Office/Contact: Division of Technology and Security
Source: U.S. Department of Commerce, Bureau of Industry and Security, Export Administration Regulations; U.S. Department of State, International Traffic in Arms Regulation; 20 U.S.C. § 1232g, 34 CFR Part 99, and amendments thereto; 42 U.S.C. § 1320d – 6, 45 CFR Part 160 and Subparts A & E of Part 164
Link: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear; https://www.pmddtc.state.gov/

4. Foreign visa number,
5. Tax information,
6. Credit reports,
7. Anything that can be used to facilitate identity theft (e.g., mother's maiden name),

ii. Statutorily protected data, including;
    1. FERPA-protected information (e.g., student information and grades),
    2. HIPAA-protected information (e.g., health, medical, or psychological information),
    3. Export Controlled information,
    4. Other data required to be protected by statute or regulation,

iii. University restricted data;

iv. Human subjects research data;

v. Passwords;

vi. Data required to be protected by contract.

f. The University's key length requirements will be reviewed annually by the Division of Technology and Security and upgraded as technology allows.

g. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by