SMPH GitLab – Public, Internal, Sensitive, and Restricted Data Guidelines

Basic Policy

This page was moved to kb.wisc.edu/134071
Click in the link above if you are not automatically redirected in 10 seconds.

The current UW-Madison GitLab instance as a whole is not set up to be used with sensitive or restricted data. The goal is for the SMPH GitLab instance to provide a secure environment for public, internal, and sensitive data. It is unlikely that restricted data will be able to be securely used within GitLab. However, there is always an option to have data de-identified or utilize another more secure storage option for that type of data. The examples below are not all encompassing. If you are unsure of what type of data you have, please see the troubleshooting section below. GitLab is intended for collaboration, code review, and code management. It is NOT intended for data storage/sharing.

Examples of Public Data

- Publicly shared research
- Internally developed and/or owned computer applications and/or source code designated in the public domain
- Public announcements
- Statements and other reports filed with federal or state authorities and generally available to the public

Examples of Internal Data

- Asset registers
- Internal communications
- Contracts
- Manuals/policies/procedures

Examples of Sensitive Data

- Intellectual property including research data or results prior to publication or the filing of a patent application
- Private industry sponsored or non-disclosure agreement research
- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value
- Information that is proprietary or produced only for use only by members of the university, such as project plans and email reports
- Internally developed and/or owned computer applications and/or source code not designated as in the public domain
- Computer applications to which the university owns the code
- Proprietary financial, budgetary, or personnel information not explicitly authorized for public release
- Emails and other communications that have not been specifically approved for public release

Examples of Restricted Data

- Personal Health Information (PHI)
- Family Educational Rights and Privacy Act (FERPA) data
- Payment Card Industry Data Security Standard (PCI DSS)
- Social Security Numbers
- Driver's license numbers and state resident/personal identification numbers
- Financial account numbers and associated security codes or passwords
- Deoxyribonucleic acid profile
- Personal Identifiable Information (PII)
- Trade secrets or information where confidentiality must be ensured
- Unique biometric data, including fingerprint, voice print, retina or iris image
- Digitized signature
- Authentication information, such as passwords, security codes, and key codes
- Security plans and procedures

For more information on sensitive and restricted data and for more classification examples, please see the IT Data Classification Policy and UW System's "Information Security: Data Classification" page.

Troubleshooting

- For general questions on data classification, reach out to SMPH Cybersecurity.
- For questions on PHI, reach out to the SMPH HIPAA Privacy Coordinator.
- For questions on FERPA, reach out to Angie Rieves or Phil Hull in the Office of the Registrar.