

Restricted Information

The types of information listed below are examples of Restricted Information, which is confidential, and if disclosed, has the highest impact on in the university. Use of Restricted Information carries the burden of extensive management controls, known as [Tier III Controls](#), to protect the confidentiality of the information, the information systems that contain it, and the data storage mechanisms where it is stored. By definition, this level of information is not to be shared without proper agreements or need-to-know access.

- legal investigations conducted by the university
- internal audit and compliance data (integrity)
- working data of tenure committees (pre-selection)
- social security numbers associated with a person's name
- birth date associated with a person's name
- credit card transaction data, CVV numbers (pertaining to university purchasing cards or PCards)
- CWRU Network ID combined with its password (note that the Network ID by itself is Public information)
- intellectual property, trade secrets, and technical data supporting technology transfer agreements (before public disclosure decisions have been made)
- proprietary information entrusted to the university by agreements with third parties
- detailed information pertaining to university incidents which must not be disclosed until approved by university marketing and communications (UMC)
- any information designated in writing as Restricted by the Vice President of Information Technology/Chief Information Officer

An additional category of Restricted Information, related to clinical research patient information, is to be managed by the [HIPAA Standards](#) to augment Tier III Controls.

- electronic personal health information (ePHI)
- limited data sets