Managing Research Data Risks

All data, including research data, carries risk. Although risk management probably isn’t the primary focus of your research efforts, it’s an important step in helping your project stay on track and avoiding penalties.

To help you spend less time managing risk and more time conducting your research, UD IT Security provides this resource to explain the different risks that could affect your data and your project and assist you in planning how to appropriately manage those risks.

You can use the information in this guide to inform your data management plan. You can also contact IT Security (secadmin@udel.edu) for a consultation about research data risk and for assistance in incorporating risk management strategies into your data management plan and research practices. For more information, explore the research security materials available on the Secure UD website: www.udel.edu/security/data/research

### CONFIDENTIALITY RISKS:
Will your project involve any data that has restrictions on who can view or access it?

<table>
<thead>
<tr>
<th>Do you have any data that...</th>
<th>If you do, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>can only be disclosed to authorized parties?</td>
<td>encrypt the data at rest and in transit</td>
</tr>
<tr>
<td>is required by law, regulation, or contract to remain confidential?</td>
<td>control access to the data¹</td>
</tr>
<tr>
<td>may not be published or made public until authorized by a funding agency?</td>
<td>physically secure devices and paper documents</td>
</tr>
<tr>
<td>is sensitive by nature and would have a negative impact if disclosed?</td>
<td>securely dispose of unneeded data and devices</td>
</tr>
<tr>
<td>would be valuable to hackers, corporate spies, foreign intelligence, etc.?</td>
<td>acquire data only as needed</td>
</tr>
</tbody>
</table>

**The big picture:** Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

### INTEGRITY RISKS:
Will your project involve any data that, if not maintained with integrity, would significantly impact the accuracy or feasibility of the study?

<table>
<thead>
<tr>
<th>Do you have any data that...</th>
<th>If you do, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>must remain accurate and uncorrupted?</td>
<td>back up the data</td>
</tr>
<tr>
<td>must only be modified by certain individuals or in a controlled manner?</td>
<td>control access to the data¹</td>
</tr>
<tr>
<td>must come only from trusted sources?</td>
<td>log data access and changes</td>
</tr>
</tbody>
</table>

**The big picture:** Data integrity is about protecting data against improper maintenance, modification, or alteration. It includes data authenticity.

### AVAILABILITY RISKS:
Will your project involve any data that, if lost, stolen, or destroyed, would be irreplaceable or would significantly impact the feasibility of the study?

<table>
<thead>
<tr>
<th>Do you have any data that...</th>
<th>If you do, then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>must remain available or accessible during the project?</td>
<td>back up the data</td>
</tr>
<tr>
<td>must remain available or accessible after the project is complete?</td>
<td>inventory the data</td>
</tr>
<tr>
<td>cannot be easily re-obtained or re-created?</td>
<td>use metadata to identify and describe data</td>
</tr>
</tbody>
</table>

**The big picture:** Data availability is about the timeliness and reliability of access to and use of data. It includes data accessibility.

---

¹ For more information, consult IT Security (secadmin@udel.edu) for detailed advice and guidance.
### PRIVACY RISKS: Will your project involve any data that, either by itself or in combination with publicly available information, has the potential to violate privacy expectations of individuals?

**Do you have any data that...**
- involved human subjects?
- has explicit legal or regulatory privacy protection requirements?
- is sensitive, or has the potential to be sensitive if combined with other information?

**If you do, then...**
- de-identify or aggregate data where appropriate
- provide fair notice of monitoring, data collection, and/or data usage
- see the recommendations for confidentiality risks on the other side of this resource

**The big picture:** Data privacy is about respecting individuals’ reasonable expectations to be free from unreasonable observation and excessive collection of personal data (what is being observed and collected and how it is being used).

### LEGAL, REGULATORY, AND CONTRACTUAL RISKS: Will your project involve any data that is subject to legal, regulatory, or contractual requirements?

**Do you have any data that...**
- is subject to laws or regulations (e.g., FERPA, HIPAA, COPPA)?
- is provided to you under a contract or agreement?
- is subject to grant or contract restrictions or security requirements?

**If you do, then...**
- be aware of relevant laws, regulations, and contract requirements and how they apply to your data
- include requirements in your data management plan
- consult General Counsel or IT if you have compliance questions

**The big picture:** Data laws and regulations govern the handling of particularly sensitive kinds of information and may present the risk of fines, funding loss, or even imprisonment. Health data, education records, defense articles, and other data present legal and regulatory risk that goes hand-in-hand with other risks like confidentiality, privacy, human, etc. Sponsored research agreements may specify data security standards and requirements that must be followed during or after the study. Data contracts may govern how data from a particular source or generated by a particular contract can be used or what rights researchers acquire to that data.

### HUMAN RISKS: Is every member of your team, including you, aware of data risk and security?

**Is your team...**
- aware of their responsibility for security?
- aware of security best practices?
- watchful for unusual behavior that may indicate data theft?

**If not, then...**
- sign up for Secure UD Training
- discuss security with your team and make it integral to your project
- consult IT if you have questions

**The big picture:** Human risk includes human vulnerability to social engineering, awareness of security practices, and insider threats.

### Notes

1. Controlling access to data includes: authorizing access based on “need to know,” uniquely identifying and authenticating users, using two-factor authentication (2FA) where practical, setting roles and permissions for access, and periodically reviewing access.

2. Managing devices includes: using anti-virus software, routinely patching software, whitelisting applications, using device passcodes, suspending inactive sessions, enabling firewalls, and using whole-disk encryption.