UNIVERSITY OF MINNESOTA

Employee Self-Service | Policies | Forms | OHR Directory

Office of Human Resources

Employment | Benefits | Training & Development | Compensation | Employee Relations | Work/Life & Wellness | Manager's Toolkit

Home > Training & Development > Leadership > President's Emerging Leaders Program > Leadership Projects

WHAT'S INSIDE

About the Program

Participant Profiles

Leadership Projects

Apply to the Program

President's Emerging Leaders Program

Dave Dorman, Coordinator

200 Donhowe Building
319 15th Avenue S.E.
Minneapolis, MN 55455-0106

612-626-0561
612-625-2574 (fax)

dorma001@umn.edu

Search OHR

Go

HIPAA and Research

Sponsors:
Steve Cawley, University Chief Information Officer
Terry Bock, Associate Vice President and Chief of Staff of Health Sciences

Overview of the Project

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains provisions that have significant implications for University researchers who use health information in their research. The HIPAA Privacy Rule, effective April of 2003, defined the types of organizations that are subject to HIPAA and the concept of Protected Health Information (PHI). The Privacy Rule specified that PHI could be used, created, or disclosed for research purposes only if authorized by a signed authorization, or waiver of that authorization by an Institutional Review Board or Privacy Board. The HIPAA Security Rule, effective April 2005, defines electronic PHI and establishes required and addressable administrative, physical, and technical safeguards that must be implemented to protect the privacy and confidentiality of PHI in electronic format.

Most research data is maintained locally by investigators using a variety of technologies that may range from Personal Digital Assistants and laptop computers to multi-user shared data repositories. The use of personal workstations running simple single-user database or spreadsheet programs is common in research settings. Compliance with the Security Rule for these types of systems will vary widely depending on the data and how it is created, used, shared, or stored. As a practical matter, many researchers may not possess the skill set or have the resources to fully implement the safeguards required by HIPAA. Information technology groups that do possess the requisite skills may have limited resources to support the hundreds of researchers who work with health data. In addition, some widely used computer technologies are not compliant with the Security Rule. Examples include workstations with no login security (e.g., Windows98) and data management and analysis applications used to store PHI that have no ability to generate audit trails. A common example would be the use of Excel spreadsheets containing ePHI, for which there is no technical capability to generate an audit trail, which is one of the required Technical Safeguards.

There are know compliance risks associated with health data and many common security needs in research. The University needs to develop a strategic response to the challenges of securing private data in research. The response needs to allow for the various and important needs for access to and sharing of research data while ensuring that the data is safeguarded in a method that meets compliance requirements and institutional expectations.

Project Goals

Specific strategic questions include:

- What systems, policies, and procedures are in place or needed to ensure the security of protected health data in research?
- What is an appropriate balance between research needs for access to private data and the mechanisms used to safeguard data?
- What security standards for use and transmission of ePHI for research are in place or need to be established to ensure the security of ePHI in University servers, networks, and databases?
- How do we identify, develop, and implement strategic initiatives that overcome traditional barriers and generate changes in organizational dynamics and are truly transformative (i.e., culture change)?

- How can we document the efforts here to develop a model for other enterprise projects that include culture change as an initiative outcome?
- How do we develop and engage the University's leadership to support this initiative in a way that will provide for leveraging institutional assets and the mobilization of required additional human and technical resources?
- How do we identify and develop useful data management models for researchers?
- What is the process for identifying projects with ePHI, the security requirements, and the method for securing the data?

The goals of this initiative would include:

1. Interpreting and addressing federal requirements for data security and identifying when data security safeguards are required.
2. Identifying the need for technical resources for researchers.
3. Developing data security resources and information for our investigators.
4. Enhancing the institution's culture with regard to data privacy and security and the institution's culture of regulatory compliance.
5. Establishing expectations security compliance and practices.
6. Develop strategies, recommendations, and materials for implementing this initiative.
7. Identifying and developing opportunities to leverage existing resources for education and outreach efforts.

Specific tactics or project tasks might include:

- Data security research and information gathering. Where is our private/protected data? What regulations are involved? What are other institutions like us doing? Academic Health Centers, large research universities?
- Identify work already done regarding the goals of this initiative and develop a plan for leveraging the work.
- Interview/meet with business process owners and administrative staff to develop the requirements for such an initiative.
- Enterprise project planning.
- Working with experts to develop instructional/educational materials for researcher regarding new processes or security expectations.
- Creating or updating web material and potentially web based tools.
- Work with communications experts to develop messages to be incorporated into a communications plan and implementation of plan components.
- Integrate data security requirements and documentation requirements into the Institutional Review Board's existing application, review, and approval process in a manner that is least costly in terms of time and resources for the investigators.
- Developing an appendix to be used with the existing IRB application that is specific to data security and data management.
- Researching best practices for various data security issues (e.g., using, collecting, sharing).
- Developing data management models based on best practices for data security.
- Designing a process for reviewing and approving data management proposals contained in the proposed new appendix.
- Identify the staff and processes that this initiative will impact and develop an awareness program for the owners and managers of these processes.

Project Team

Proposed Advisory Committee(s): University Research Compliance Committee

Team Lead

Ross Janssen, University Privacy and Security Officer and Director, Office for Occupational Health and Safety

Team Members

Catherine Fejes
Human Resources Consultant
Academic Health Center
612-626-4011
fejes001@umn.edu
Coach: Mary Ann Hennen

Claire Kari
Biosafety Specialist
Environmental Health and Safety
612-626-2145
karix001@umn.edu
Coach: Susan Rafferty

Bryan Rumple
Financial Reporting & Budgetary Analyst
University Services Finance – Project Finance & Accounting
612-625-4037
rumpl001@umn.edu
Coach: Ryan Warren

Jodie Walz
Curator
Digital Collections and Archives
612-624-4080
jwalz@umn.edu
Coach: Amy Lund-Swalley

top

Contact Webmaster | Privacy Statement

The University of Minnesota is an equal opportunity educator and employer.

Last modified October 1, 2007