THE UNIVERSITY OF UTAH®

**Title:** Sanctions Matrix Guidelines
**Number:** G4-004S
**Responsible Office:** Information Security and Privacy Office (ISPO)
**Last Revision:** January 2011
**Owner:** Director, ISPO. 801-587-9241 it_policy@utah.edu

I. OVERVIEW

A. This guideline is meant to provide procedures, standards, and other guidance for the implementation of University Policy 4-004: The University of Utah Information Security Policy – Section S: Sanctions and Violations.

II. GUIDELINES

A. In an effort to assign a more appropriate severity of sanction to the level of severity of a violation, the Information Security and Privacy Office has developed this 3-tiered system of sanctions. This was accomplished after much research and consideration of models of sanction from other academic institutions. The model presented here does not mandate a particular penalty; rather, it allows the supervisor and Human Resource specialist for Staff and Non-Faculty Academic Employees (or cognizant authority for Faculty or Students) to choose from an appropriate menu of options.

B. The Information Security and Privacy Office has submitted the matrix to leadership as recommended tiered guidance for imposing sanctions for confirmed privacy and security violations.

C. The guidance should be not be used as a hard and fast rule, it merely provides some structure for case-by-case decision makers to work with as the totality of circumstances must be considered, and decisions must be made within the framework of all applicable University Regulations (including the Student Code 6-400 for actions involving students, and the Faculty Code 6-316 for actions involving Faculty).

**University of Utah Health Sciences**
**Information Privacy Sanctions Matrix**
**Actions in Response to Privacy & Security Violations**

| Level of Violation | Cause or Motivation | Type of Violation | Examples of Violations | Recommended Actions (one or more) |
|---|---|---|---|---|
| **Level I**<br>Errors in handling restricted or sensitive information or in maintaining security measures | • Unintentional<br>• Lack of training<br>• Inexperience<br>• Poor judgment; mistakes made while operating in good faith<br>• Poor process | • Clerical Error<br>• Process Error<br>• Technical Error<br>• Judgment Error | • Leaving an active computer screen with access to PHI/PII unattended<br>• Leaving PHI/PII, in any format, unattended in public areas.<br>• Disclosing PHI/PII without identity verification<br>• Discussing PHI/PII in public or other inappropriate areas<br>• Sending PHI/PII to wrong postal, FAX, or e-mail address<br>• Theft after appropriate safeguards implemented | • Letter of expectations, including provisions for mitigation, if appropriate<br>• Inclusion of expectations/mitigation steps on performance evaluation<br>• Repeat of Privacy & Security training<br>• Discussion of policy and procedures<br>• Verbal warning or oral reprimand<br>• New Confidentiality Agreement signed |
| **Level II A** | • Intentional, but non-malicious<br>• Curiosity<br>• Concern<br>• Compassion | • Unauthorized<br>• Non-job related | • Accessing the electronic medical record (not MyChart) of family member/friend without a job-related need-to-know<br>• Accessing PHI of patient no longer in your care<br>• E-mail forwarding<br>• Password sharing<br>• Disclosing diagnosis to family member or friend without giving patient opportunity to object<br>• Transmission/storage of PHI in unsecure manner<br>• Transmission of excessive amounts of data, but not breach<br>• Failure to implement appropriate safeguards for electronic PHI/PII.<br>• Improper disposal of paper PHI (trash bin v shredder) | • Written warning |

| | | | | |
|---|---|---|---|---|
| | | | • Failure to complete required Security and Privacy Training and/or to sign appropriate Confidentiality Agreements<br>• Failure to report a security or privacy violation<br>• Failure to establish a Business Associate Agreement<br>• Installing unauthorized software with potential to harm University systems<br>• Repeat or egregious commission of Level I Violation | |
| **Level II B**<br>Breach in the terms of the Confidentiality Agreement and/or University policies concerning use and disclosure of restricted or sensitive information or in maintaining security measures. | • Intentional, but non-malicious<br>• Curiosity<br>• Concern<br>• Compassion<br>• Carelessness<br>• Compulsiveness | • Unauthorized<br>• Disrespect for co-workers, supervisor, and patients<br>• Non-job related<br>• Stealth | • Disregard of University Policy and Procedure resulting in a breach of confidential, restricted, or sensitive information.<br>• Violation of policy to the extent that organizational harm may result.<br>• Loss of unencrypted portable device due to carelessness or negligence<br>• Failure to properly dispose of paper and electronic media appropriately.<br>• Failure to encrypt devices used for University business<br>• Downloading PHI to unencrypted storage device<br>• Transmission of excessive amounts of data resulting in breach<br>• Unauthorized access of record of co-workers without a professional need-to-know<br>• Unauthorized use, access, or disclosure with no known re-disclosure<br>• Disclosure of confidential information to co-workers with no job-related need to know<br>• Using someone else's computer account | • Any Level I or Action PLUS:<br>• Final written warning, requiring written corrective action plan (for faculty, referral to Dept. Chair, UUHC Medical Director and CMIO for review of violation)<br>• Suspension of information system user privileges<br>• Suspension of employment<br>• Suspension of research projects<br>• Inability to participate in research for up to 12 months.<br>• Letter of reprimand, requiring written corrective action plan and acknowledgement of consequences of subsequent infractions; e.g., expulsion, and obligation to make restitution, as appropriate<br>• Temporary loss of University privileges<br>• Contract of restitution |

| | | | | |
|---|---|---|---|---|
| | | | • Adding, deleting, or altering electronic information without authorization<br>• Taking an identifiable photograph of a patient against policy<br>• Posting any personally identifiable form of PHI on social media that poses harm to the University or the subject of the post<br>• Failure to follow Special Restriction for Out-of-Pocket Payment for Services<br>• Repeat or egregious commission of Level I or IIA violation | |
| **Level III**<br>Breach in the terms of the Confidentiality Agreement and/or University Policies concerning use and disclosure of restricted or sensitive information, for personal gain or to affect harm on another person | • Malicious intent<br>• Personal gain<br>• Financial gain<br>• Revenge<br>• Protest<br>• Gross negligence | • Theft, including identity theft<br>• Malicious actions: e.g., alteration or deletion of data; making systems inaccessible | • Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person<br>• Unauthorized access of celebrity or VIP PHI/PII for any reason<br>• Malicious alteration, deletion or removal of PHI/PII, from University facilities<br>• Unauthorized publication or broadcasting of PHI/PII<br>• Use or disclosure of PHI for illegal purposes<br>• A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline<br>• Repeated Level I or II Violations | • Suspension of employment<br>• Suspension of research projects<br>• Termination of information system user privileges<br>• Referral to VP as violation of faculty code<br>• Revocation of Medical Staff privileges<br>• Termination of employment; ineligible for rehire and future information systems access<br>• Expulsion without opportunity to continue at the University of Utah in any status, and ineligible for University privileges<br>• Contract of restitution |