JOHNS HOPKINS PERSONALLY IDENTIFIABLE INFORMATION POLICY IMPLEMENTATION/ENFORCEMENT PLAN

Background

The proposed Personally Identifiable Information Policy ("PII Policy") is a collaborative effort between the University and Health System to ensure policy coverage for the protection of sensitive and confidential personal information throughout the institutions. There are a number of institutional policies that cover elements of PII, and this policy does not supplant those. It is designed to fill perceived or actual policy gaps, assist individuals and organizations in characterizing types of PII, provide a set of guidelines for assessing the risk associated with handling and storing PII, and identify practices that set the institution's expectations.

Data Privacy and Protection Program

This policy is unusual in that its implementation in many ways precedes its drafting. It is principally a work product and objective of the University's Data Privacy and Protection Program ("DP3"). In March 2014, the University initiated the DP3 under the leadership of the Chief Risk Officer and Chief Information Officer. The DP3 instituted several reforms, including drafting appropriate policy. There was, however, no need to wait for the completion of a policy-drafting process to begin making substantial efforts in privacy protection.

One of the first actions taken was the establishment of a group of representatives from University divisions and departments under the name Privacy Liaisons ("PL's"). The role of these Privacy Liaisons was modeled on a pre-existing group covering the same organizations, the Security Liaisons. The principal difference is that Security Liaisons are principally concerned with information technology protection, including but not exclusively privacy, whereas the Privacy Liaisons are concerned specifically with privacy, but more broadly than simply IT and thus including business operations, physical documents, and individual and organizational behaviors. The PL's are drawn from institutional leadership and serve as the organizational watchdogs for privacy risks and practices.

Privacy Liaisons and Policy Implementation

The implementation and operational surveillance of compliance with the PII Policy is largely in the hands of the PL's, with support and guidance from Human Resources, Finance, OHIA, JHU General Counsel, IT@JH, and Risk Management (along with other relevant institutional entities such as the IRBs). The PL's have completed first-phase security plans and inventories, reported back progress to the larger group, and documented progress according to the DP3 charter.

The PL's are currently working on educational materials and methods for awareness and education using current materials, policies and the proposed PII Policy. While most divisions and departments have already delivered awareness and training to their staffs, it is important to distill the PII Policy and best practices into coherent communications across divisions.

The next phase of the DP3 implementation will be to follow-up on previous inventory and planning work, by implementing a close peer review process. We intend to identify and prioritize the entities with the highest inherent data privacy risks, create a risk assessment rubric (based on the PII Policy), and review and report-out on each entity's status. In order to do so, we will divide the PL's into groups of three or four to conduct the peer reviews, with a schedule that results in each entity being reviewed at least once every three years. The focus will be on identifying risk areas, effective implementation of the PII Policy, gaps, and corrective actions. Each small group will provide a detailed report-out to the entire PL group. This program of continuous peer review reflects the close relationship between privacy protection and effective organizational operation. It is critical that privacy protection not be reduced to simple box-checking, and the organizations in best position to identify gaps and response are peers facing many of the same issues.

In addition, the Security Liaisons will continue their practice of completing security documentation developed by the Chief Information Security Officer and the Office of Hopkins Internal Audits ("OHIA") every three years for general information security controls. These documents are meant to streamline internal audits and provide some audit coverage for those departments that have not undertaken an audit.

In addition, the PII Policy will become a template for OHIA when conducting organizational audits and translate into best practices, many of which are already included in audits but not necessarily with clear attribution.

Enforcement

In the proposed PII Policy, divisional, entity, and departmental leadership are provided explicit authority to enforce the data handling practices discussed therein. By *enforcement*, we mean a combination of surveillance and detection of non-compliance with the Policy, the identification and implementation of individual- and organizational-level corrective actions, and (where appropriate) the imposition of sanctions.

In this regard, it is important to note that the PII Policy requires that divergence from the practices described therein must be evaluated and documented at a leadership level. This implies that the practices as described set the Policy's expectation, and that compliance is benchmarked against those practices.

Incident Response

The PII Policy does not change the current process for rapidly responding to incidents, communicating to stakeholders and the community as a whole and violation remediation processes. Privacy violations will be handled by the appropriate legal and/or compliance office, with strong input from Risk Management, IT@JH, divisional and University leadership, and other stakeholders.

The principal change from current practice will again involve the Privacy Liaisons. For any substantial University breach in privacy, a sub-group of the PL's will be convened after the

incident in order to conduct a “Lessons Learned” review. It would not normally necessitate a full-blown investigation, but would require that the any involved PL work with a group of her peers to identify risk areas and remediation steps that could be generalized to the larger community. The Lessons Learned review will be reported out to the larger PL group.