WASHINGTON STATE STATISTICAL ANALYSIS CENTER

Criminal Justice Research & Statistics Center

Informing a data-driven justice system

The Justice Data Warehouse (JDW): Data Governance and Data Security

Vasiliki Georgoulas-Sherry, Ph.D. & Hanna Hernandez, M.A.

Contents

About the CJRSC – the Washington SAC 4

Abstract 5

Background 5

- Cross-Sector Data Linkage and Identity Resolution 5
- Data Governance in Criminal Justice Data Systems 6
- Data Security in Criminal Justice Data Systems 6
- The Justice Data Warehouse 6

JDW Core Data Contributors 7

Data Governance Overview 8

- Data Movement Process Map 8
- Data Access 8
- Data Minimization 8
- Data Privacy and Confidentiality 9
- Data Destruction 9
- Data Flow Process 9

Data Sharing Requirements 10

- Data Confidentiality and Non-Disclosure Agreements 10
- Data Use Restrictions 10
- Data Security Requirements 10
- Data Retention and Destruction Requirements 10
- Data Destruction Methods 10

Data Security Overview 11

- Security 11
- Minimization/Purpose Driven 11
- Transparency 11
- Accountability 11
- Value Driven 11
- Culture Driven 11
- Due Diligence/Lawful Use 11

Privacy Principles and Considerations 12

Lawful, Fair, and Responsible Use 12
Data Minimization 12
Small Number Standards 12
Transparency and Accountability 12
Due Diligence 12
Security 12
OCIO Data Categories 13

To accommodate people with disabilities, this document is available in alternate formats by calling the Office of Financial Management at 360-902-0555.

About the CJRSC – the Washington SAC

SACs are found across the nation in 51 states and territories. As the Washington SAC, the CJRSC is responsible for collecting, analyzing, and reporting public safety and criminal justice related statistics to federal, state, and local levels of government. We also facilitate the sharing of state-level information nationally. The information produced by SACs and their involvement in criminal justice projects is critical to local, state, and federal criminal justice agencies and community organizations as they develop programs and policies related to crime, illegal drugs, victim services, and the administration of justice.

SACs play a vital role in developing criminal and juvenile justice policy at the state and local levels. Their research provides evidence that policymakers use to guide their decision-making. By furthering the use of evidence-based practices in their states, SACs promote the effective and efficient administration of criminal and juvenile justice.

Contact Us

Phone	Fax	Address	Website
360-902-0599	360-586-1988	P.O. Box 43113 Olympia, WA 98504-3113	sac.ofm.wa.gov

Acknowledgements

This CJRSC – the Washington SAC would not be possible without the help and support of the Department of Justice (DOJ)'s Bureau of Justice Statistics (BJS)' State Justice Statistics (SJS) grant.

Version History

Date	Version	Author(s)	Revision Note
05/12/2026	1.0	Vasiliki Georgoulas-Sherry, PhD	Document creation

Abstract

Washington state's criminal justice system has long operated in disconnected silos across federal, state, and local levels, limiting the ability to assess performance, address disparities, and improve outcomes.

To respond to these impacts, the Criminal Justice Research and Statistics Center (CJRSC)-Washington Statistical Analysis Center (WA SAC) applied for and received the 2023 State Justice Statistics (SJS) grant from the Bureau of Justice Statistics (BJS). To address these challenges, the SAC, in partnership with the Public Safety Policy and Research Center (PSPRC), established the Justice Data Warehouse (JDW). This integrated platform links data from courts, jails, prisons, community supervision, and related systems, offering a comprehensive, longitudinal view of individuals' justice system involvement. As the JDW has evolved, strong data governance has become central to its mission.

This document describes the data governance structure and the data security for the JDW. Through rigorous governance and review procedures, the JDW mitigates the adverse effects of poor data quality, promotes responsible and secure data management, enhances transparency, and supports data-driven policy and cross-sector collaboration. By centralizing justice data while safeguarding privacy and supporting state and local jurisdictions, the JDW plays a pivotal role in building a fairer and more accountable justice system.

Background

Criminal justice systems historically developed as fragmented entities operating within agency-specific silos (court systems, law enforcement, corrections, and community supervision). This structural fragmentation has limited researchers' and policymakers' ability to conduct longitudinal analyses, assess system performance, measure disparities, and evaluate policy outcomes. Integrated justice data systems like the JDW emerged in response to these limitations, enabling cross-agency data linkage to support evidence-based decision-making.

To strengthen research and policy analysis, the BJS has supported SJS programs — like the CJRSC-WA SAC — to facilitate statewide data integration across multiple justice agencies, enhance statewide research capacity, and improve multi-jurisdictional data integration. These initiatives recognize that comprehensive justice reform depends on linking data across arrest, adjudication, sentencing, incarceration, and reentry systems. Integrated systems allow for examination of recidivism, sentencing disparities, jail utilization, and cross-sector service needs. By providing a unified view of justice system interactions, these programs help identify gaps in services and inform evidence-based policy decisions.

Research on justice system modernization emphasizes that integrated data infrastructures enhance transparency, accountability, and policy responsiveness. However, integration also introduces heightened risks related to privacy, confidentiality, and governance, particularly when personally identifiable information (PII) is involved. To balance the benefits of integration with these risks, robust governance and security frameworks are essential for ensuring that justice data are used responsibly and safely. Through robust governance and security, the JDW centralizes justice data to ensure privacy, improve data quality, and support transparent, evidence-based policy across Washington state.

Cross-Sector Data Linkage and Identity Resolution

The technical backbone of integrated data systems like the JDW relies on data standardization, extract-transform-load (ETL) processes, and master data management (MDM) frameworks. Identity resolution — the process of accurately linking records belonging to the same individual across disparate systems — is central to longitudinal justice analysis. Probabilistic matching, blocking techniques, and cardinality analysis are widely recognized methods for improving match precision while reducing false positives. MDM environments, such as those used in large-scale government repositories, assign unique person identifiers following tokenization and de-duplication procedures. These techniques reduce redundancy, improve analytic accuracy, and support data minimization principles by separating analytic identifiers from direct identifiers. Yet scholars caution that the linkage of records can amplify privacy risks if governance frameworks are not rigorously

implemented. Even de-identified datasets may be vulnerable to re-identification. Therefore, identity resolution processes must be paired with strong legal and administrative oversight.

Data Governance in Criminal Justice Data Systems

Data governance encompasses the policies, roles, standards, and accountability structures that regulate how data are collected, stored, accessed, shared, and destroyed. In public-sector justice environments, governance frameworks must balance competing priorities, including transparency, research utility, and public accountability. Effective governance structures include clearly defined data-sharing agreements (DSAs), formalized access approval processes, institutional review boards, and defined retention and destruction standards. The JDW's structured DSAs and contributor approval processes exemplify these best practices, incorporating audit rights, confidentiality, and access restrictions based on data sensitivity.

In criminal justice systems, robust governance is particularly critical given the sensitivity of personally identifiable information and the potential consequences of misuse. Data governance in this context ensures that multi-agency integration supports evidence-based decision-making while protecting individuals' rights. Well-defined governance frameworks facilitate interagency collaboration, establish accountability for data handling, and provide clear protocols for access, analysis, and reporting. By implementing these structures, criminal justice agencies can safely leverage integrated data to assess system performance, identify disparities, and guide policy reforms without compromising confidentiality or public trust.

Data Security in Criminal Justice Data Systems

Integrated justice systems operate under complex federal and state confidentiality and records protection laws. Security measures — including encryption, role-based access, audit logging, and secure data destruction — are reinforced by state-level data classification frameworks, such as those used by Washington's Office of the Chief Information Officer (OCIO), which tier data by sensitivity for proportional protection and compliance. Compliance is further supported through formal policies; training; ongoing monitoring; layered technical, and physical safeguards; and regular audits. These measures collectively ensure the confidentiality and integrity of justice data while enabling secure multi-agency data sharing.

In the criminal justice context, robust data security is critical given the sensitive nature of personally identifiable information, case details, and behavioral health records. Properly implemented frameworks protect individual privacy, maintain public trust, and support evidence-based decision-making. By applying tiered access, encryption, audit logging, and strict retention policies, agencies can safely integrate data to analyze and guide policy reforms without compromising confidentiality or violating statutory requirements.

The Justice Data Warehouse

Washington's criminal justice system, like those across the nation, has historically operated in silos, with state and local agencies maintaining separate, fragmented data systems. This structural separation limits the ability to evaluate system performance, measure outcomes, or understand how decisions at one stage — such as arrest, adjudication, or incarceration — affect later stages. To address these challenges, the JDW was created to integrate disparate criminal justice databases, enabling a holistic, longitudinal view of system involvement. By linking data across agencies and jurisdictions, the JDW allows policymakers and researchers to track individuals from arrest through court proceedings, incarceration, and community supervision, identifying bottlenecks, disparities, and opportunities for intervention.

Cross-sector research and analysis supported by the JDW allows for proactive, data-driven strategies to reduce justice involvement and improve outcomes. By integrating arrest records, court filings, incarceration data, and recidivism trends, agencies can identify systemic gaps, high-risk populations, and effective intervention points. This approach supports alternatives to incarceration, reentry supports, and preventive strategies. The JDW fosters a comprehensive and equitable accountable justice system by combining rigorous data analysis with cross-sector collaboration to promote public safety and community well-being.

JDW Core Data Contributors

Several organizations contribute data to the JDW. The PSPRC signs a data sharing agreement with each agency that outlines several components, including but not limited to the purpose of sharing data with the PSPRC, data access, security, and disposition, as well as language regarding redisclosures.

Currently, the JDW houses data from the Washington State Patrol (WSP), Washington State Department of Corrections (DOC), Administrative Office of the Courts (AOC), Caseload Forecast Council (CFC), and Washington Association of Sheriffs and Police Chiefs (WASPC).

The JDW is implemented via a grant through the Department of Justice's Bureau of Justice Statistics' State Justice Statistics (SJS) Program.

Data Governance Overview

Data Governance and Data Security are two interconnected, yet distinct programs that ensure the privacy and safekeeping of data that enters and leaves the JDW. Data governance is the framework that defines how the data is managed, ensuring it is accurate, consistent, and used responsibly. Data security focuses on protecting that data from unauthorized access, breaches, or loss through tools like encryption and access controls.

Data Governance for the PSPRC is documented through:

1. **Business and Technical Processes –** The PSPRC business processes ensure compliance with regulatory requirements in state and federal policies. They also ensure compliance within the various data sharing agreements and data requests in which the PSPRC engages, in terms of proper access, use, and storage of data. Technical processes are followed to ensure accurate, timely, and pertinent data analysis to help maintain limited access and the safe exchange of data with contributors and requestors.
2. **People Roles –** Our governance ensures that staff meet professional standards for privacy and data use, that we involve our data contributors, and that we maintain trusting relationships with informed data requestors.

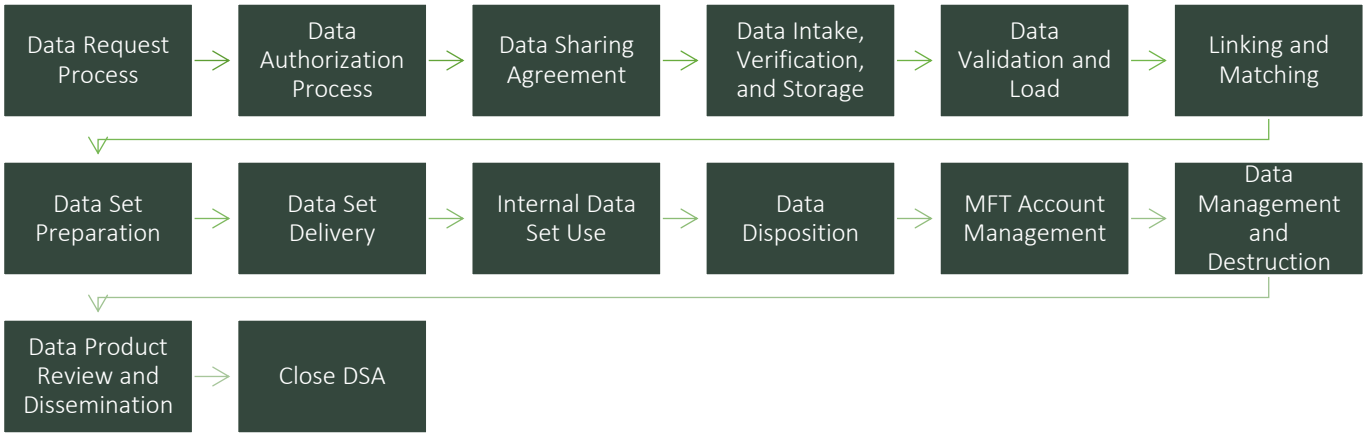
Data Security for the PSPRC is documented through:

1. **Business and Technical Processes –** Our business processes are designed to ensure the security of data as it moves from the PSPRC partners to the PSPRC, as it resides within the PSPRC repository, and as it moves on to data requestors. This includes safeguards to protect PSPRC's physical and electronic data assets from unauthorized access or misuse.
2. **People Roles –** The PSPRC staff and contractors who access and/or work with the data, the system, or both in a research or technical capacity operate in a manner that precludes inappropriate data access.

Data Movement Process Map

The PSPRC's business processes are performed with the goal of providing data products to requestors and maintaining and safeguarding data within the repository. Figure 1 describes the data governance processes.

FIGURE 1: DATA GOVERNANCE AND DATA MOVEMENT PROCESS MAP



Data Access

Data access to the JDW is limited to analysts and researchers following approval from data contributors and the Washington State Institutional Review Board (WSIRB).

Data Minimization

Data minimization ensures that only relevant data is collected and shared, aligning with policies that promote responsible data use. This reduces the risk of unauthorized access, improves data quality, and supports compliance with legal and ethical standards.

Data Privacy and Confidentiality

Data supplied to requestors from the JDW repository is limited to de-identified data. Personally identifiable information (PII) will not be shared. The JDW protects individual data contained in the repository from unauthorized access, misuse, or disclosure and ensures compliance with legal and ethical standards.

Data Destruction

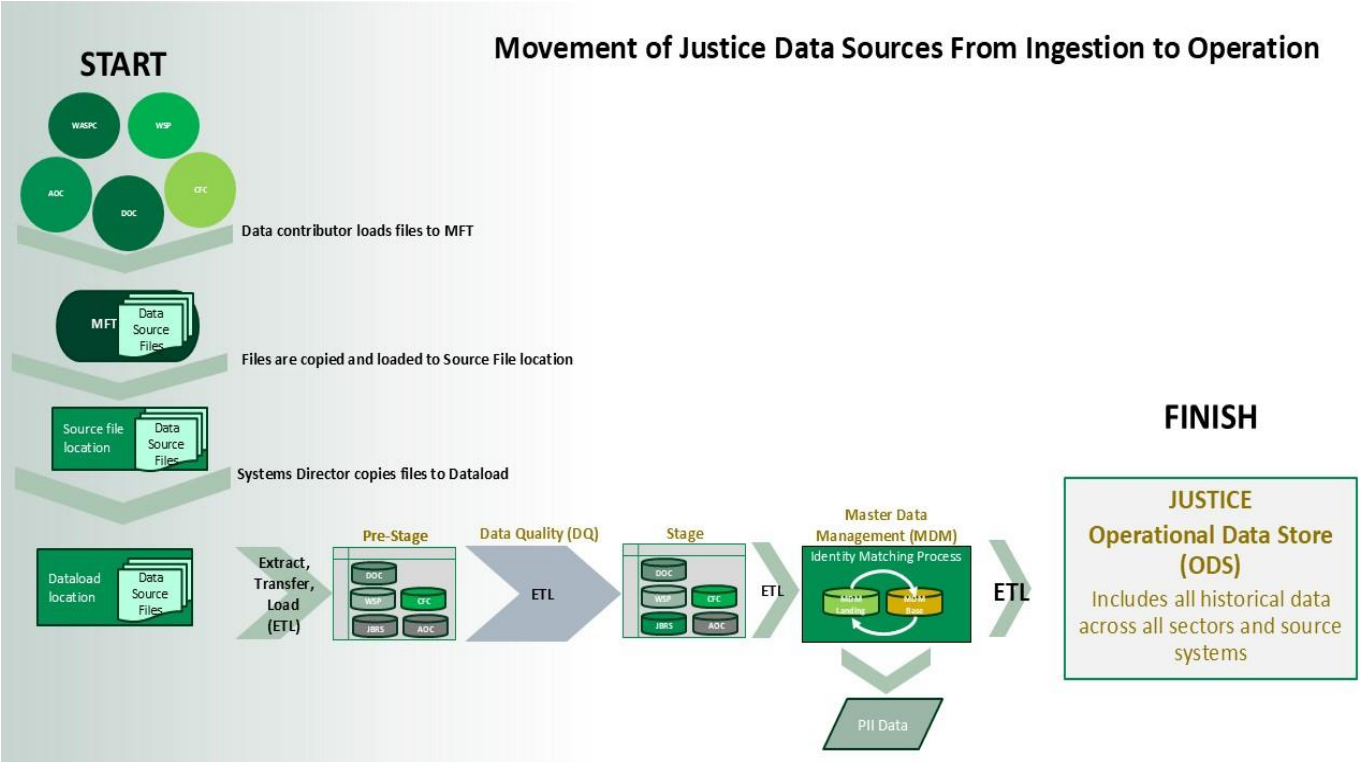
At the end of each project, data must be destroyed and purged from the applicable system(s), and a data destruction form will be completed, signed, and provided to confirm the destruction of the data.

Data Flow Process

Figure 2 illustrates the data flow and loading process for the JDW. The process includes:

(1) following retrieval of the source data, completing an initial data profile (e.g., did we get what we were expecting, are counts accurate);
(2) updating ETL routines if necessary (e.g., new fields, new codes) and loading them into the Pre-Stage environment (i.e., environment used to receive, clean, and prepare raw data before it is loaded into the main staging or data warehouse layers);
(3) loading to Stage environment (i.e., environment in which raw or semi-processed data is placed before it undergoes further transformations and loaded into the warehouse for analysis and reporting);
(4) loading to Master Data Management (MDM) environment (i.e., the framework that performs identity resolution within and between datasets); and
(5) loading to Operational Data Store (ODS) environment (i.e., environment consisting of a centralized database designed to integrate and store data from the different source systems).

FIGURE 2: FLOWCHART OF DATA THROUGH STAGES OF THE JDW LOADING PROCESS



Data Sharing Requirements

Data sharing agreements (DSAs) are formal contracts that govern how data are accessed, used, and protected between participating agencies. They define roles, responsibilities, privacy protections, security requirements, and permissible uses for sensitive information. DSAs provide the framework for lawful, accountable data sharing while supporting collaboration across agencies. Data shared under these agreements are recurring sources loaded into the JDW and matched with other JDW data to support cross-sector research and analysis.

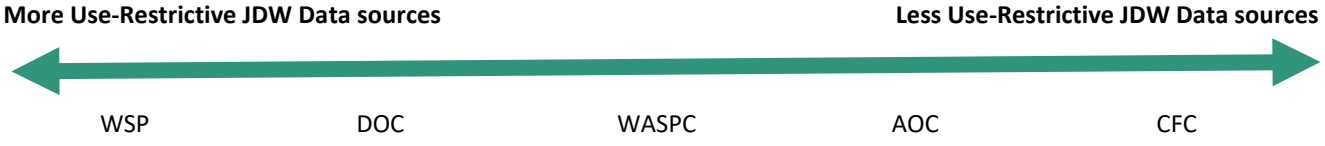
Data Confidentiality and Non-Disclosure Agreements

Some of the JDW data contributors require signed confidentiality acknowledgements. For example, DOC mandates a confidentiality and nondisclosure agreement, while WSP requires a compliance certification affirming adherence to terms. Other agreements similarly reinforce data confidentiality and prevent unauthorized disclosure.

Data Use Restrictions

JDW data access is limited to authorized persons who require the information to perform official duties under applicable DSAs. Although external researchers may request JDW data for approved purposes, sharing with third parties generally requires contributor approval, a formal data-sharing agreement, or, at minimum, notification to the data provider. Figure 3 illustrates the varying levels of use restrictions across JDW data sources, summarized below.

FIGURE 3: SPECTRUM OF JDW DATA ACCESS/USE RESTRICTIONS



Notes: "Less use-restrictive" data refers to JDW sources that permit use by OFM/PSPRC staff or agents and allow external researchers or state agencies to access the data through a formal request process, subject to contributor notification or written consent. "More use-restrictive" data refers to JDW sources limited to staff and agents of the contributing agency, OFM/PSPRC, and/or designated partners, typically with additional access limitations.

Data Security Requirements

All JDW data-in DSAs include standard security requirements aligned with federal and state law and industry best practices. Commonly referenced standards include Department of Defense data sanitization standards, NIST SP 800-40, and OCIO Policies SEC-04 through SEC-10. Core safeguards include encryption, restrictions on copying or duplicating data, and access limited to authorized users with unique, role-based credentials. Data-in DSAs for AOC, CFC, and WASPC data also require OFM/PSPRC to implement reasonable safeguards against unauthorized access.

Data Retention and Destruction Requirements

OFM/PSPRC's data-in DSAs with WSP and DOC contain the most detailed security requirements, including specific physical, network, and documentation controls. The DOC agreement also requires OFM to maintain tamper-protected system logs and audit trails for all JDW transactions involving DOC data. Data retention and destruction provisions generally limit retention to the minimum period necessary to fulfill the DSA or until the agreement expires. Destruction methods must comply with federal and state law, WaTech policies, and NIST guidelines. Some contributors also require a Certificate of Data Destruction or similar documentation verifying proper disposal.

Data Destruction Methods

Acceptable destruction methods vary by data type, but JDW data contributors' DSAs are largely consistent:

- Digital files on servers, workstations, or removable media: Wipe utilities, degaussing, or physical destruction.
- Paper documents: Confidential recycling, on-site shredding, pulping, or incineration.
- Optical discs: Incineration, shredding, or defacing with a coarse abrasive.
- Magnetic tapes: Degaussing, incineration, or crosscut shredding, especially for confidential or sensitive data.

Data Security Overview

PSPRC adheres to OFM's privacy program, as well as a set of more specific privacy principles. OFM's privacy program moves the idea of privacy into a culture of privacy by identifying our compliance obligations associated with data, combining those compliance obligations with best practices, and then aligning OFM policy and internal controls to reflect a high level of data stewardship in the protection of confidential information. A privacy program gives us a framework for managing privacy-related issues consistently by creating policies and procedures at a functional level, reducing risk and building trust. OFM's privacy program is built with a broad base of support throughout OFM's Forecasting and Research division to work on development and implementation of the privacy program. OFM Forecasting and Research currently has three privacy champions. Privacy Champions help facilitate awareness of privacy principles and their application to collecting, handling, and disseminating OFM's confidential information. They also assist in the creation, review, monitoring, and implementation of OFM's Privacy Program.

Security

We protect the confidential information entrusted to us against unauthorized access. Confidential Information is specific information that is not disclosable, is made confidential by law, or for which special handling is required.

Minimization/Purpose Driven

We limit the collection, access, and use of confidential information to only what we require to provide OFM services and retain it only as long as necessary to meet our business needs and legal requirements.

Transparency

We are transparent about what confidential information we collect, why we collect it, and how it is used.

Accountability.

We are accountable for collecting, using, managing, and disposing of confidential information in a manner that is consistent with best practices and as required by law, OFM policies, and procedures.

Value Driven

We are respectful of privacy rights associated with confidential information entrusted to us.

Culture Driven

We will ensure that OFM staff have access to relevant privacy training, resources, and guidance.

Due Diligence/Lawful Use

We only share confidential information consistent with the law and under an OFM agreement. Agreements shall include instructions about how confidential information is protected. For public records, we shall apply all applicable exemptions before sharing records containing confidential information. For all confidential information shared, we shall apply data minimization principles and redactions as possible.

Privacy Principles and Considerations

The PSPRC values the protection of privacy for all people and is guided by the following privacy priorities:

Lawful, Fair, and Responsible Use

The JDW's data collection, use, and disclosure is based on legal authority. The PSPRC collects, uses, and discloses information responsibly and ethically, avoiding discrimination, deception, or harm. The PSPRC follows privacy laws to safeguard the confidentiality of data. The PSPRC's privacy practices are also guided by Office of the Chief Information Officer (OCIO) Policy 141.10 and the Washington State Agency Privacy Principles. Additionally, per Revised Code of Washington (RCW) 42.48, the WSIRB is responsible for providing the requisite regulatory review, approval, and oversight of research that may involve these state agencies' clients, beneficiaries, patients, wards, and state agency employees (or these individuals' state agency personal records), in order to ensure the protection of the rights and welfare of human subjects of research.

Data Minimization

The PSPRC collects, uses, or discloses the minimum amount of information to accomplish the stated purpose for collecting the information. The PSPRC implements this by collecting only data that is essential for research related to criminal justice.

Small Number Standards

The PSPRC respects and honors the data that is included in the JDW. The PSPRC implements this by following small numbers standards in data reporting, suppressing all non-zero counts that are less than 10.

Transparency and Accountability

The PSPRC strives for both transparency and accountability. Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances. Accountability means being responsible and answerable for following data privacy laws and principles. The PSPRC implements this by ensuring that data processes, policies, and decision-making are clearly documented and available to research partners, committees, and oversight entities, as appropriate.

Due Diligence

The PSPRC takes reasonable steps and exercises care before and after entering into data use agreements with state agencies and third parties that include sharing personal information.

Security

The PSPRC uses appropriate administrative, technical, and physical security practices to protect the confidentiality, integrity, availability, and control of personal information. The PSPRC implements this through a combination of policies, technologies, and procedures designed to protect sensitive crash and crash-related data from unauthorized access, breaches, and misuse.

OCIO Data Categories

OCIO Policy 141.10 Securing Information Technology Assets, Standard 4.1 Data Classification requires that agencies "must classify data into categories based on the sensitivity of the data." Additionally, agency data classifications must translate into or include four categories identified by the OCIO. Under 141.10, 4.2 Data Sharing, when sharing Category 3 or 4 data outside the agency, an agreement must be in place unless otherwise prescribed by law. The agreement must, among other things, include the categorization of the data.

The division, in coordination with OFM Legal and Legislative Affairs' contracts unit, prepares Data Sharing Agreements and Data Use Agreements. Data Classification Agencies must classify data into categories based on the sensitivity of the data. Agency data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

(2) Category 2 – Sensitive Information
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

(3) Category 3 – Confidential Information
Confidential information is information that is specifically protected from either release or disclosure by law. This includes but is not limited to:

- Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
- Information about public employees as defined in RCW 42.56.250.
- Lists of individuals for commercial purposes as defined in RCW 42.56.070 (9).
- Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

(4) Category 4 – Confidential Information Requiring Special Handling
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanction.