INDIANA UNIVERSITY
SCHOOL OF MEDICINE

IU School of Medicine Policy on Access to Administrative Data

ds-bi-0001

About This Policy

Effective Dates:
01-01-2024

Last Updated:
09-15-2023

Responsible University Administrator:
Jamie Dimond Executive Associate Dean for Administrative Services

Policy Contact:
Ben Steckler bejsteck@iu.edu

Scope

All employees, including faculty, staff, and student employees, of the IU School of Medicine (IUSM), as well as those individuals with approved IU-affiliate status, are subject to the provisions of this policy. Any other parties who use, work on, or provide services involving IUSM computers and technology systems are also subject to the provisions of this policy.

The scope of this policy is to address the School of Medicine's approach towards granting employees and IU affiliates access to IUSM administrative data sources utilized for operational, analytical, and business intelligence purposes within IUSM's Business Intelligence environment. This policy pertains only to administrative data, including financial, human resources, compensation, research administration, student services, educational operations, and space management. Administrative data may be either university or non-university data due to the nature of IUSM's business activities.

Clinical trials, instructional, scientific research, and other non-administrative data are excluded from this policy.

This policy applies to all data and information contained within the business intelligence environment, regardless of business purpose and the format or mechanism by which the data and information is used.

This policy addresses all data classifications as defined by the University (Data Classification: IU Data Management: Indiana University):

1. Public – data in which little to no restrictions apply.
2. University-internal – data accessed by all eligible employees of the university in the conduct of university business.
3. Restricted (limited access) – data that may not be accessed without specific authorization, or only selective access may be granted because of legal, ethical, or other constraints.
4. Critical – data that has the highest level of protection by which inappropriate handling could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.

The business intelligence environment may also contain data from IUSM partners or third parties. These data are classified as “IUSM-internal,” defined as non-university data contained within the business intelligence environment used for internal IUSM business purposes. IUSM-internal data should be treated in the same manner as restricted classified data and is only accessible by those with access to the business intelligence environment and comparable restricted data.

Policy Statement

The IUSM operates on a model of transparency of administrative data where reasonable, and in a manner that ensures that those who have a business reason to access data are provided access to the necessary data environments and are also informed of the management expectations associated with this access.

Access to the business intelligence environment is granted on a case-by-case basis. Approvals are granted based on an individual’s role and their documented need, based upon the procedure below, for access to data/reports in a specific data domain. Where data access levels have not been set for a particular role, such as executive associate dean, requests will be approved or denied by the school or university’s data steward for that data domain.

To obtain access to elements of the business intelligence environment, the requestor should follow the access requests procedure found on BI Central. Once the required forms, acknowledgments, and training requirements are complete, data access is facilitated by IUSM Business Intelligence.

Management expectations and associated University policies will be in force for all those who have access to the business intelligence environment. Access to the business intelligence environment is contingent upon users maintaining current compliance with all necessary trainings (FERPA, HIPAA, etc.) and may be removed at any time or at the discretion of the school or university leadership.

Non-University data is made available within the business intelligence environment upon approval and agreement between IUSM and the affiliated partner unless available publicly. Unless otherwise specified, all non-IU data is be treated as restricted-level data. This means that non-IU data is used only for internal IUSM business purposes.

Reason For Policy

The purpose of this policy is to accomplish the following:

1. Address administrative data access needs
2. Protect data and information assets
3. Preserve data integrity, confidentiality, and availability
4. Be compliant with FERPA, HIPAA, federal, state, local, and university regulations
5. Raise awareness of appropriate data use
6. Improve the management of data access

Procedure

Request for Access to the IUSMBI Environment

1. The requestor should complete the Data Access Request form on BI Central.
2. Upon completion of the form, the IUSMBI team will be notified and will review the request.
3. If the IUSMBI team approves the access request, the user will be added to the appropriate roles and groups. The user and their supervisor will then be notified that access has been granted and is complete.
4. If the IUSMBI team denies the access request, the user and their supervisor will be notified via automated email and provided with a reason. Appeals may be filed by emailing IUSMBI@iu.edu.
5. Requests for additional access may be made using the same process.

Maintenance of Business Intelligence Environment Access

1. Users are required to renew their IUSM Data Acknowledgement annually. If at any point their acknowledgement, IU Acceptable Use Agreement, or required compliance (FERPA, HIPAA, etc.) expires, user access will be removed until that user has renewed all appropriate agreements.
2. Each September, IUSM business intelligence staff will coordinate a review of appropriate roles and access with data owners throughout the school.
3. Data owners or designated proxies will inform business intelligence staff of any users who should be removed from roles or groups.
4. The business intelligence team will notify users if access has been revoked and will direct any appeals to IUSMBI@iu.edu.
5. Data owners may contact IUSMBI@iu.edu to request users be removed from any applicable roles or groups due to change in roles, responsibilities, employment status, or at data owner and IUSM discretion.

Definitions

The IUSM Business Intelligence Environment encompasses data and dashboards maintained by IU School of Medicine Business Intelligence. Elements of the environment include, but are not limited to:

- Tableau reports housed on the University Tableau server
- SQL Server Reporting Services Reports and Power BI Reports on IUSM servers
- Data models such as the General Ledger cube and Compensation cube
- Data sets in IUSM BI owned Denodo databases
- Data files stored in IUSM BI managed SharePoint locations

FERPA stands for Family Educational Rights and Privacy Act.

HIPAA stands for Health Insurance Portability and Accountability Act.

Sanctions

Should an individual not complete the required forms and training, access to the BI data environment will not be granted. Also, should those with access not maintain a current status of the required training as stipulated in this policy, access may be revoked.

History

1. IUSM BIOP-PO-0001, 13 September 2013, first draft of policy.
2. Policy reviewed, edited, and completed in new format on 27 September 2013.
3. Policy given final approval and published on 12 December 2013 (first version).
4. Policy draft revisions made on 09 September 2014.
5. Policy given final approval and published on 23 September 2014 (second version).
6. Policy updated on 08 May 2017.
7. Policy updated on 02 January 2018.
8. Policy updated on 07 June 2023.
9. Policy updated on 29 February 2024.