Office of the Washington State Auditor

# The State Auditor's Office, data protection and data privacy

## Data privacy and artificial intelligence present significant concerns

Policy makers in states across the nation are considering how best to place regulatory safeguards around generative artificial intelligence technology, particularly concerning AI's potential for workforce disruption, bias in decision-making and new intrusions into personal privacy.

The Office of the Washington State Auditor shares those concerns, as an agency committed both to government transparency and to the proper use of data to ensure government accountability.

Privacy can be protected, and other concerns of the artificial intelligence era can be addressed, without blocking access to the data that independent reviewers need to ensure government accountability.

## The State Auditor's Office conducts thousands of audits every year

Our Office published an average of 45 audits a week in fiscal year 2023, a total of 2,379 reports. Included are more than a dozen separate types of audits of governments as different as King County and the Quincy Cemetery District. Among the audits we perform are:

- **Accountability audits** assess whether public funds and assets are protected and accounted for, and governments are following applicable laws, regulations and their own policies.
- **Cybersecurity audits** look for weaknesses in government technology systems and propose solutions to help strengthen them.
- **Financial audits** provide an independent audit opinion on whether state and local government financial reports are accurate and complete.
- **Performance audits** evaluate the efficiency and effectiveness of government processes and programs with the goal of making them work better.
- **Fraud investigations** look into the alleged loss of public funds or other potentially illegal activity.

#BeCyberSmart

*December 2023*

## Data is the cornerstone of accountability

Without data, there can be no audits of government. Every type of audit is based on fact, and those facts are established by the data auditors collect and analyze. For example:

- Financial audits require **detailed government financial data**.
- Cybersecurity audits require **sensitive information about a government's computer systems** and their vulnerabilities.
- Fraud investigations may gather **personal financial information** about the subject of the inquiry.
- Audits of health care services may include certain **health care billing records**, which can be reviewed to ensure they were processed for payment properly.

## Data protection is a priority for the State Auditor's Office

- The Office has established more than **2,000 data sharing agreements** with local governments and state agencies. These agreements specify roles, responsibilities and expectations for the secure handling of sensitive data during an audit.
- By Office policy, auditors **collect the minimum amount of sensitive data needed** for each audit. There are also protocols in place to destroy data when no longer required by audit or records retention rules.
- **We work with each auditee** to determine and ensure data is transferred securely.
- We offer a **secure method of data transfer** that is built on the state's Enterprise Shared Tenant, but often we use the entity's preferred data transfer method.
- Audit data is **stored in a secure location** that allows audit teams to specify who can see data, and later ensure the data is destroyed when no longer in use
- The Office also established a **Data Risk Workgroup**, which continuously adapts internal policies and procedures to maintain high levels of security, in addition to reviewing new technology applications.
- To complete its work, the Office also employs a cadre of **cybersecurity professionals**, including a chief information security officer and staff, a dedicated artificial intelligence expert, a team of cybersecurity auditors and specialist in expedited cybersecurity reviews of local governments.

As the State implements new policies governing the use of AI, caution must be exercised to ensure that access to data for audit purposes is not inhibited.

*December 2023*

#BeCyberSmart