**Researcher Data Protection and Security Awareness Tool for Education**

**PURPOSE**
The Harvard Catalyst Data Protection Subcommittee designed this resource to help researchers to assess the research data security of their existing studies. Researchers and institutions prefer to identify and resolve issues internally rather than wait for an audit or breach to discover gaps in a program’s privacy or security practices. The questions selected for this document are intended to help identify gaps, where any exist, and to encourage the researcher to have a conversation with the appropriate individuals in their institutions to help close the gap. Those conversations can help elucidate best practices. We recommend this tool be updated with your institution specific guidelines and contact information and shared as an educational tool and/or posted to an internal webpage where researchers frequent. This document can then be shared with researchers prior to research being conducted as a starting point for developing awareness, discussing and developing knowledge about research data protection and security.

The questions are divided into two sections:
1. **INSTITUTIONAL INFORMATION**
2. **RESEARCH DATA PROTECTION AND SECURITY INFORMATION**

**FOR RESEARCH ADMINISTRATION/INFORMATION TECHNOLOGY STAFF: HOW TO USE THIS TOOL**

- Review the Researcher Data Protection and Security Awareness Tool for Education and complete all the fields in blue. *(For more information about attribution, sharing, and adapting, please see the last two pages of this document)*
- Determine if there are questions specific to your institution and/or the research study that should be added for the researcher to review.
- After all the updates have been made, share with the researcher and schedule a time to discuss and review.
We recommend that researchers respond with candor. It is best to develop an awareness for research data protection and security and resolve any issues upfront.

Step 1: Respond to the questions in sections one and two to the best of your ability.

SECTION ONE: INSTITUTIONAL INFORMATION

1. Did you know that the [insert the department name, contact name(s), phone number(s), and email address(s)] is responsible for information security?
2. Did you know that you should contact [insert the department name, contact name(s), phone number(s), and email address(s)] if there is a suspected data/information incident or breach?
3. Did you know that you should contact [insert the department name, contact name(s), phone number(s), and email address(s)] with any of your research data protection questions?
4. Did you know that some institutions classify their data into different levels/categories? For example, Harvard University, classifies data into five levels, with Level 1 being the least risk going all the way to, Level 5, being the highest risk. For additional information about Harvard’s data classification levels, please go to their Information Security website.

   Harvard’s data classification levels:
   **Level 1:** Public information
   **Level 2:** Information the disclosure of which would not cause material harm, but which the hospital has chosen to keep confidential
   **Level 3:** Information that could cause risk of material harm to individuals or the hospital if disclosed
   **Level 4:** Information that would likely cause serious harm to individuals or the hospital if disclosed
   **Level 5:** Information that would cause severe harm to individuals or the hospital if disclosed

5. Did you know that you could find information about [insert the institution name, contact name(s), phone number(s), and email address(s)] policies on research data protection on our website? These policies include [insert additional examples]:
   a. Data Protection Policy Name: [insert policy name and storage location/link to access the document]
   b. Privacy Policy Name: [insert policy name and storage location/link to access the document]
c. Information Security Policy Name: [insert policy name and storage location/link to access the document]
d. Data Sharing Policy Name: [insert policy name and storage location/link to access the document]
e. Other Policy Name: [insert policy name and storage location/link to access the document]

6. Do you know if everyone on your team has reviewed these policies?

SECTION TWO: RESEARCH DATA PROTECTION AND SECURITY INFORMATION

1. Did you know that research subject data has different protection requirements based on if the data is identifiable or not?
2. Did you know that you should never store research subject identifiable data on an unencrypted portable device (e.g., laptop, smart phone, tablet, etc.)?
3. Did you know that you should never store research subject identifiable data on any personal device, home computer, or other privately owned machine?
4. Did you know that you should never share passwords or account information with other team members?
5. Did you know that you should regularly monitor and assess the permissions to the data?
6. Did you know that you should remove an individual’s access privileges (e.g., folders and files that contain data sets) to research data when they leave the research project or the institution?
7. Did you know that you should dispose of printed data that contains identifiers securely by utilizing the office/department shredder or records removal container (e.g., Iron Mountain)?
8. Did you know that sharing research data with collaborators may require special agreement or memorandum, such as, data use agreement, data transfer agreement, or a memorandum of understanding?
   a. If you are not sure if sharing your research data requires a special agreement or memorandum, you should contact [insert the department name, contact name(s), phone number(s), and email address(s)].

Step 2: Review your responses to sections one and two. Determine questions you were unsure or didn’t know the answer.

Step 3: Reach out to your research contacts (listed below) and request a time to review your responses for support and guidance.
RESOURCES

Institution resources: [insert institution specific resources such as websites(s), educational tools and resources, contact name(s), phone number(s), and email address(s)]

Additional recommended resources:

- Harvard Catalyst Education Video Library: https://catalyst.harvard.edu/services/educationvideolibrary
- Harvard University Information Security: http://security.harvard.edu/

RESEARCH CONTACTS

- Institutional Review Board: [insert contact name(s), phone number(s), and email address(s)]
- Information Security: [insert contact name(s), phone number(s), and email address(s)]
- Privacy Office: [insert contact name(s), phone number(s), and email address(s)]
- Office of Compliance: [insert contact(s) name, phone number(s), and email address(s)]
ATTRIBUTION, SHARING, AND ADAPTING

We encourage you to:

▪ **Request** – email us and request the materials
▪ **Share** – copy, distribute, and transmit the work
▪ **Adapt** – adapt the work to suit your needs

Under the following conditions:

▪ **Attribution**: We encourage the broad research data security self-assessment. In freely using the materials or when citing this document, we require that you acknowledge Harvard Catalyst as the publisher and that you give appropriate credit to any individual named authors.

▪ **Suggested citation**: This material is the work of the Harvard Catalyst Data Protection and Privacy Subcommittee of the Regulatory Foundations, Ethics, and Law Program. This work was conducted with support from Harvard Catalyst | The Harvard Clinical and Translational Science Center (National Center for Research Resources and the National Center for Advancing Translational Sciences, National Institutes of Health Award 8UL1TR000170-05 and financial contributions from Harvard University and its affiliated academic health care centers). The content is solely the responsibility of the authors and does not necessarily represent the official views of Harvard Catalyst, Harvard University, and its affiliated academic health care centers, or the National Institutes of Health.

With the understanding that:

▪ **We might contact you**: We are interested in gathering information regarding who is using the materials and how they are using it. We may contact you by email to solicit information on how you have used the materials or to request collaborations or input on future activities

▪ **When reusing or distributing, make clear the above terms**: For any reuse or distribution, you must make clear to others the terms of this work. The best way to do this is with a link to the web page containing this document.

▪ **When adapting**: Please share improvements to the tool back with us so that we may learn and improve our materials as well.
CONTACT US

Please send any suggestions, feedback, or questions regarding this research data security self-assessment to regulatory@catalyst.harvard.edu and visit the Data Protection Subcommittee page here.

ACKNOWLEDGMENTS

We would like to thank The Harvard Catalyst Data Protection and Privacy Subcommittee of The Harvard Catalyst Regulatory Foundations, Ethics, and Law Program for their contributions and review.

CORE WRITING GROUP

We would like to thank and acknowledge the core writing team of The Regulatory Foundations, Ethics, and Law Program whose writing and editing made this document possible.

<table>
<thead>
<tr>
<th>Name</th>
<th>Company/Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gina Prochilo-Cawston</td>
<td>Beth Israel Deaconess Medical Center</td>
</tr>
<tr>
<td>Joanna Myerson</td>
<td>Harvard Catalyst</td>
</tr>
<tr>
<td>Sabune Winkler</td>
<td>Harvard Catalyst</td>
</tr>
<tr>
<td>Liz Witte, Editor</td>
<td>Harvard Catalyst</td>
</tr>
</tbody>
</table>