

# Data Security Levels - Research Data Examples Quick Reference Guide

CLASSIFICATION				
IRB Determined as Non-Sensitive		IRB-Determined as Sensitive		
<b>L1 = Public</b> Publicly available and unrestricted data	<b>L2</b> Unpublished non-sensitive research data, whether identifiable or not. Active research at Harvard is at least L2 until published.	<b>L3</b> Some regulated data, or data that could be damaging to the subject's financial standing, career or economic prospects, personal relationships, insurability, reputation, or be stigmatizing	<b>L4</b> Data that could place the subject at risk of significant criminal or civil liability or data that require stronger security measures per regulation	<b>L5</b> Data that could place the subject at severe risk of harm or data with contractual requirements for exceptional security measures
<b>Examples</b> <ul style="list-style-type: none"> <li>Published research data</li> <li>Data that is publicly available</li> <li>Non-restricted, publicly available datasets (e.g., Behavioral Risk Factor Surveillance System (BRFSS); NHIS: National Health Interview Survey) as long as the following criteria are met:                             <ol style="list-style-type: none"> <li>1) Research will NOT involve merging any of the data sets in such a way that individuals might be identified;</li> <li>2) Researcher will NOT enhance the public data set with identifiable, or potentially identifiable data</li> </ol> </li> </ul>	<b>Examples</b> <ul style="list-style-type: none"> <li>De-identified data that has yet to be posted to an open-access repository</li> <li>Anonymous surveys (online or in-person w/o the collection of identifiers)</li> <li>Aggregate statistics</li> <li>De-identified biospecimens or genomic data</li> <li>Recipient receipt of coded data where the provider will not release the identifiers to the recipient</li> <li>Research data that is identifiable but is not considered sensitive</li> <li>Non-sensitive surveys, interviews, interventions</li> <li>Non-sensitive MTurk or SONA data</li> <li>Non-sensitive self-reported health history</li> <li>Anthropometric data, Biometric/physiological data (unless associated with sensitive data or diagnosis), MRI/EEG (unless associated with sensitive data or diagnosis)</li> <li>Usability data</li> <li>Non-sensitive audio or video data</li> <li>Private observations recorded with identifiers that are not capturing sensitive information (e.g., interviews in a church setting)</li> </ul>	<b>Examples</b> <ul style="list-style-type: none"> <li>Education records covered by FERPA</li> <li>Employment records, employee performance data</li> <li>Sensitive self-reported health history</li> <li>Constellation of variables, when merged, becomes sensitive</li> <li>Personal or family financial circumstances (record via surveys or interviews)</li> <li>Data collection about controversial, stigmatized, embarrassing behaviors (e.g., infidelity, divorce, racist attitudes)</li> <li>U.S. prisoner administrative data that would not cause criminal or civil liability</li> <li>Information about U.S. criminal conduct that, if disclosed, could damage the subject's reputation, relationships, or economic prospects<sup>1</sup></li> <li>Other information about U.S. criminal conduct that, if disclosed, would not place the subject at risk of significant criminal punishment (see Level 4)</li> <li>Data sets shared with Harvard under contractual obligation (e.g. corporate NDA, DUA, other contracts at OVPR) at Level 3 controls or with general expectation of confidentiality or data ownership</li> <li><b>Non-US criminal data: PI should consult with Research Compliance or OGC for guidance</b></li> <li><b>GDPR data <u>not</u> reaching level of "extra sensitive"</b> – this includes racial or ethnic origin, political opinions, religious, or philosophical beliefs, trade union membership, sex life or sexual orientation</li> </ul>	<b>Examples</b> <ul style="list-style-type: none"> <li>Government issued identifiers (e.g. Social Security Number, Passport number, driver's license, travel visa, known traveler number)</li> <li>Individually identifiable financial account information (e.g. bank account, credit or debit card numbers)</li> <li>HIPAA-regulated PHI (including 18 identifiers)/ HIPAA-regulated Limited Data Set (even if Not Human Subject Research)<sup>2</sup></li> <li>Information that, if disclosed, could place the subject at risk of significant criminal punishment (e.g., violent crimes, theft and robbery, homicide, sexual assault, drug trafficking, fraud and financial crimes)<sup>3</sup></li> <li>Information that, if disclosed, could put the subject at risk of violent reprisals from the government or other social or political groups</li> <li>Identifiable U.S. prisoner data that could lead to additional criminal or civil liability</li> <li>Individually identifiable genetic information that is not Level 5</li> <li>Data sets shared with Harvard under contractual obligation at Level 4 controls (whether corporate NDA, DUA, other contracts at OVPR)</li> <li><b>GDPR "extra sensitive" data</b> – biometric, genetic, or health information.</li> </ul>	<b>Examples</b> <ul style="list-style-type: none"> <li>Data with implications for national security</li> <li>Certain individually identifiable medical records and genetic information categorized as extremely sensitive.</li> <li>Data that would put subject's life at risk, if disclosed</li> </ul>

**GDPR data sensitivity:** See <https://security.harvard.edu/eu-general-data-protection-regulation-gdpr>

<sup>1</sup>ADVISORY NOTE: This could include past crimes for which the subject has served time but that are not matters of public record or are not known to the subject's family, employer, or local community.

<sup>2</sup>Harvard is a hybrid entity, meaning that only certain divisions (HUHS, HSDM Clinic) are HIPAA covered entities. Each Harvard Investigator is required to comply with all applicable privacy and security policies of the HIPAA-covered entity in which that Investigator, as part of a research protocol, is handling PHI or from which the Investigator is drawing PHI. However, data that leaves the covered entity and is transferred to a non-HIPAA covered entity of Harvard is not considered to be HIPAA regulated data.

<sup>3</sup>ADVISORY NOTE: Investigators should consider the criminal laws applicable to the subject. For example, a subject's abortion history could be Level 4 data if she resides in a jurisdiction that criminalizes abortion; and a subject's political activism may expose the subject to prosecution in certain nations. Investigators should also take into account the likelihood of prosecution, considering, among other factors, how much time has passed, the severity of the conduct in question, and the nature and extent of punishment ordinarily imposed in the jurisdiction. Information about conduct that is punishable by civil or even criminal fines, but not imprisonment, often may not merit Level 4 classification.