### Level 5

**Information that would cause severe harm to individuals or the University if disclosed.**

Level 5 information includes individually identifiable information which if disclosed would create risk of criminal liability, loss of insurability or employability, or severe social, psychological, reputational, financial or other harm to an individual or group. Level 5 includes research information classified as Level 5 by an IRB, Information Covered under HIPAA, FERPA, FISMA, and other regulatory bodies.

**Examples:** Information covered by a regulation or agreement that requires that data be stored or processed in a high security environment and on a computer not connected to the Howard data networks, or to be handled in the same manner as the University’s most sensitive data; certain identifiable medical records and identifiable genetic information categorized as extremely sensitive.

* "Howard Confidential Information." refers to all types of data under Levels 2-5. The higher the data level, the greater the required protection.*

---

### Level 4

**Information that would likely cause serious harm to individuals or the University if disclosed.**

Level 4 information includes High Risk Confidential Information (HRCI), as defined below, and research information classified as Level 4 by an IRB. Level 4 also includes other individually identifiable information which if disclosed would likely cause risk of serious social, psychological, reputational, financial, legal or other harm to an individual or group.

“**High Risk Confidential Information**” means an individual’s name together with any of the following data about that individual: social security number, bank or other financial account numbers, credit or debit card numbers, driver’s license number, passport number, other government-issued identification numbers, biometric data, health and medical information, or data about the individual obtained through a research project.

**Examples:** personal financial or medical** information and information commonly used to establish identity protected by state, federal or foreign privacy laws and regulations, such as law protecting personal information, and not classified in Level 5; genetic information that is not in Level 5; national security information (subject to specific government requirements).

**See note below on HIPAA.**

---

*For more information on Howard’s data security policies, see ________________ To report a data breach, contact your Help Desk.*
# University Data Classification Table

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Level 2</th>
<th>Level 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information that presents a risk of material harm to individuals or the University if disclosed.</strong> &lt;br&gt;Level 3 information includes individually identifiable information which if disclosed could reasonably be expected to be damaging to reputation or to cause legal liability*. Level 3 also includes research information classified as Level 3 by an IRB.</td>
<td><strong>Information the disclosure of which would not ordinarily cause material harm, but which the University has chosen to keep confidential.</strong> &lt;br&gt;Level 2 information includes unpublished research work and intellectual property not in Level 3 or 4. Level 2 also includes information classified as Level 2 by an IRB.</td>
<td><strong>Public information.</strong> &lt;br&gt;Examples: research data that has been de-identified in accordance with applicable rules; published research data; published information about the University; course catalogs; directory information about students who have not requested a FERPA block; faculty and staff directory information.</td>
</tr>
</tbody>
</table>

*See note below on contractual obligations. 
** Howard ‘s Confidential Information policy does not restrict or limit the rights of employees to discuss terms and conditions of their employment, including salary and benefits, with each other or with third parties.

Note on Medical Records and HIPAA: Howard University units or programs that are so-called "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA’s data security rules. As of the effective date of this policy, the covered entities are University Health Sciences and Services, Harvard Dental Services, and certain University benefits plans. Other units or programs may be required to comply with HIPAA data security rules for limited purposes under the terms of specific contracts, such as a business associate agreement. HIPAA rules, when applicable, will take priority over Howard’s data security requirements relating to medical records.

Note on Contractual Obligations: Data use agreements, research consent forms and other contracts under which Howard personnel receive confidential information from outside parties often state specific data use and protection requirements. Howard University personnel working with such information must comply with such requirements. Use of such information must also comply with the applicable Howard data security requirements if the contract calls for lesser levels of protection than the Harvard rules.