UNIVERSITY OF MASSACHUSETTS MEDICAL SCHOOL

LEVEL

Data Classification Examples

4 Highly Restricted Use

Information that would cause severe harm to individuals, UMMS, or the State if disclosed in an unauthorized manner. Controls strictly limit the ability to use this information, including no ability to extract for operational purposes

- Social Security Numbers in association with Personal Health Information
- Certain individually identifiable medical records and genetic information (for example: HIV Status associated with a Person's Name or Social Security Number)
- Specific contractual or customer obligations
- Research information classified as highly restricted use

3 Confidential

Information that would likely cause harm to individuals, UMMS, or the State if disclosed in an unauthorized manner. Controls limit access but allow information to be extracted and accessed for operational purposes.

- Personal Health Records / Protected Health Information
- Personally Identifiable Information, including Social Security Number and National ID
- Financial Records, including banking information for direct deposit
- Student Records
- Research information classified as confidential
- Passwords that can be used to access confidential information
- Other personal information protected under state, federal, and foreign privacy laws not classified as Level 4.

2 Internal

Information which would not cause harm if disclosed in an unauthorized manner, but UMMS has chosen to keep confidential. Controls allow access with little technical barriers.

- Institutional financial records
- Patent applications and work papers, draft research papers
- Research information classified as internal
- Not routinely distributed outside of the School : internal communications, minutes of meetings (i.e. IRB meetings, IACUC meetings) and internal project reports.
- Other personal information protected under state, federal, and foreign privacy laws not classified as Level 4 or 3.

1 Public

Public Information. No control limitations.

- Published research
- Course catalogs
- Faculty and Staff Directory Information
- Routinely distributed to the public regardless of whether the School has received a public records request, such as: annual reports, publicly accessible web pages, marketing materials and press statements.

Need to talk to an expert? Contact ITSecurity@umassmed.edu

University of Massachusetts Medical School

<table>
<tr><th colspan="2">Data Classification & Encryption</th></tr>
<tr><th>Highly Restricted Use</th><th>Confidential</th></tr>
<tr><td>Information that would cause severe harm to individuals, UMMS, or the State if disclosed in an unauthorized manner. Controls strictly limit the ability to use this information, including no ability to extract for operational purposes</td><td>Information that would likely cause harm to individuals, UMMS, or the State if disclosed in an unauthorized manner. Controls limit access but allow information to be extracted and accessed for operational purposes.</td></tr>
<tr><td colspan="2">Encryption is required for all laptops, workstations, mobile devices and portable drives that may be used to store or access this data.</td></tr>
<tr><td colspan="2">All portable media (including thumb drives or portable disks) must be encrypted and physical access to those devices must be restricted (i.e. a locked desk drawer)</td></tr>
<tr><td colspan="2">Laptops and Desktops that access third-party data (i.e., UMMHC) must comply with all data protection and encryption policies of the third-party</td></tr>
<tr><td colspan="2">This type of data, while stored within our data center, is not required to be encrypted at rest. However, if the data is stored <b><u>outside</u></b> of the data center, the data must be encrypted. *unless required by contract</td></tr>
<tr><td colspan="2">All databases, application servers and file systems must leverage appropriate access controls to ensure that access to the data is limited to those whose job functions require access. (i.e. - regulated environment). We have additional controls in our regulated environment for data that must be accessible from the internet (i.e. - VPN)</td></tr>
<tr><td colspan="2">All backups, for business continuity purposes, must be encrypted</td></tr>
</table>