Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 15.26

Subject:	HRIS Data Warehouse Administration
Information Contact:	HRIS Program MS 45830 (360) 725-5888 E-mail: hris@dshs.wa.gov
Authorizing Source:	DSHS Secretary
Effective Date:	April 10, 2019
Revised:	March 31, 2023
Approved By:	**Original signed by Wendy Long** Senior Director, Human Resources Division

Purpose

This policy identifies the definitions, access criteria, roles, and responsibilities associated with the administration of the human resources information services (HRIS) data warehouse. This policy also establishes the HRIS data warehouse (HRISDW) as the authoritative repository of HRMS data for department employees, systems, and applications to use, in cases where direct access to the HRMS application is not available, or appropriate for the specific business need.

Background

The human resources division (HRD) is the steward of department data extracts derived from HRMS, i.e. "gap files", as designated by the office of financial management (OFM). HRD has a responsibility to safeguard confidential data, and follow applicable federal and state laws regarding disclosure.

As business owner, HRD is responsible for the development, maintenance, and operation of the HRIS data warehouse (HRISDW). The HRISDW is a central repository of confidential HR data, designed for use by interested parties with an appropriate and documented business need to obtain information relevant to their organizational unit or units.

Scope

This policy applies to all organizational units of the Department of Social and Health Services (DSHS).

Additional guidance

Chapter 42.52 RCW ethics in public service
Chapter 42.56 RCW Public Records Act
Chapter 70.02 RCW Health Care Information Act
42 CFR § 403.812 Health Insurance Portability and Accountability Act of 1996
AP 4.05, Delegation of authority – personnel actions
AP 5.01, Privacy policy – safeguarding confidential information
AP 9.13, Enterprise risk management
AP 15.10, Information and technology security
AP 15.21, Information technology standards compliance
AP 18.64, Standards of ethical conduct for employees
Information security procedures manual
Information security standards manual
Information technology standards manual
HRIS Reporting user access request and agreement
HRISDW access – criteria, roles and responsibilities
HRISDW maintenance and operation – roles and responsibilities
Governor's Executive Order 00-03 Public Records Privacy

Definitions

Data exchange: An interface created for an organizational unit, with a documented and specific business need, to obtain data from the HRIS data warehouse. This data interface is designed to be used on an on-going basis, for use by a specific system or application under the organizational unit's control, in order to support a business activity.

Data sharing agreement: An agreement between HRD and an organizational unit to establish a data exchange. This agreement permits the organizational unit to obtain data from the HRIS data warehouse, and identifies the organizational unit's requirements and responsibilities for appropriately safeguarding confidential data. The agreement serves as documentation for the need to grant a data exchange to an organizational unit.

Database administrator (DBA): The individual, or group of individuals, responsible for the on-going maintenance, operation, and security of the server assets utilized by the HRIS data warehouse. The information administration unit (IAU) team within the technology information administration's technology services division (TIA/TSD) fulfills this role.

HRIS architect: The individual, or group of individuals, responsible for the design, development, maintenance and operation of the HRIS data warehouse application. The HRIS architect is also

responsible for developing and implementing data architecture standards for the application, and ensuring developed solutions meet department standards. The HRIS architect resides within the HRIS Program.

HRIS data warehouse (HRISDW): The database containing confidential data from various HR data sources and systems, as well as any associated reporting and analytics platforms.

HRIS developer: The individual, or group of individuals, responsible for development of the HRIS data warehouse. The HRIS developer resides within the HRIS program.

HRIS program: HRD has overall responsibility and oversight for the management of HR data for DSHS, including the human resources information services (HRIS) program; while the technology innovation administration has responsibility for the administration of the HRIS program.

Information security office (ISO): The information security office (ISO) provides department-level oversight of information security and reports to the chief information security officer. ISO's responsibilities include developing information security policy and standards, providing support and solutions to emerging security and disaster recovery challenges across DSHS, administering policy oversight, responding to information security incidents and attacks, and working closely with DSHS administrations to protect information and assets. The IT security administrator (ITSA) within TIA/TSD serves as the conduit to the ISO for the HRIS program.

Organizational unit: An administration, division, or office that functions at a headquarters, regional or local office level within DSHS.

Reporting user: A DSHS employee, with a documented and specific business need, who obtains data from the HRIS data warehouse for their individual use.

User agreement: An agreement by a reporting user, permitting them to obtain data from the HRIS data warehouse. This agreement confirms the reporting user's understanding and acceptance of applicable laws and policies regarding confidentiality, ethics, and appropriate use of resources. The agreement serves as documentation for the need to grant a reporting user's access.

Policy

HRD has created the HRISDW to serve as the authoritative repository of HRMS data for use by DSHS employees, systems, and applications in cases where direct access to the HRMS application is not available or not appropriate for the specific business need.

HRD is the data steward of DSHS HRMS data, the business owner of the HRISDW, and is responsible

for establishing and maintaining:

- All criteria, roles, and responsibilities involving access to the HRISDW. This information is available in the HRISDW access – criteria, roles and responsibilities.
- A maintenance and operation plan for the HRISDW. This information is available in the HRISDW maintenance and operation - roles and responsibilities.