September 2026

DPM Dashboard Data Sharing Guidelines

Background: DPM published interactive dashboards to facilitate data availability and to support data-driven decision making. Access to dashboards containing sensitive information has been restricted to HR audiences and other authorized users who support HR on a need-to-know basis to protect confidentiality. Furthermore, dashboards have been designed to limit risk and mitigate exposure of protected information including but not limited to personally identifiable information (PII) beyond that which is necessary to perform the work.

Purpose: HR professionals and staff with authorized access are expected to maintain confidentiality and exercise discretion when encountering sensitive data in their roles. The following guidelines provide expectations to authorized users of restricted access dashboards regarding data sharing to support responsible data stewardship and to prevent disclosure of protected information to unauthorized parties.

Guidelines:

- Only share with those who need to know to perform the work
- Only share the information that is absolutely necessary to accomplish the work
- Present aggregate data whenever feasible
- Remove any personal identifiers that may exist before sharing
- Provide data in the most secure way possible
    - Consider how to share the information and whether the information can be provided verbally rather than in written form
    - Consider what is defined as a public record and is subject to open records requests
    - If you must transfer data, take additional steps to ensure secure transfer:
        - Protect with a password
        - Use encryption
        - Save a copy to a shared secure location
- Store any data that has been exported from a dashboard in a secure location
- Consider ethical use standards and ensure the data is only being used for the intended purposes
- Comply with all applicable laws, policies, rules, and regulations

Contact BMRS when:

- You have difficulty understanding or explaining the data
- You have questions about what is and is not appropriate to share
- You have concerns that data is being misused for reasons beyond the intended purposes

Refer to the State of Wisconsin – Acceptable Technology Use, Access, and Security Policy and the State of Wisconsin IT Security Policy Handbook if there has been disclosure of information that would constitute a clearly unwarranted invasion of a person's privacy or a data breach. Depending on the nature and scope of the breach, you may need to follow your assigned agency's data breach policy, as well.