. JIS Person Business Rules for entry of addresses.

Tab 4. Examples of how addresses are entered into JIS. Includes PER and ADH screen shots.

Tab 5. Examples of how addresses are entered into Odyssey.

Tab 6. Examples of addresses used in case type 7s and tied to a PER record. Example is an individual with case types 7 and 8.

Tab 7. Example of Case Type 3 with WIP Minors.

Tab 8 Example of Sexual Assault Protection Order Case with Minor.

Tab 9 Example of Case with Offender and Victim are both Minors.

Tab 10 Law Enforcement Information form.

Tab 11 JIS Security for JIS LINK users.

Tab 12 Statutes and Court Rules.

4. Discussion

Ms. Miner inquired about Tab 10, Law Enforcement Information (LEI) form and its similarities to the Confidential Information Form (CIF) that was not included in the binder. Ms. Miner expressed concerns about courts using these forms interchangeably and asked why there were

no examples of the CIFs included. DDA Happold explained that Judge Wynne did not request for a copy of the CIF to be included, but instead asked her to answer the question of why there were two different CIFs being used by the courts. DDA Happold contacted Merrie Gough, the staff attorney for the Pattern Forms Committee, prior to the work session and asked about the two different CIFs. Ms. Gough conveyed that there was no reason for two different versions, that she would make the recommendation to the Pattern Forms Committee to use just one, and she thanked the DDC for bringing it to her attention.

The DDC continued to discuss how the LEA and CIF are filled out by parties during case initiation and are not meant to be entered into JIS. The LEI form includes two fields for Protected Parties to enter their address information: one for confidential address information and a separate box for non-confidential address information. The members discussed how this form should be a pass-through form and not kept in the court file.

Ms. Miner and Ms. Marley explained how the forms are used in their offices and that they do not enter any LEA or CIF information into JIS. Ms. Marr commented that there is some information on those forms that may be used by the courts while inputting the cases into JIS. Judge Leach noted both forms imply to the petitioner that the information will be confidential, therefore information from forms should not be entered into any system where it might be publicly viewable.

DDA Happold wanted to remind the group that as information passes between JIS and Odyssey and goes to the AOC data warehouse, there is no indicator or flag in place to differentiate whether addresses are marked public or confidential.

Ms. Kraski discussed how this is an issue as during her county's Odyssey implementation she was notified that confidential names, addresses, and birthdates that were in a public case type were being displayed in Odyssey Portal. After learning of this, Ms. Kraski notified the AOC SC-CMS team to immediately turn off all addresses and birthdates in Odyssey Portal to prevent the information being displayed.

DDA Happold then reviewed *Tab 3, the JIS Person Business Rules for Entry of Addresses (PBR)*, which provides additional detail regarding the Secretary of State's Confidential Program for Victims of Crimes. She highlighted a PBR requirement that:

> *'At no time should the word CONFIDENTIAL be added to the Name or Address Fields of the person record.'*

DDA Happold then reviewed *Tab 4, Examples of how addresses are entered into JIS - Includes PER and ADH screen shots.* The screens provided were training screens. She explained the status codes contained in the ADH screen, how they relate to the addresses entered into the system, and that the status code CA stands for Confidential Address when the Secretary of State (SOS) confidential address program is being used by the party. DDA Happold noted that JIS Link level 1 users do not have access to the ADH and the PER screens, and that Public Defenders have access to the ADH screen but not the PER screen. DDA Happold was not sure if the CA address is flagged at the data warehouse and suggested they ask Ms. Jensen when she is able to call into the meeting.

Ms. Marr stated Tab 4 was not an accurate example of the SOS Confidential Address as the screen shot showed a residential address and the SOS address is a Post Office Box. DDA

Happold agreed that the training data was not the most accurate example and that it should be a PO Box.

DDA Happold then presented tab 5 and how addresses are entered into Odyssey. Judge Leach asked if a box on the CIF is checked then how did the information become confidential. DDA Happold responded that the check box is not conveyed in JIS/Odyssey as those parties are well identified parties/persons and an address is needed to complete the person's case management information. Judge Leach expressed concern over the implied privacy in the current version of the CIF language.

DDA Happold then explained that the Status Code in JIS and the Source Code in Odyssey have the same function and illustrated the differences of how information is inputted into the two systems. She also pointed out that the Odyssey confidential address check box is only for the SOS address program per the PBRs and not for any other purpose. Ms. Kraski commented that this is not known by the clerks using Odyssey. Ms. Powell stated that Odyssey makes it easy to make this mistake and Ms. Marley agreed. Ms. Sapinoso indicated AOC educators are now aware of these issues and will update training materials and online manuals about how to use this screen.

DDA Happold also described how Odyssey address entries require another source code when the confidential address is checked, whereas JIS considers the CA a source code on its own. Mr. Keeling asked Mr. Farrow if there is a way the Odyssey field can be updated. Mr. Farrow said yes, but that it would cost the project in development hours.

DDA Happold stated that the AOC Person Maintenance Team reviews replication errors and then updates records to ensure JIS information is accurate, including address issues between the two systems. During this process JIS and Odyssey status and source codes are mirrored.

Judge Leach asked Mr. Farrow if the Odyssey DMS has the capability to differentiate whether an address originated from a specific case type, giving criminal or domestic violence cases as examples. Mr. Farrow said Odyssey can be configured that way, but Odyssey Portal cannot.

Judge Leach asked what is possible as far as specifying information as confidential. DDA Happold stated that JIS limits access internally by protecting some screens, but the data warehouse has no way to interpret or differentiate these confidential settings so information in the data warehouse can include confidential addresses.

Judge Leach asked DDA Happold how the expansion of JABS access to Law Enforcement Agencies might affect access to confidential information. DDA Happold indicated she would follow up and report back. Judge Leach also inquired who at the courts are granting access to JABS and questioned if anyone really knew who had this access. Ms. Miner asserted that AOC should be administering the access, not court staff which is the current process. Mr. Keeling indicated that AOC has the ability to run reports to show who currently has JABS access.

Ms. Jensen then joined the meeting telephonically. DDA Happold asked Ms. Jensen to elaborate on how the SOS address gets into the data warehouse. Ms. Jensen explained the address follows the person record that does not show the confidential residential address but the SOS PO Box. The same SOS PO Box information displays for each person in the program.

Ms. Miner indicated the SOS address shows in the PER screen, but the ADH has the SOS PO Box listed as well as all other addresses and asked how much protection does the SOS PO Box offer if all the other addresses are still listed.

The Committee Members asked what JIS LINK users had access to the ADH screen. DDA Happold responded that it was level 20 Public Defenders, Level 22 Law Enforcement, Level 25 Prosecutors, and Level 30 Non-JIS Courts. Committee members discussed whether or not public defenders should have access to the ADH screen if it lists all addresses as there is a possibility that public defenders may share this confidential information with their clients.

Ms. Miner asked why the PER history screen is confidential; DDA Happold answered that the screen displays personal identifiers.

The DDC members continued to discuss whether or not public defenders should have access to confidential information screens. Ms. Powell asked if it is realistic to find a way to filter the information with the current system(s) constraints. Judge Wynne and Judge Leach both agreed that the discussion should be moved toward an all or nothing alternative rather than trying to find a 'sweet spot' that is not currently attainable.

The concern was raised again that prohibiting all addresses from being disseminated would affect the county clerks and the court staff in completing their work. It was suggested that the addresses would be prohibited from dissemination unless a court order allowed for it. Ms. Miner responded that this did not satisfy the county clerks' needs and suggested changing the policy to state that exemptions are allowed for conducting court and county clerk business. Judge Leach also mentioned that the DDC would continue to allow address dissemination for research purposes.

The Committee then asked DDA Happold to go through the examples provided in Tabs 6-9. The tabs illustrated that even if an address is marked confidential in one scenario, if an individual is tied to other cases as a WIP it is not hard to piece together the individual's address from other cases or applications. Also the data warehouse has no way to limit the information.

Judge Wynne asked Mr. Keeling if it is possible to remove all addresses from the data warehouse. DDA Happold indicated that addresses are currently not disseminated in public bulk data requests and they provide at most the county. Judge Leach asked if the zip code could be provided instead and DDA Happold stated it could.

Judge Leach asked if the data warehouse can be structured to allow courts to have information, but block the information for everyone else. Mr. Keeling indicated AOC will be moving away from the data warehouse management structure and using the EDR in its place. Mr. Keeling went onto explain that JABS can be controlled by rules and that should not be a huge impact on the data warehouse. The courts would be responsible for adopting address dissemination practices after AOC makes system changes for all of this to be successful.

The Committee then discussed if the CIF could be sealed in Odyssey via a docket code so it would not display in Odyssey Portal. Tyler Technologies is working to use guidance from GR 22 as a driver for how information is displayed in Portal. DDA Happold asked if the term 'sealed' would be confusing to future users. Some DDC members thought the term 'restricted' was good. Mr. Mejia volunteered to take the verbiage discussion to the SC-CMS CUWG to discuss and settle upon a mutually agreeable term. Mr. Allen suggested using the CNRC code.

The Committee then discussed if a comment was needed in the proposed DD policy to mention that addresses are not disseminated due to technical limitations and cost.

The Committee also discussed what participants/parties should be added to the list in Section III.G.1. The Odyssey/JIS WIP is different than a civil person because of the three required

personal identifiers that includes an address; therefore any person that was considered a WIP would need to be added to the list. It was suggested that DDA Happold add a definition of a WIP in the DD policy to also cover any participant that was not mentioned in Section III.G.1. Ms. Miner and Ms. Kraski also mentioned victims eligible for restitution and asked that either the WIP definition be written to include them or they are added specifically to Section III.G.1.

The Committee also agreed on language for Sections III.G.4-6 that would allow for courts and county clerks to continue to dissemination addresses for their work without impediment.

Next, the Committee agreed that the ADH screen needs to be removed for the JIS-LINK level 20 Public Defender access. This will be voted on at the next DDC meeting.

DDA Happold asked if addresses and dates of birth can be turned back on in the Odyssey Portal for law enforcement and prosecutor roles. The Committee agreed that they should and would officially vote on it at the next meeting. Ms. Beck asked if that included confidential SOS addresses and the Committee confirmed that it did.

Judge Wynne asked DDA Happold to set up a meeting with Ms. Gough and the Chair of the Pattern Forms Committee to discuss the CIF confidential address check box.

Ms. Powell expressed concern over how the Confidential Address Box in Odyssey Client is being misused. Ms. Sapinoso indicated she would work with BPEs and trainers to make sure the Odyssey training materials clearly explain the purpose of the box. Ms. Powell asked if it would be possible to include a prompt or warning screen when the box is selected by the user. Mr. Farrow indicated that was a sizable request.

5. Conclusion

Judge Wynne indicated he would reach out to Ms. Vance to make sure her previous concerns about Section III.G.6 were properly addressed.

DDA Happold will notify the SC-CMS CUWG about the DDC decision to allow prosecutors and law enforcement agencies the ability to view addresses and dates of birth in the Odyssey Portal.

The DDC will vote to finalize the amended DD policy on October 28, 2016, and then bring the recommendation to the JISC. No changes, such as those proposed for the public defender access, will be made until the DD policy is implemented.

6. Meeting Adjourned

There is no other business, Judge Wynne adjourned this working meeting.

2. Washington State Attorney General Request

Robert W. Ferguson
ATTORNEY GENERAL OF WASHINGTON
Criminal Justice Division
800 Fifth Avenue • Suite 2000• MS TB 14 • Seattle WA 98104-3188
(206) 464-6430

October 4, 2016

Data Dissemination Committee
c/o Ms. Stephanie Happold
Administrative Office of the Courts
PO Box 41170
Olympia WA 98504
Stephanie.Happold@courts.wa.gov

RE:

Dear Members of the Data Dissemination Committee:

I am an Assistant Attorney General at the Washington State Attorney General's Office. Our office manages the Child Rescue Fund, pursuant to RCW 9.68A.200. Currently, the Fund is empty. The purpose for this request is to ascertain whether any fines have been imposed or collected and to help us anticipate potential future funds for purposes of distribution.

This request is for the data relating to:

(1) All charges filed for Possession of depictions of minor engaged in sexually explicit conduct (RCW 9.68A.070) from January 2014 to present, including the Court ID and the date the case was filed;

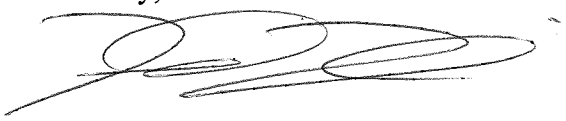
(2) All convictions for Possession of depictions of minor engaged in sexually explicit conduct (RCW 9.68A.070) from January 2014 to present, including the Court ID and the date the case was filed;

(3) All fines imposed under RCW 9.68A.107, which is a $1,000 fine for each count, during the time period of January 2014 to present. Include the Court ID and the date when the fine was imposed.

(4) The amount (if any) of these particular fines have been paid/collected. Include the Court ID and date when the fine was collected.

As previously mentioned, this is for internal accounting purposes for our financial division. If you have any further questions, please feel free to contact me for more details.

Sincerely,



FARSHAD M. TALEBI
Assistant Attorney General
WSBA No. 40461
Attorney for the State of Washington

cc: Ms. Stephanie Happold

3. Office of the Spokane Regional Criminal Justice Administrator Request

Spokane County
WASHINGTON

OFFICE OF THE SPOKANE REGIONAL CRIMINAL JUSTICE ADMINISTRATOR
Jacqueline van Wormer, Ph.D.

August 29, 2016

Ms. Callie T. Dietz
State Court Administrator
Washington State Administrative Office of the Courts
PO Box 41170
Olympia, WA 98504-1170

RE: Spokane Regional Risk/Needs/Responsivity System

Dear Administrator Dietz:

The City of Spokane and Spokane County are one of eleven selected sites participating in the MacArthur Foundation Safety and Justice Challenge. The purpose of this initiative is to safely reduce our local jail population, reduce our average length of stay for defendants, and to address racial and ethnic disparities in the criminal justice system. One of our main deliverables is to build a risk/needs/responsivity (RNR) system across pretrial (PTS), jail booking and county/city probation.

We are partnering with Dr. Zach Hamilton of Washington State University to assist us in developing a locally normed and validated RNR tool for our region. One of our first deliverables is to build the PTS tool in order for judicial officers to make informed release decisions from the bench. A necessary component of the PTS tool is access to current criminal history data in order to auto-populate the criminal history and warrant information on the tool.

I am writing to seek permission to access AOC criminal history and warrant data, on a daily basis, so that we can create a highly functional tool. Specifically, we would look to collect the following information:

Variable	Type	Description
CcrdCaseID	identifier, numeric and character, varied lengths	Combination of letters and numbers assigned to the case, to be used as an identifier
CcrdCourtLevel	categorical, single letter	The court where the case is tried (juvenile, district, municipal, or superior)
CcrdCaseType	categorical, 1-5 characters	Type of case (criminal, status offense, dependency, etc.)
CcrdOffenseDate	date, MMDDYYYY	Date offense occurred
CcrdCaseFileDate	date, MMDDYYYY	Date case was filed
CcrdAdjudicationDate	date, MMDDYYYY	Date adjudication occurred
CcrdDispositionCode	categorical, 3 letters	Type of disposition (conviction, deferral, diversion, dismissal, no action taken, etc)
CcrdLawDescription	categorical (barely), combination of words and numbers	Written description of the charges, but there are many variations of the same offense

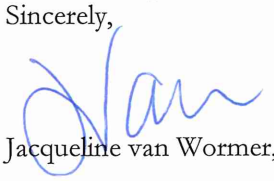
1116 W. BROADWAY AVE. • ADMINISTRATIVE SERVICES • SPOKANE WA. 99260
PHONE: (509) 477-5773 • EMAIL: JVANWORMER@SPOKANECOUNTY.ORG

CcrdLawSeverity	Numerical from -1 to 142	WSIPP law severity code, which includes scores from all offenses from non-criminal offenses to felony homicide
CcrdCountyText	categorical	The name of the county where the court action took place
sdk_cd	categorical, 1-6 letters	Docket data for identifying FTA cases in Superior Courts
CLJ warrant data		Docket data for identifying FTA cases in District Courts

We are hopeful that we can partner with AOC in order to make this important component of our tool operational. It will save thousands of hours of manual input in the tool if we are able to partner. We have tight timelines with our MacArthur project, and we are currently aiming for a mid-October launch of the PTS tool. Although the auto-population of the criminal history does not have to be in place when we launch, we would like to have auto-population in place before the end of the year.

I would be happy to set up a conference call to discuss this project further. Please advise as to the best next steps. I look forward to hearing from you. Thank you for your consideration.

Sincerely,



Jacqueline van Wormer, Ph.D.

1116 W. BROADWAY AVE. • ADMINISTRATIVE SERVICES • SPOKANE WA. 99260
PHONE: (509) 477-5773 • EMAIL: JVANWORMER@SPOKANECOUNTY.ORG

4. Data Dissemination Policy Draft

New edits since 6/24/16 meeting in yellow highlight.

Data Dissemination Policy

- AUTHORITY AND SCOPE
- DEFINITIONS
- ACCESS TO JIS LEGAL RECORDS
- JIS PRIVACY AND CONFIDENTIALITY POLICIES
- LIMITATION ON DISSEMINATION OF JUVENILE OFFENDER COURT RECORDS
- PROCEDURES
- ACCESS TO AND USE OF DATA BY COURTS
- ACCESS TO AND USE OF DATA BY CRIMINAL JUSTICE AGENCIES
- ACCESS TO AND USE OF DATA BY PUBLIC PURPOSE AGENCIES
- ~~E-MAIL~~
- VERSION HISTORY

I. AUTHORITY AND SCOPE

A. ~~These policies govern~~This policy governs the release of information ~~in~~ from the case management systems maintained by the Administrative Office of the Courts (AOC), such as the Judicial Information System (JIS), the Superior Court Management Information System (SCOMIS), the Appellate Court System (ACORDS) and Odyssey. It also includes data collected by AOC from other court case management systems~~.~~. The policy has been approved ~~and are promulgated~~ by the Judicial Information System Committee (JIS Committee), pursuant to JISCR 12 and JISCR 15(d)~~. They~~, and ~~apply~~ applies to all requests for computer-based court information subject to JISCR 15.

B. ~~These policies are to~~This policy is to be administered in the context of the requirement of Article I, § 10 of the Constitution of the State of Washington that "Justice in all cases shall be administered openly, and without unnecessary delay," as well as the privacy protections of Article I, § 7, and GR 31.

C. ~~These policies do~~This policy does not apply to requests initiated by or with the consent of the ~~Administrator for the Courts~~State Court Administrator or his/her ~~for~~designee for the purpose of answering a request vital to the internal business of the courts. See JISCR 15(a).

D. This policy does not apply to documents filed with the local courts and county clerk's offices.

II. DEFINITIONS

A. "JIS" is the acronym for "Judicial Information System" and as used in this policy represents all the case management systems that the AOC currently maintains.

New edits since 6/24/16 meeting in yellow highlight.

B. ~~Records~~ "JIS record" is an electronic representation of information stored within, or derived from the case management systems that the AOC maintains. It is programmed to be available in readable and retrievable form.

~~1. "**JIS record**" is an electronic representation (bits/bytes) of information either stored within, derived from, or accessed from the OAC. *(Amended February 27, 1998.)*~~

~~"**JIS legal record**" is a JIS record that is the electronic duplication of the journal of proceedings or other case-related information which it is the duty of the court clerk to keep, and which is programmed to be available in human readable and retrievable form. Case information reflecting the official legal file and displayed by JIS programs are JIS legal records.~~

C. JIS Reports

1. "**JIS ~~reports~~reports**" are the results of special programs written to retrieve and manipulate JIS records into a ~~human~~ readable form~~, other than the JIS legal record~~. It includes, but is not limited to, index reports, compiled aggregate numbers, and statistics.

~~2. "**Compiled reports**" are based on information related to more than one case or more than one court. As used in this policy, "compiled reports" do not include index reports.~~

~~3.~~2. **"Index reports"** are reports containing bulk court data with set data elements**.**

~~4.~~3. **"Compiled aggregate numbers"** are JIS reports containing only total numerical quantities without case level data elements.

~~5.~~4. **"Routine summary reports"** are JIS reports automatically generated by courts, county clerk's offices, or the AOC during the course of daily business.

D. Data Dissemination Management

1. "**Data dissemination**" is the reporting or other release of information derived from JIS records.
2. ~~The~~ "**~~data~~ Data dissemination ~~manager~~administrator**" is the individual designated within the ~~Office of the Administrator for~~Administrative Office of the Courts and within each individual court or county clerk's office, ~~and~~ that is assigned the responsibility ~~for~~ of administration of data dissemination, including responding to requests of the public, other governmental agencies, or other participants in the judicial information system. Courts and county clerk's offices may use multiple staff to satisfy this role.~~The name and title of the current data dissemination manager for each court and the Office of the Administrator for~~Administrative ~~the Courts shall be kept on file with the Office of the Administrator for the Courts.~~

New edits since 6/24/16 meeting in yellow highlight.

E. ~~Electronic~~ **Data Dissemination Contract**

The **"~~electronic~~ data dissemination contract"** is an agreement between ~~the~~ a county clerk's office, a Washington state court, or the ~~Office of the Administrator for~~Administrative Office of the Courts and any non-Washington state court entity~~, except a Washington State court (Supreme Court, court of appeals, superior court, district court, or municipal court), that is provided information~~for release of data contained in the JIS ~~in an electronic format~~. The data dissemination contract shall specify terms and conditions, as approved by the ~~Judicial Information System~~JIS Committee, concerning the data including but not limited to restrictions, obligations, and cost recovery ~~agreements~~fees. ~~Any such contract shall at a minimum include the language contained in Exhibit A – Electronic Data Dissemination Contract. *(Amended February 27, 1998.)*~~

F. Well Identified Person

"Well Identified Person" is defined for the purposes of this policy as an individual whose name and address are entered into the case management system with the possible addition of a date of birth, driver's license number, SID, or DOC number.

III. ACCESS TO JIS ~~LEGAL~~ RECORDS

~~**Open Records Policy**. The following principles apply to the interpretation of procedural rules or guidelines set forth in this policy.~~

A. Access to and release of JIS data will be consistent with Article I, § 10 of the Constitution of the State of Washington, GR 31 and Washington state statutes. Statutes, court rules, case law, and policy guidelines that protect individual privacy and confidential court records shall be adhered to when JIS records or JIS reports are disseminated. All access to JIS records and JIS reports is subject to the requirements of the criteria for release of data specified in JISCR 15(f): availability of data, specificity of the request, potential for infringement of personal privacy created by release of the information requested, and potential disruption to the internal ongoing business of the courts. JIS records or JIS reports provided in electronic format shall be subject to provisions contained in the data dissemination contract.~~Information related to the conduct of the courts' business, including statistical information and information related to the performance of courts and judicial officers, is to be disclosed as fully as resources will permit. In order to effectuate the policies protecting individual privacy which are incorporated in statutes, case law, and policy guidelines, direct downloading of the database is prohibited except for the index items identified in Section III.B.6. Such downloads shall be subject to conditions contained in the electronic data dissemination contract. *(Amended February 27, 1998.)*~~

New edits since 6/24/16 meeting in yellow highlight.

~~3. Dissemination of compiled reports on an individual, including information from more than one case, is to be limited to those items contained in a case index, as defined in Section III.B.6.~~

B. Privacy protections accorded by the United States Congress and by the Washington State Legislature to records held by other state agencies are to be applied to requests for ~~computerized information from court~~JIS records or JIS reports, unless such record is a "court record" as defined in GR 31 and access is controlled by GR 31(d) and GR 31(e). ~~admitted in the record of a judicial proceeding, or otherwise made a part of a file in such a proceeding, so that court computer records will not be used to circumvent such protections.~~

C. **Contact Lists**: ~~Access to JIS information will not be granted when to do so would have the effect of providing access to lists of individuals for commercial purposes, defined as set forth in RCW 42.17.260(6) and WAC 390-13-010, i.e., that in connection with access to a list of individuals, the person requesting the record intends that the list will be used to communicate with the individuals named in the record for the purpose of facilitating profit expecting activity.~~ The use of JIS records or JIS reports for the purpose of commercial solicitation of individuals named in the court records is prohibited. Requests for JIS data for this purpose will be denied.

~~6. Except to the extent that dissemination is restricted by Section IV.B, or is subject to provisions in the electronic data dissemination contract, electronic records representing court documents are to be made available on a case-by-case and court-by-court basis as fully as they are in hard copy form. *(Amended February 27, 1998.)*~~

~~All access to JIS information is subject to the requirements of the criteria for release of data specified in JISCR 15(f): availability of data, specificity of the request, potential for infringement of personal privacy created by release of the information requested, and potential disruption to the internal ongoing business of the courts. JIS information provided in electronic format shall be subject to provisions contained in the electronic data dissemination contract. *(Amended February 27, 1998.)*~~

D. Court and county clerk data dissemination ~~managers~~ administrators will restrict the dissemination of JIS reports to data related to the ~~manager's~~ administrator's particular court, or court operations subject to the supervision of that court~~, except where the court has access to JIS statewide indices~~. A court or county clerk may disseminate a report or data summarizing an individual's criminal history.

E. Courts and county clerk's offices may direct requestors to the Administrative Office of the Courts if the request falls under GR 31 (g)(2) and creates an undue burden on the court's or the county clerk's operations because of the amount of equipment, materials, staff time, computer time or other resources required to satisfy the request.

New edits since 6/24/16 meeting in yellow highlight.

F. Routine summary reports will be made available to the public upon request, subject to the payment of an established fee and so long as such request can be met without unduly disrupting the on-going business of the courts.

~~3. Access to JIS legal records, in the form of case specific records, will be permitted to the extent that such records in other forms are open to inspection by statute, case law and court rule, and unless restricted by the privacy and confidentiality policies below.~~

~~4. Individuals, personally or through their designees, may obtain access to compiled legal records pertaining to themselves upon written request, accompanied by a signed waiver of privacy.~~

~~5. No compiled reports will be disseminated containing information which permits a person, other than a judicial officer or an attorney engaged in the conduct of court business, to be identified as an individual, except that data dissemination managers may disseminate the following:~~

~~a. Public agency requested reports. Reports requested by public agencies which perform, as a principal function, activities directly related to the prosecution, adjudication, detention, or rehabilitation of criminal offenders, or to the investigation, adjudication, or enforcement of orders related to the violation of professional standards of conduct, specifically including criminal justice agencies certified to receive criminal history record information pursuant to RCW 10.97.030(5)(b).~~

~~b. Personal reports, on the request or signed waiver of the subject of the report.~~

~~c. On court order.~~

G. Index Report

1. An index report~~, containing some or all of the following information, may be disseminated: *(Amended February 27, 1998.)*~~ shall not contain confidential information as determined by Court Rules, Washington state law and Federal law. In addition, the following data is confidential information:

~~1~~a. ~~filing date;~~social security numbers;
~~2~~b. ~~case caption;~~financial account numbers;
~~3~~c. ~~party name and relationship to case (e.g., plaintiff, defendant);~~driver's license numbers;
~~4~~d. ~~cause of action or charge;~~dates of birth of a minor child;
~~5~~e. ~~case number or designation;~~ party addresses and telephone numbers;
~~6~~f. ~~case outcome;~~ witness and victim addresses and phone numbers;
~~7~~g. ~~disposition date.~~abstract driving records as defined in RCW 46.52.130; and
h. well identified person addresses and phone numbers.

New edits since 6/24/16 meeting in yellow highlight.

COMMENT

The JISC DD Policy adopted May 19, 1995 limited public access to JIS data to an index report. Address information was not a data element included in that index report. The DD Policy also prohibited public access to compiled reports. This policy predated the adoption of GR 31 and GR 22. Neither GR 15, GR 31 nor GR 22 provide for confidentiality of party addresses. A Confidential Information Form promulgated by the Pattern Forms Committee must be completed and provided to the Clerk upon filing a family law matter or domestic violence petition. The current version of the CIF, as of 11/1/2016, provides a block, which may be checked by a party providing: "the health, safety, or liberty of a party or child would be jeopardized by disclosure of address information because: ." No additional security is provided in the JIS system by a party checking this block. A reasonable expectation of privacy in the address information on the CIF is created by checking this block.

Neither the JIS system, nor Odyssey can differentiate the source of an address currently contained in the system.

2. No screen or report in a JIS system shall be made available for public dissemination if it contains confidential information, as defined in this section, notwithstanding any other provision of this policy.

~~*(III.B.6.f. and III.B.6.g. added December 5, 1997.)*~~

3. An index report provided in electronic format shall be subject to the provisions contained in the ~~electronic~~ data dissemination contract. *(Amended February 27, 1998.)*

~~A report sorted by case resolution and resolution type, giving index criteria except individual names, may be compiled and released. *(Section added June 21, 1996.)*~~

4. A local court or county clerk's office is not precluded by this policy from releasing, without redaction, a document or pleading containing a residential address, as this policy does not apply to documents filed with local courts or county clerk's offices.

5. A local court or county clerk's office is not precluded by this policy from providing the address of a party or well identified person to a state agency to meet requirements of law or court rules.

6. A local court or county clerk's office is not precluded from providing the address of a party or well identified person for the purpose of conducting the court's or the county clerk's business

New edits since 6/24/16 meeting in yellow highlight.

H. Financial Data.

1. Requests to courts or county clerk's offices will be handled by that individual office in the same manner as all other requests for court data.
2. Requests to the AOC for statewide financial court data or for an individual court's data will be handled in the following manner:
   a. Requestor will provide as much detail as possible regarding specific financial information requested. Explanations may include such information as specific codes, accounting or non-accounting needs, statewide aggregate, court aggregate or case-by-case data, and court levels.
   b. The AOC will review the request and submit any clarifications to the requestor. Communications may need to take place between the AOC staff and the requestor so the parties know what is being asked for and what can be provided. The time taken for clarifications and meetings will be in addition to any time estimates given for compiling the data. Further, the requestor will be charged for the staff time under the approved cost recovery fee for research/programming.
   c. Prior to release of the report, the data will be reviewed by delegated court and/or county clerk representatives for accuracy and completeness. Review period for representatives will be ten (10) days. Any disputes between AOC and the court/county clerk representatives regarding the data contained in the reports shall be resolved by the JISC Data Dissemination Committee.

IV. JIS PRIVACY AND CONFIDENTIALITY POLICIES

A. Information in JIS records which is sealed, exempted, or otherwise restricted by law, including ~~or~~ court rule, whether or not directly applicable to the courts, may not be released except by specific court order or by statutory authority.

B. Confidential information regarding individual litigants, witnesses, ~~or~~ jurors, or well identified persons that ~~has been collected for the internal administrative operations~~ is contained in case management systems of the courts will not be disseminated. ~~This information includes, but is not limited to, credit card and P.I.N. numbers, and social security numbers.~~ Identifying information (including, but not limited to, residential addresses and ~~residential~~ personal phone numbers) regarding individual litigants, witnesses, ~~or~~ jurors, or well identified persons will not be disseminated, except that the residential addresses of litigants will be available to the extent otherwise permitted by law, including court rule. *(Section amended September 20, 1996; June 26, 1998.)*

New edits since 6/24/16 meeting in yellow highlight.

C. A data dissemination ~~manager~~ administrator may provide data for a research report when the identification of specific individuals is ancillary to the purpose of the research, the data will not be sold or otherwise distributed to third parties, and the requester agrees to maintain the confidentiality required by these policies. In such instances, the requester shall complete a research agreement in a form prescribed by the ~~Office of the Administrator for~~ Administrative Office of the Courts. The research agreement shall: 1) require the requester to explain provisions for the secure protection of any data that is confidential, using physical locks, computer passwords and/or encryption; 2) prohibit the disclosure of data in any form which identifies an individual; 3) prohibit the copying or duplication of information or data provided other than for the stated research, evaluative, or statistical purpose. *(Amended June 6, 1997.)*

V. LIMITATION ON DISSEMINATION OF JUVENILE OFFENDER COURT RECORDS*

The dissemination of juvenile offender court records maintained in the Judicial Information System shall be limited as follows:

A. Juvenile offender court records shall be excluded from any bulk distribution of JIS records by the Administrative Office of the Courts otherwise authorized by GR 31(g), except for research purposes as permitted by statute or court rule.

B. The Administrative Office of the Courts shall not display any information from an official juvenile offender court record on a publicly-accessible website that is a statewide index of court cases.

* Juvenile offender court records shall remain publicly accessible on the JIS Link notwithstanding any provision of this section. *(Section added September 6, 2013.)*

Commented [HS1]: Shall we add extra language for future systems?
Example:

…on the JIS LINK or any JIS LINK replacement system other than those that distribute data in bulk,

VI. PROCEDURES

A. Uniform procedures for requesting JIS information, and for the appeal of decisions of data dissemination ~~managers~~administrators, shall be as set forth in policies issued by the ~~Office of the Administrator for the Courts~~Administrative Office of the Courts pursuant to JISCR 15(d).

B. In any case where a report is provided, the report must be accompanied by a suitable disclaimer noting that the court, the county clerk's office, and the Administrative Office of the Courts can make no representation regarding the identity of any persons whose names appear in the report, and ~~that the court makes~~can make no representation as to the accuracy and completeness of the data except for court purposes.

VII. ACCESS TO AND USE OF DATA BY COURTS

New edits since 6/24/16 meeting in yellow highlight.

The ~~Courts~~courts, the county clerk's offices, and their employees may access and use JIS records only for the purpose of conducting official court business. Such access and use shall be governed by appropriate security policies and procedures. Each year, all court staff, county clerk staff, and anyone receiving access from a court or a county clerk's office, including prosecutors and public defenders with access to JABS, will sign a confidentiality agreement by January 31. The courts and the county clerk's offices will then submit a Statement of Compliance to the AOC by March 31 confirming that their staff and any other users receiving access from their office have executed the agreements.

VIII. ACCESS TO AND USE OF DATA BY CRIMINAL JUSTICE AGENCIES AND BY THE WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

A. "Criminal justice agencies" as defined in ~~RCW Chapter~~ chapter 10.97 RCW shall have additional access to JIS records beyond that which is permitted the public.

B. The JIS Committee shall approve the access level and permitted use(s) for classes of criminal justice agencies including, but not limited to, law enforcement, prosecutors, and corrections. An agency that is not covered by a class may request access.

C. Agencies requesting access under this provision shall identify the information requested and the proposed use(s).

D. Access by criminal justice agencies shall be governed by a~~n electronic~~ data dissemination contract with each such agency. The contract shall:

1. Specify the data to which access is granted.
2. Specify the uses which the agency may make of the data.
3. Include the agency's agreement that its employees will access the data only for the uses specified.

E. The Washington State Attorney General's Office will be provided additional access to JIS records for those cases in which it represents the State.

IX. ACCESS TO AND USE OF DATA BY PUBLIC PURPOSE AGENCIES

A. "Public purpose agency" includes governmental agencies included in the definition of "agency" in RCW ~~42.17.020~~42.56.010 and other non-profit organizations whose principal function is to provide services to the public.

B. A public purpose agency may request court records not publicly accessible for scholarly, governmental, or research purposes where the identification of specific individuals is ancillary to the purpose of the request.

~~C. Upon approval by the JIS Committee, public purpose agencies may be granted additional access to JIS records beyond that which is permitted the public.~~

New edits since 6/24/16 meeting in yellow highlight.

~~D.~~C. Agencies requesting additional access under this provision shall identify the information requested and the proposed use(s). In reviewing such requests, the ~~JISC~~ courts, the county clerk's offices, and the JIS Committee will consider such criteria as:

1. The extent to which access will result in efficiencies in the operation of a court or courts.
2. The extent to which access will enable the fulfillment of a legislative mandate.
3. The extent to which access will result in efficiencies in other parts of the criminal justice system.
4. The risks created by permitting such access.

The courts, the county clerk's offices, and the JIS Committee must determine that fulfilling the request will not violate GR 31, and must determine the minimum access to restricted court records necessary for the purpose of the request.

~~E.~~D. Access by public purpose agencies shall be governed by ~~an electronic~~a data dissemination contract ~~with each such agency~~. The contract shall:

1. Require the requestor to specify provisions for the secure protection of any data that is confidential.

~~1.~~2. ~~Specify the data to which access is granted.~~Prohibit the disclosure of data in any form which identifies an individual.

~~2.~~3. ~~Specify the uses which the agency may make of the data~~Prohibit the copying, duplication, or dissemination of information or data provided other than for the stated purpose.

~~3.~~4. ~~Include the agency's agreement that its employees will access the data only for the uses specified~~Maintain a log of any distribution of court records which will be open and available for audit by the court, the county clerk's office or the AOC. Any audit should verify that the court records are being appropriately used and in a manner consistent with GR 31.

~~**X. E-MAIL**~~

~~The JIS provides e-mail for official court business use only. Access to judicial officers' and court employees' e-mail is restricted. Access to a judicial officer's e-mail files shall only be granted with the permission of the judicial officer involved. Request for access to a court employee's e-mail or to logs containing records on an employee's e-mail shall be subject to the review and approval of the county clerk if the employee is employed in the clerk's office, or the presiding judge or court administrator if the employee is employed by the court. Nothing in this policy shall be used as a reason to withhold records which are the subject of a subpoena or otherwise available to the public.~~

~~XI.~~X. VERSION HISTORY

New edits since 6/24/16 meeting in yellow highlight.

These policies shall take effect 30 days from the date of their adoption by the Judicial Information Systems Committee, May 19, 1995.

- Adopted May 19, 1995
- Amended June 21, 1996
- Amended September 20, 1996
- Amended June 6, 1997
- Amended December 5, 1997
- Amended February 27, 1998
- Amended June 26, 1998
- Amended September 6, 2013

New edits since 6/24/16 meeting in yellow highlight.

Data Dissemination Policy

- AUTHORITY AND SCOPE
- DEFINITIONS
- ACCESS TO JIS LEGAL RECORDS
- JIS PRIVACY AND CONFIDENTIALITY POLICIES
- LIMITATION ON DISSEMINATION OF JUVENILE OFFENDER COURT RECORDS
- PROCEDURES
- ACCESS TO AND USE OF DATA BY COURTS
- ACCESS TO AND USE OF DATA BY CRIMINAL JUSTICE AGENCIES
- ACCESS TO AND USE OF DATA BY PUBLIC PURPOSE AGENCIES
- VERSION HISTORY

I. AUTHORITY AND SCOPE

A. This policy governs the release of information from the case management systems maintained by the Administrative Office of the Courts (AOC), such as the Judicial Information System (JIS), the Superior Court Management Information System (SCOMIS), the Appellate Court System (ACORDS) and Odyssey. It also includes data collected by AOC from other court case management systems. The policy has been approved by the Judicial Information System Committee (JIS Committee), pursuant to JISCR 12 and JISCR 15(d), and applies to all requests for computer-based court information subject to JISCR 15.

B. This policy is to be administered in the context of the requirement of Article I, § 10 of the Constitution of the State of Washington that "Justice in all cases shall be administered openly, and without unnecessary delay," as well as the privacy protections of Article I, § 7, and GR 31.

C. This policy does not apply to requests initiated by or with the consent of the State Court Administrator or his/her designee for the purpose of answering a request vital to the internal business of the courts. See JISCR 15(a).

D. This policy does not apply to documents filed with the local courts and county clerk's offices.

II. DEFINITIONS

A. "JIS" is the acronym for "Judicial Information System" and as used in this policy represents all the case management systems that the AOC currently maintains.

New edits since 6/24/16 meeting in yellow highlight.

B. "JIS record" is an electronic representation of information stored within, or derived from the case management systems that the AOC maintains. It is programmed to be available in readable and retrievable form.

C. JIS Reports

1. "**JIS reports**" are the results of special programs written to retrieve and manipulate JIS records into a readable form. It includes, but is not limited to, index reports, compiled aggregate numbers, and statistics.
2. **"Index reports"** are reports containing bulk court data with set data elements**.**
3. **"Compiled aggregate numbers"** are JIS reports containing only total numerical quantities without case level data elements.
4. **"Routine summary reports"** are JIS reports automatically generated by courts, county clerk's offices, or the AOC during the course of daily business.

D. Data Dissemination Management

1. "**Data dissemination**" is the reporting or other release of information derived from JIS records.
2. "**Data dissemination administrator**" is the individual designated within the Administrative Office of the Courts and within each individual court or county clerk's office that is assigned the responsibility of administration of data dissemination, including responding to requests of the public, other governmental agencies, or other participants in the judicial information system. Courts and county clerk's offices may use multiple staff to satisfy this role.

E. **Data Dissemination Contract**
The **"data dissemination contract"** is an agreement between a county clerk's office, a Washington state court, or the Administrative Office of the Courts and any non-Washington state court entity for release of data contained in the JIS. The data dissemination contract shall specify terms and conditions, as approved by the JIS Committee, concerning the data including but not limited to restrictions, obligations, and cost recovery fees.

F. Well Identified Person
"Well Identified Person" is defined for the purposes of this policy as an individual whose name and address are entered into the case management system with the possible addition of a date of birth, driver's license number, SID, or DOC number.

New edits since 6/24/16 meeting in yellow highlight.

III. ACCESS TO JIS RECORDS

A. Access to and release of JIS data will be consistent with Article I, § 10 of the Constitution of the State of Washington, GR 31 and Washington state statutes. Statutes, court rules, case law, and policy guidelines that protect individual privacy and confidential court records shall be adhered to when JIS records or JIS reports are disseminated. All access to JIS records and JIS reports is subject to the requirements of the criteria for release of data specified in JISCR 15(f): availability of data, specificity of the request, potential for infringement of personal privacy created by release of the information requested, and potential disruption to the internal ongoing business of the courts. JIS records or JIS reports provided in electronic format shall be subject to provisions contained in the data dissemination contract.

B. Privacy protections accorded by the United States Congress and by the Washington State Legislature to records held by other state agencies are to be applied to requests for JIS records or JIS reports, unless such record is a "court record" as defined in GR 31 and access is controlled by GR 31(d) and GR 31(e).

C. **Contact Lists**: The use of JIS records or JIS reports for the purpose of commercial solicitation of individuals named in the court records is prohibited. Requests for JIS data for this purpose will be denied.

D. Court and county clerk data dissemination administrators will restrict the dissemination of JIS reports to data related to the administrator's particular court, or court operations subject to the supervision of that court. A court or county clerk may disseminate a report or data summarizing an individual's criminal history.

E. Courts and county clerk's offices may direct requestors to the Administrative Office of the Courts if the request falls under GR 31 (g)(2) and creates an undue burden on the court's or the county clerk's operations because of the amount of equipment, materials, staff time, computer time or other resources required to satisfy the request.

F. Routine summary reports will be made available to the public upon request, subject to the payment of an established fee and so long as such request can be met without unduly disrupting the on-going business of the courts.

G. Index Report

1. An index report shall not contain confidential information as determined by Court Rules, Washington state law and Federal law. In addition, the following data is confidential information:

    a. social security numbers;
    b. financial account numbers;
    c. driver's license numbers;

New edits since 6/24/16 meeting in yellow highlight.

d. dates of birth of a minor child;
e. party addresses and telephone numbers;
f. witness and victim addresses and phone numbers;
g. abstract driving records as defined in RCW 46.52.130; and
h. well identified person addresses and phone numbers.

COMMENT

The JISC DD Policy adopted May 19, 1995 limited public access to JIS data to an index report. Address information was not a data element included in that index report. The DD Policy also prohibited public access to compiled reports. This policy predated the adoption of GR 31 and GR 22. Neither GR 15, GR 31 nor GR 22 provide for confidentiality of party addresses. A Confidential Information Form promulgated by the Pattern Forms Committee must be completed and provided to the Clerk upon filing a family law matter or domestic violence petition. The current version of the CIF, as of 11/1/2016, provides a block, which may be checked by a party providing: "the health, safety, or liberty of a party or child would be jeopardized by disclosure of address information because:_____." No additional security is provided in the JIS system by a party checking this block. A reasonable expectation of privacy in the address information on the CIF is created by checking this block.

Neither the JIS system, nor Odyssey can differentiate the source of an address currently contained in the system.

2. No screen or report in a JIS system shall be made available for public dissemination if it contains confidential information, as defined in this section, notwithstanding any other provision of this policy.

3. An index report provided in electronic format shall be subject to the provisions contained in the data dissemination contract. *(Amended February 27, 1998.)*

4. A local court or county clerk's office is not precluded by this policy from releasing, without redaction, a document or pleading containing a residential address, as this policy does not apply to documents filed with local courts or county clerk's offices.

5. A local court or county clerk's office is not precluded by this policy from providing the address of a party or well identified person to a state agency to meet requirements of law or court rules.

6. A local court or county clerk's office is not precluded from providing the address of a party or well identified person for the purpose of conducting the court's or the county clerk's business.

H. Financial Data.

1. Requests to courts or county clerk's offices will be handled by that individual office in the same manner as all other requests for court data.
2. Requests to the AOC for statewide financial court data or for an individual court's data will be handled in the following manner:
   a. Requestor will provide as much detail as possible regarding specific financial information requested. Explanations may include such information as specific codes, accounting or non-accounting needs, statewide aggregate, court aggregate or case-by-case data, and court levels.
   b. The AOC will review the request and submit any clarifications to the requestor. Communications may need to take place between the AOC staff and the requestor so the parties know what is being asked for and what can be provided. The time taken for clarifications and meetings will be in addition to any time estimates given for compiling the data. Further, the requestor will be charged for the staff time under the approved cost recovery fee for research/programming.
   c. Prior to release of the report, the data will be reviewed by delegated court and/or county clerk representatives for accuracy and completeness. Review period for representatives will be ten (10) days. Any disputes between AOC and the court/county clerk representatives regarding the data contained in the reports shall be resolved by the JISC Data Dissemination Committee.

IV. JIS PRIVACY AND CONFIDENTIALITY POLICIES

A. Information in JIS records which is sealed, exempted, or otherwise restricted by law, including court rule, whether or not directly applicable to the courts, may not be released except by specific court order or by statutory authority.

B. Confidential information regarding individual litigants, witnesses, jurors, or well identified persons that is contained in case management systems of the courts will not be disseminated. Identifying information (including, but not limited to, residential addresses and personal phone numbers) regarding individual litigants, witnesses, jurors, or well identified persons will not be disseminated, except that the residential addresses of litigants will be available to the extent otherwise permitted by law, including court rule. *(Section amended September 20, 1996; June 26, 1998.)*

C. A data dissemination administrator may provide data for a research report when the identification of specific individuals is ancillary to the purpose of the research, the data will not be sold or otherwise distributed to third parties, and the requester agrees to maintain the confidentiality required by these policies. In such instances, the requester shall complete a research agreement in a form prescribed by the

Administrative Office of the Courts. The research agreement shall: 1) require the requester to explain provisions for the secure protection of any data that is confidential, using physical locks, computer passwords and/or encryption; 2) prohibit the disclosure of data in any form which identifies an individual; 3) prohibit the copying or duplication of information or data provided other than for the stated research, evaluative, or statistical purpose. *(Amended June 6, 1997.)*

V. LIMITATION ON DISSEMINATION OF JUVENILE OFFENDER COURT RECORDS*

The dissemination of juvenile offender court records maintained in the Judicial Information System shall be limited as follows:

A. Juvenile offender court records shall be excluded from any bulk distribution of JIS records by the Administrative Office of the Courts otherwise authorized by GR 31(g), except for research purposes as permitted by statute or court rule.

B. The Administrative Office of the Courts shall not display any information from an official juvenile offender court record on a publicly-accessible website that is a statewide index of court cases.

* Juvenile offender court records shall remain publicly accessible on the JIS Link notwithstanding any provision of this section. *(Section added September 6, 2013.)*

VI. PROCEDURES

A. Uniform procedures for requesting JIS information, and for the appeal of decisions of data dissemination administrators, shall be as set forth in policies issued by the Administrative Office of the Courts pursuant to JISCR 15(d).

B. In any case where a report is provided, the report must be accompanied by a suitable disclaimer noting that the court, the county clerk's office, and the Administrative Office of the Courts can make no representation regarding the identity of any persons whose names appear in the report, and can make no representation as to the accuracy and completeness of the data except for court purposes.

VII. ACCESS TO AND USE OF DATA BY COURTS

The courts, the county clerk's offices, and their employees may access and use JIS records only for the purpose of conducting official court business. Such access and use shall be governed by appropriate security policies and procedures. Each year, all court staff, county clerk staff, and anyone receiving access from a court or a county clerk's office, including prosecutors and public defenders with access to JABS, will sign a confidentiality agreement by January 31. The courts and the county clerk's offices will

then submit a Statement of Compliance to the AOC by March 31 confirming that their staff and any other users receiving access from their office have executed the agreements.

VIII. ACCESS TO AND USE OF DATA BY CRIMINAL JUSTICE AGENCIES AND BY THE WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

A. "Criminal justice agencies" as defined in chapter 10.97 RCW shall have additional access to JIS records beyond that which is permitted the public.

B. The JIS Committee shall approve the access level and permitted use(s) for classes of criminal justice agencies including, but not limited to, law enforcement, prosecutors, and corrections. An agency that is not covered by a class may request access.

C. Agencies requesting access under this provision shall identify the information requested and the proposed use(s).

D. Access by criminal justice agencies shall be governed by a data dissemination contract with each such agency. The contract shall:

1. Specify the data to which access is granted.
2. Specify the uses which the agency may make of the data.
3. Include the agency's agreement that its employees will access the data only for the uses specified.

E. The Washington State Attorney General's Office will be provided additional access to JIS records for those cases in which it represents the State.

IX. ACCESS TO AND USE OF DATA BY PUBLIC PURPOSE AGENCIES

A. "Public purpose agency" includes governmental agencies included in the definition of "agency" in RCW 42.56.010 and other non-profit organizations whose principal function is to provide services to the public.

B. A public purpose agency may request court records not publicly accessible for scholarly, governmental, or research purposes where the identification of specific individuals is ancillary to the purpose of the request.

C. Agencies requesting additional access under this provision shall identify the information requested and the proposed use(s). In reviewing such requests, the courts, the county clerk's offices, and the JIS Committee will consider such criteria as:

1. The extent to which access will result in efficiencies in the operation of a court or courts.

2. The extent to which access will enable the fulfillment of a legislative mandate.
3. The extent to which access will result in efficiencies in other parts of the criminal justice system.
4. The risks created by permitting such access.

The courts, the county clerk's offices, and the JIS Committee must determine that fulfilling the request will not violate GR 31, and must determine the minimum access to restricted court records necessary for the purpose of the request.

D. Access by public purpose agencies shall be governed by a data dissemination contract. The contract shall:

1. Require the requestor to specify provisions for the secure protection of any data that is confidential.
2. Prohibit the disclosure of data in any form which identifies an individual.
3. Prohibit the copying, duplication, or dissemination of information or data provided other than for the stated purpose.
4. Maintain a log of any distribution of court records which will be open and available for audit by the court, the county clerk's office or the AOC. Any audit should verify that the court records are being appropriately used and in a manner consistent with GR 31.

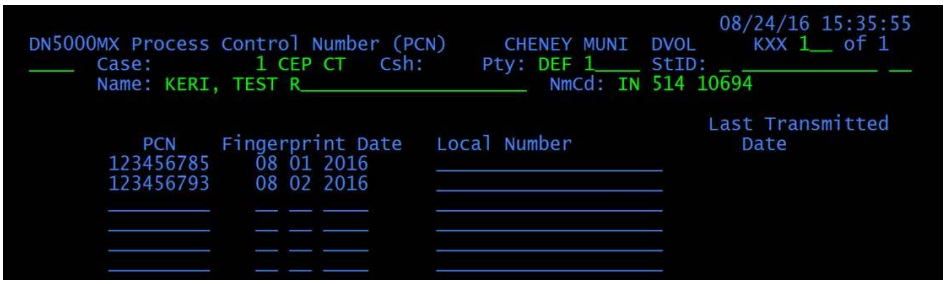
X. VERSION HISTORY

These policies shall take effect 30 days from the date of their adoption by the Judicial Information Systems Committee, May 19, 1995.

- Adopted May 19, 1995
- Amended June 21, 1996
- Amended September 20, 1996
- Amended June 6, 1997
- Amended December 5, 1997
- Amended February 27, 1998
- Amended June 26, 1998
- Amended September 6, 2013

5. PCN View Only Screen Access

Proposed PCN Screen for JIS LINK Users



Current PCN Screen for JIS Court Users

(with redactions)