HIPAA and Research

UNIVERSITY OF MINNESOTA

President's Emerging Leaders Program

2007-2008

Sponsors:

Terry Bock, Associate Vice President & Chief of Staff
Academic Health Center

Steve Cawley, Vice President & University Chief Information Officer
Office of Information Technology

Project Advisor:

Ross Janssen, Director
University Privacy & Security Project
And Office of Occupational Health & Safety

Project Team:

Cathy Fejes, Human Resources Consultant
Academic Health Center

Claire Kari, Environmental Health Specialist
Office of Environmental Health & Safety

Bryan Rumple, Principal Accountant
University Services – Finance

Jodie Walz Double, Director/Curator
College of Design, Digital Collections & Archives
Academic Resources Unit

June 30, 2008

HIPAA and Research

TABLE OF CONTENTS

ATTACHMENTS

HIPAA and RESEARCH

EXECUTIVE SUMMARY

"The mission of the University of Minnesota is deeply connected to the conduct of research. It is of critical importance to the reputation and future of this institution that we remain committed to the highest standards of research integrity in all work conducted in our institution."
- University President Robert H. Bruininks

In the fall of 2007 our President's Emerging Leaders (PEL) group was charged with looking into the issue of data security for human subject research involving electronic Protected Health Information (ePHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA). The University has the goal of being one of the top three public research institutions in the world. This project helps to work towards that goal by seeking to improve the utilization, storage, and transfer of ePHI in Human Subject Research; works towards compliance with HIPAA and related laws; assists researchers and staff conduct their work in ways that ensure the security of the subject's private information.

During the course of our project we interviewed key internal University stakeholders, and people involved with either Information Technology or Human Subject research at selected peer institutions. We reviewed the HIPAA incident log which goes back to 2003. From the interviews and the incident log we drafted a root cause analysis. Our recommendations are a result of all the information we obtained, but were primarily informed by the themes that were so often brought up during the course of the internal interviews.

"Money is not the first answer to this problem."
- U of M researcher & administrator

We repeatedly heard that there are varying levels of computer sophistication among PI's and their staff. Even if they have the time and knowledge, their efforts are best directed at conducting and analyzing research, and not in keeping up with the latest technological challenges of computer security. Money is an issue as most grants do not provide funds for computer equipment or software, or professional IT staff. We heard from our peers that they are all wrestling with the same issues – constantly-evolving technology, limited dollars, increased collaboration and sharing, restrictions of grant funding, and a culture of independence among faculty. Some peers are also dealing with state laws that place greater requirements and restrictions on private health data than do HIPAA, Minnesota law, or NIH requirements.

Based on our analysis, we recommend the following:

1. Adding an **appendix to the Institutional Review Board (IRB) approval process** that specifically inquires about the data security practices for research involving human subjects. We recommend for this review to be completed and routed electronically. All research involving human subjects must be approved by the IRB. Some of the current IRB questions inquire about practices for monitoring research data to minimize physical risks to the subjects. Our proposal deals solely with the security of the electronic data. A new panel comprised of Information Technology (IT) and research experts would review the appendix. They would be able to follow-up with the Principal Investigator (PI) to either directly help him or her with improving their data security practices, or would identify local IT resources for that purpose. The panel would evaluate the security practices on a research project and determine if it "meets standards" or "does not meet standards". Ideally, this Data Security Review (DSR) would occur prior to when the rest of the IRB application was submitted. That would provide sufficient time to address any needed improvements, and need not hold up the IRB approval. The panel would keep a log or record of the type of security assistance addressed, or a database would capture information if the appendix is submitted electronically. This information would provide administrators with hard data that could be used to allocate IT/security related resources in a focused and efficient manner. We strongly recommend that the infrastructure of the DSR panel, and more importantly the available IT staff to actually follow-up, advise, and help implement are in place before this appendix and subsequent DSR are actually required as part of IRB approval. We cannot recommend an un-resourced and un-funded mandate.

2. Implementating a **web-based resource (web-board)** where researchers can ask questions related to data security of ePHI, and also search past questions and answers in a knowledge base format. This web-board would be monitored and answered by an information technology group similar to the one conducting the DSR. The working title for the web-board is askIT. The questions and responses would be posted on the web-board (without attribution), which would be grouped by topic and could be searched by keyword. Over time this accumulated question-and-answer exchange would create a resource for researchers. This information could also be used to identify issues for which training would be helpful. This tool should have the ability to create reports on volume and type of question. As with our Recommendation #1 this information would provide administrators with hard data on the security issues facing researchers, and would indicate the extent and type of enterprise resources that should be allocated. We can use technology to address technology.

3. Rolling out a robust **awareness and marketing campaign** as part of launching both the DSR and the web-board. The campaign should emphasize that the purpose of both the DSR and the web-board is to help researchers protect the security of their ePHI. They won't be expected to spend so much of their time and energies figuring out computer technology. They won't have to guess if their research data is as secure as it could be. They will now have someone

contacting them to offer help on computer security, and someone who can make recommendations based on their specific needs.

> "You enhance compliance by making it as simple as possible."
> *- U of M administrator*

The challenges posed by computers and related technology are always changing and multiplying. The challenges are often unforeseeable and therefore difficult to plan for. Both the DSR and the web-board will allow the University to be extremely responsive as new technology, and their attendant challenges, are presented. The information gathered will inform future decisions. We think that in the not too distant future all research universities will be required to put more security structures into place. If we start addressing this now it will likely be easier and less costly than it will be to start years from now.

None of the peer institutions we spoke with have the kind of partnership between human subject research and information technology as we are proposing. If successfully implemented, our recommendations could become a model and may be used to attract and retain world-class researchers. This is an opportunity for the University to provide leadership in academic research. Providing proactive and customer service-oriented IT assistance in the area of research data security can help move the University to its strategic goal of becoming one of the top three public research institutions in the world.

On a broader scale, successful implementation of this security review could have practical applications well beyond health data in research. All manner of research should receive the utmost security because of the programmatic, financial, and reputational risks of not doing so. But we also collect and use private and sensitive data for non-research purposes all across the University. The DSR could become a model for efficient, effective, and welcomed compliance assistance.

INTERVIEW THEMES

UNIVERSITY OF MINNESOTA INTERVIEWS

METHODOLOGY

During the course of the FY08 PEL year our project team conducted interviews with thirty-six individuals whose work encompasses various aspects of HIPAA, ePHI, research, or data security. The team interviewed faculty/principal investigators, key senior administrators, Associate Deans, research staff, and IT professionals across several sectors of the University and across colleges. We also spoke with those who work in the areas of compliance, legal, and research-related services.

Questions for each interviewee and/or group were tailored to their particular role in research-related ePHI and data security. We inquired about the successes, challenges, needs, and resources as seen from their perspectives. The interviews were intended to gather general information, opinions, and best practices, and were not intended to be surveys with any statistical relevance.

Despite having different interview questions for each interview, several themes started to emerge fairly quickly. At times opinions directly contradicted one another, but fairly clear ideas were articulated over and over again.

The following illustrates ten themes that we identified during the interview process. This list reflects their frequency. Additionally, we have included select minority viewpoints at the end because we felt they have particular insights. The interviews are also presented in a different format in Attachment B of this report. We have removed the names of the interviewees so as not to directly ascribe an idea to any individual.

THE TEN THEMES IDENTIFIED ARE:

1. ***There needs to be information on HOW to comply, and not just what to comply <u>on</u>.***
2. ***The behavior of individuals and/or human error poses significant risks.***
3. ***Some 'centralization' of IT/security would be good, but it's important for a PI to be able to provide their own resources.***
4. ***It is not the role of the IRB to assess security issues.***
5. ***PI's often do not have expertise in technology or security.***
6. ***There should be more assistance in advising on, or reviewing, security plans.***
7. ***There should be specific risk assessments made as to the level of security actually needed.***
8. ***The future of research involves an increasing level of sharing and collaboration.***

9. ***Most grants do not pay for computer equipment, upgrades, or IT personnel.***

10. ***For any changes to policy, additional compliance, or systems changes, it's important to the success of those initiatives to demonstrate how it can make the work of research easier, and/or take minimal time and expense.***

INTERVIEW THEMES EXPANDED

(1) There needs to be information on HOW to comply, and not just what to comply <u>on</u>.
People at the U of M believe we have very good training and awareness about what one needs to do, but little guidance or suggestions on <u>how</u> to do it. As an example, one is informed that performing data back-ups is considered a standard but there is no clear place to learn about a range of good options for how to do that. Our interviewees often do not know of clearly identified resources for asking those kinds of specific questions. There is a requirement to encrypt, but people too often end up determining the best way to do that on their own.

(2) The behavior of individuals and/or human error poses significant risks.
There is acknowledgement that despite having gone through training and "knowing better" there are still instances of people not using cable locks on their laptops, not encrypting laptops, not performing secure back-ups, etc. People place private information onto easily transportable devices such as thumb drives (and don't secure them) out of convenience. As devices get increasingly varied and small, the future security challenges related to human behavior can only be guessed at. In many ways we are better able to solve the issue of making networks secure and having strong system authentications in place, even as we become more vulnerable to someone leaving an unencrypted laptop in their car when stopping for dinner on the way home.

(3) Some 'centralization' of IT/security would be good, but it's important for a PI to be able to provide their own, equally sufficient and secure, resources.
The notion that "one size fits all" when it comes to research needs just won't work for implementation and compliance to be successful. While many feel that each PI shouldn't have to figure out IT issues all on their own, we also heard that resources should not be mandatory. If a PI can demonstrate that they will provide sufficient services and protections using an alternative security plan, they should be able to do so. This opting out will also help foster those who will successfully innovate and help to bring about practices that may one day be commonplace.

We left 'centralization' without a specific definition as it could mean different things to different people. It could mean University-wide, college-wide, or other variation. Basically, it's some alternative to having every PI being on his or her own. It's interesting to note that none of our interview questions directly asked about centralization of IT/security, and that this frequently-expressed opinion was brought up by many of the interviewees.

(4) It is not the role of the IRB to assess security issues.
The IRB is a good focal point since most, if not all, research involving ePHI would at some point submit a proposal through the IRB. But none of the interviewees thought the IRB has the actual role to assist on technology and security matters. There currently are questions on the IRB proposal form(s) that address security issues for which the PI must self-report, but the IRB makes no assessment or verification for these matters. Some of the current IRB appendices inquire about PHI or data, but not to a degree that security is addressed. There currently are questions about 'data

safety monitoring', but this relates to monitoring research data for the purpose of ensuring minimal risk to human subjects. This does not address the security of the ePHI.

It was suggested several times over that a separate review committee (or panel) of IT security experts should be reviewing these protocols in order to ensure that the PI 's know how to undertake data security, and also for the panel to be a point of contact for questions.

(5) PI's often do not have expertise in technology or security.
It's seldom that a faculty member will have the requisite expertise in technology and security to be able to determine the best solution to their needs. Varying levels of overall computer sophistication make for inconsistent application of security standards. And even if researchers did have strong computer skills there are many competing interests for their time and attention.

The speed of technological change and the attendant security challenges keeps increasing. New challenges continually emerge while the old ones still remain. Successfully keeping up with this requires a significant investment in time. As part of the University's goal to be among the top three public research institutions, it's important to allow PI's to focus on their research, and not spend time determining the best way to encrypt and store data.

(6) There should be more assistance in advising on, or reviewing, security plans.
What assistance people get, they need to take the initiative to seek out. It's usually not clear who they need to contact. Oftentimes faculty members don't even know the right questions to ask. Sometimes IT staffs aren't really knowledgeable about how research needs may be unique from other technology uses. IT will sometimes solve a problem taking a solely IT-centric approach and not be customer-service oriented. Many people brought up a need to have IT staff competent in the specific areas of security and research.

(7) There should be specific risk assessments made as to the level of security actually needed.
PI's are concerned about being constrained by security measures their research data may not in fact warrant. There should be some consideration of varying levels of access related to the roles and authorizations different positions may have. Over-protecting can have significant negative impact, and may lead to work-arounds that could actually create security issues. Assessments would also help to ensure that the most sensitive data receives the most expansive security measures.

(8) The future of research involves an increasing level of sharing and collaboration.
This was mentioned fairly often and illustrates the need that whatever security or privacy components are in place, they need to be flexible enough to provide for the sharing and exchanging of research information to appropriate parties around the world and at all hours of the day. Any practices the University adopts should help foster world-class research, not impede it.

(9) Most grants do not pay for computer equipment, upgrades, or IT personnel.
It is very difficult to obtain external funding for such things, and most grants consider such expenses to be indirect costs. There are of course some exceptions to this, but this was mentioned many times. Some grants will pay for computers or upgrades if they are to be used solely for the work of the grant, but in most cases this is not a workable situation.

(10) For any changes to policy, additional compliance, or systems changes, it's important to the success of any initiative to demonstrate how it can make the work of research easier and/or take minimal time and expense.
Correctly or not, many feel that the details of regulations are hampering their ability to conduct research. There's an impression that policies make things harder, or in some way hinder their ability to conduct research. It would be important to demonstrate that a 'requirement' such as backing up to

a central server, or using a particular database, saves a PI time and money as opposed to doing this all on their own.

Please note that the interviews didn't show an outright aversion to change, but rather that there should be some "selling" to get people to realize it's in their own best interest to make changes.

> "It would be great to say to a researcher, 'You don't need to worry about this because we have.'"
> *- U of M IT professional*

SECONDARY THEMES

The interviews did bring up some other topics that while not as prevalent as those mentioned above, are nonetheless noteworthy as they were mentioned enough times to reflect sub-themes:

The issue of **accountability** was brought up during many of the interviews. Several people spoke about a lack of holding people accountable for taking adequate steps to prevent security violations. A couple said that faculty in administrative roles - Deans, or Department Heads - ought to take a more proactive role in encouraging their researchers to enact all appropriate practices. Some mentioned that PI's need to hold their research staff accountable for properly following security practices. A few said that the specter of getting your name in the paper ought to be enough incentive to make people do the right thing.

One person said it was the collegial duty of researchers to ensure that ePHI is handled securely as all researchers rely on the public's trust and willing involvement to be able to conduct their research. This was echoed by someone else who said that negative news reports hurt all clinical researchers. Some people said there was a culture of autonomy but that researchers do in fact have responsibilities to their fellow researchers and to the organization as a whole.

Those who demonstrate sound security practices could be **acknowledged** and asked to present and share information at new faculty orientations, department meetings, or faculty symposiums, allowing them to share their best practices to help elevate others' practices. Successful innovators should receive acknowledgement and encouragement.

Several people said the availability and service levels of **IT support** across the University is uneven.

Several people spoke of the **uncertainties** of HIPAA compliance - Is the PI or the institution responsible for being able to provide to a research subject a list of all those with whom their protected data has been shared for the previous six years? There is no ONE understanding of HIPAA. Interpretations of HIPAA vary between geographic regions, and between institutions.

A couple of people said that the **compliance** bar was too low and that having a bar based on ethics is actually higher, and is what we should be aiming towards.

Increasingly, people are becoming aware of the full **scope** and complexity of sound security plans. People realize the importance of having disaster-recovery plans along with the more immediate needs of securing laptops and performing routine backups.

The issue of changing **old habits** came up frequently. Some people said that researchers often don't realize how expensive and time-consuming their current practices are - it's just that they're used to doing it that way. The status quo is strong. Some spoke about Excel being used to record data

because that's a program so many people already know how to use, even though the tracking and reporting capabilities of that software are very poor.

There was a good deal of **praise** for the current HIPAA and security training at the U. We have a very good system for getting people trained, with consequences if the training is not completed. The HIPAA Steering Committee has the right people at the table. The Academic Health Center (AHC) has taken a strong stance on mandatory encryption, centralized IT support, and the use of Active Directory.

Some people spoke of **ever-evolving** security standards and security challenges. FISMA-level security (from the Federal Information Security Management Act) may well become the new minimum standards. The current nineteen HIPAA identifiers could become a different, expanded list. Wireless computing is increasingly easy and convenient. And the new super-thin Apple laptop doesn't even have room for a traditional security cable lock.

There exists a **culture** where researchers want to control their data, and using systems that seem to take decisions out of their control goes against this culture. There have been several instances where 'centralized' IT units have made decisions about no longer supporting certain machines or computer applications, leaving the researchers "high and dry". So there needs to be a long-term commitment to any centralized assistance. Also, the current highly autonomous research culture should come to a greater acceptance of the shared responsibility for conducting secure research at a public university.

Several people spoke of how a more robust enterprise approach to computer security can help enable the University to reach its goal of becoming one of the **top three public research universities** in the world. Such institutional resources would also help to attract and retain top research faculty. Being able to promote a strong and effective research infrastructure that allows researchers to give their time and attention to their research would help to set us apart from other distinguished universities.

PEER INTERVIEWS

We contacted selected peer institutions across the country and asked them several questions The list of institutions, as well as the questions, is on Attachment B of this report.

We spoke with either IT professionals or administrators involved in human subject research. In contacting individuals to request an interview we stated the purpose of our project and the questions we wanted to ask. We requested if they weren't in a good position to answer the questions to please suggest the name of someone else.

Everyone we spoke with shared their information readily, but all were apprehensive about a report that would identify their institution's particular shortcomings. Therefore our report is sensitive to this.

As in our internal interviews, we soon heard our peers repeat each other. Their internal review boards (either IRB or Privacy Board) did not really address the issue of data and computer security. They don't have enterprise-wide or otherwise strong central IT support. They have the same funding challenges we have. They obviously all realize it's a big concern, and a couple had experienced security incidents that were publicly embarrassing and costly. They've all had internal discussions about how to address this, but to date they're all operating with practices that pre-date the prevalent use of laptops. One IT professional stated that his organization has drafted plans for more expansive system-wide security support and greater oversight on security compliance. But as those drafts were

being “run up the ladder” for administrative approval, their Vice President of Research left two years ago, “and the ladder broke”. Those drafts are still stalled.

Basically, none of the peers we spoke with currently have practices which are as helpful to researchers as what we’re proposing.

We see this as an opportunity for the University of Minnesota to take a leadership position and be progressive and innovative in the way we support researchers.

> “Oftentimes research staff don’t know what they don’t know.”
> *- research administrator at a peer institution, discussing computer security*

NEW IRB APPENDIX

There already exists strong awareness and compliance that clinical research involving human subjects must receive approval by the IRB. We heard in the internal interviews that the IRB does not have a role in the *assessment* of computer security. Their legal responsibility and expertise lies in other areas of research. But as the goal is to review security practices for research that is likely to involve ePHI, we suggest tapping into this firmly established IRB process to gather security information. This too is the best avenue in which to offer proactive assistance to all researchers who utilize ePHI.

While the scope of the IRB does not involve data security per se, they already have responsibility for ensuring compliance with some aspects of HIPAA. By taking the new appendix into consideration as part of their approval, the IRB is strengthening that connection to HIPAA compliance, and helping to ensure the protection of research participant's protected health information.

We are recommending that a panel be convened, staffed with IT professionals, and those who are familiar with research and its oftentimes unique security needs and challenges. The panel will operate out of the Office of Privacy & Security. Their work will start with the new appendix, which we have tentatively entitled **Appendix S**. The subsequent review and assistance process that follows receipt of the appendix is being called the **Data Security Review (DSR).** Upon completion of the DSR the panel will make a determination as to whether or not the security practices meet standards. This determination will be considered by the IRB as part of the approval process.

We are presenting Appendix S as a DRAFT. Our draft still needs more review, and approvals, before being implemented. We are recommending that usability testing be performed before roll-out, and the form could also change based on that feedback.

We recommend for the appendix to be submitted electronically. We know that the IRB application process is not currently electronic. Electronic submission would also help enable a database to track which aspects of data security require the most assistance. But electronic appendix submission or no, we are recommending that a database be created to track the new appendix. This information will help to identify a possible need for more dedicated IT resources, and the detailed information can help to direct resources to have the most influence for the time and money.

Ideally, the appendix should be submitted to the IRB/security panel prior to the rest of the IRB application, in order to allow sufficient time to make any changes that are indicated without holding up the overall IRB approval

The first part of the appendix helps to ensure compliance with the required HIPAA and security training. If this appendix is online, it can be linked to PeopleSoft information and an individual’s training record. The online form will be pre-populated with as much information as it can, particularly to the existing training tracking system. We’ve included links that can direct PI's to pertinent policies, standards, and information. The bulk of the application asks questions that try to strike a balance between not wanting to add an excessive burden to the already compliance-heavy research environment, but which also provides the DSR panel with sufficient information. We believe the appendix

questions ought to be able to be answered without undue difficulty or time. In return for these efforts, a researcher can be assured they doing all they can to conduct compliant and ethical research.

The panel will review the appendix responses and follow-up with PI's as needed. They may just talk on the phone or exchange emails, but they may also ask for a meeting so that they can better understand that researcher's particular needs and existing equipment (software and hardware). The members of the panel may be able to recommend several options to improve security. One of the things that kept coming up in the interviews is that few researchers have IT professionals regularly available to assist them. Many researchers end up trying their best to craft solutions to their own particular needs, and some are more successful at this than others.

Since there is so much follow-through that is out of their control, and security is always subject to human behavior and human error, the IT professionals we talked with were unanimously opposed to having the review result in a determination of "approved" or "certified" or "verified". We have elected to call the panel's determination "meets standards" or "does not meet standards". In practice, a "does not meet standards" determination will only result if the *interactive process* between the panel and the PI fails to reach a suitable solution. A "meets standards" determination could cover those situations where there will be some known security concerns despite everyone's best efforts. Or, the best we can do given the circumstances would not fit any preferred model. There could be outdated software or hardware that is just too cost-prohibitive to upgrade. Such instances should be brought to the attention of responsible administrators. The determinations of the panel will come from the IT staff working with the PI's making recommendations to the whole panel and coming to a group consensus.

It is not the intent of the appendix or the DSR to serve as a "gotcha" and expose security problems. Instead, it seeks to more consistently identify where issues exist and to more systematically have researchers partner with IT professionals to solve those problems.

The issue of workload and time for IT professionals to staff the DSR is an unknown factor. A number of IT areas have said they could provide some time from their existing staffs to serve on the DSR panel and/or monitor the web-board. At this time, we don't recommend that additional IT staff need to be hired, or current staff be re-assigned. It's expected that several security models with applications to many situations will become apparent relatively quickly. And we believe that with some time and experience, a legacy system whereby researchers already have good practices in place, will become clear. Both of these factors, while proven only through experience, would make for an efficient review system.

IRB Use Only
IRB Code #

Appendix S (working title)
Data Security Review
This form must be completed for all human subject research.

This Data Security Review (DSR) will be considered by the IRB as part of the approval process. You're encouraged to complete this form and have your security practices reviewed before submitting the rest of your IRB application. Please plan for sufficient time to address any security issues that may be identified.

Principal Investigator (PI)
U of M x.500 ID (ex. smith001): SET UP SO THIS SECTION AUTOFILLS OFF X.500
Name: (Last name, First name, middle initial)
Phone number:
Pager/cell phone number:
University Department:
Mailing address:
Email:

PROJECT TITLE: (if known):

Person preparing this document	
Name:	Phone number:
Email:	Fax:
University department:	
DATE:	

PLEASE COMPLETE THE FOLLOWING QUESTIONS

1. ☐ **Yes** ☐ **No** Have you completed the Electronic Protected Health Information (ePHI) training? (Click here for link to training.)

Please enter the **X.500** for all current research staff who will have access to ePHI.

eg: johndoe01@umn.edu		

This information will link to the training database to help ensure that all research staff have completed the required training.

2. ☐ **Yes** ☐ **No** Have you reviewed the UMN Data Security Requirements? Click to link to the University's STANDARD—Securing Private Data (Appendix G).

If you are non-compliant with any of the standards in Appendix G, please provide more information:

3. ☐ **Yes** ☐ **No** Will your research have access to ONLY **de-identified data**?

(Click **here** for a list of 19 subject identifiers.)

If you answered "YES", you can STOP and do not have to complete the rest of this form. The Data Security Review must still be submitted. (GO TO THE END OF THIS FORM.)

If you answered "NO", your research will be utilizing either **limited data sets** (click here for a list of limited data set identifiers) or **protected health information** (PHI) in electronic format (ePHI) and you will need to complete questions 4 through 16.

If you are de-identifying data, click on the policy for De-identifying Data for Research.

GENERAL SECURITY

4. Is the ePHI for this study to be housed on a server that meets OIT standards, and meets AHC-IS standards if you are in the AHC? For this purpose, a server is a multi-user computer, which provides some service for other computers connected to it via a network. ☐ **Yes** ☐ **No**

If you answered "YES", please specify which server:

If you have answered "NO", please describe your server security practices:

Please reference the 18 requirements found on the University's **STANDARD—Securing Private Data (Appendix G).**

For more information, click on the links to the AHC-IS server standards and to the OIT standards for critical servers.

5. Please provide an **inventory** of the electronic equipment your research will utilize. This would include the **number** and **type of equipment** such as servers, workstations, laptops, mobile devices.

6. Do you have professional IT staff who will be supporting equipment on which ePHI is used?
☐ **Yes** ☐ **No**

If "YES", please provide more detail: (names of individuals, or specify which IT department)

7. Do your workstations and laptops run up-to-date AntiVirus programs and security patches which are automatically set up to run on a regular basis? ☐ **Yes** ☐ **No**

Please link to the AHC-IS for information on Workstation Standards and Workstation Security.

8. Are all portable devices, including laptop hard drives, encrypted? ☐ **Yes** ☐ **No**

RECORDING AND HANDLING

9. Please describe the research database or spreadsheet (or other means) you will be using. (eg: SAS, Stata, Oracle, Access, Excel, etc)

Are you able to authorize access and track access if the research database will have multiple users?
☐ **Yes** ☐ **No**

10. Please describe how your research/analytic database will be updated, and how updates will be tracked.

BACKING UP, STORAGE, AND DISPOSAL

11. Please describe your method and process for backing-up ePHI data:

12. Please describe your plans for long-term storage, and possible destruction, of your ePHI data after the conclusion of your research.

13. Please state your plans for handling broken or out-dated equipment that will no longer be used in your research.

ACCESS

14. Please describe what type of technologies (software, hardware, etc) are used to ensure remote secure access to data stored on the University network? This would be if anyone will be working from a home computer, and getting into the University network.

Note: Possible responses would involve VPN, SSL used for website access, remote desktop protocol, and how remote network environments (i.e.home networks) are secured.

Please review the standards at **www.safecomputing.umn.edu**

NOTE: ePHI SHOULD ONLY BE STORED ON UNIVERSITY-OWNED COMPUTER EQUIPMENT OR PORTABLE DEVICES, and never on personally-owned equipment.

SHARING AND COLLABORATING

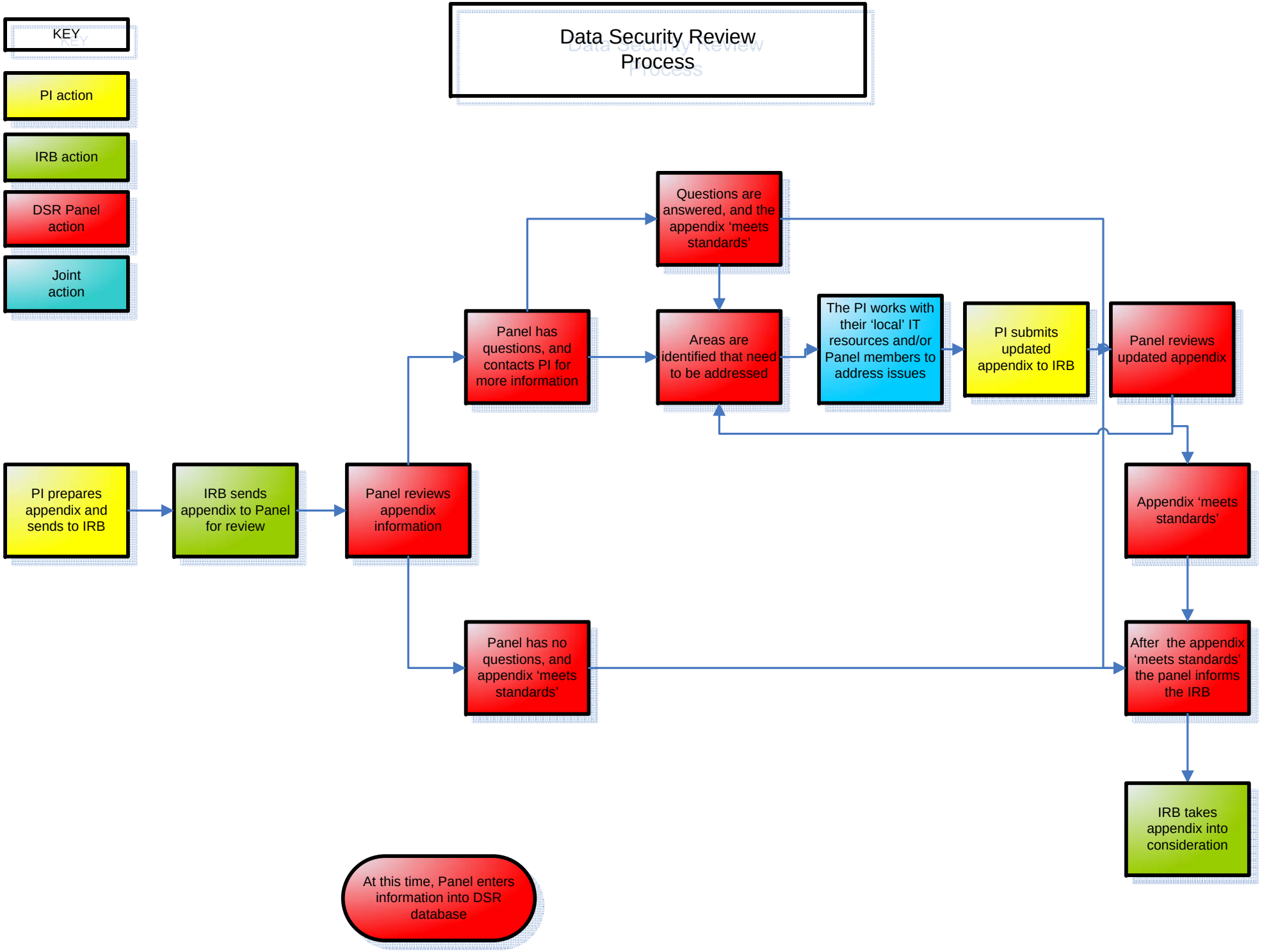
15. If you plan to share ePHI data with an external collaborator(s) or business associate(s) please describe your method and process for sharing data. Please review the policy on Use and Disclosure of Individual Health Information for Research (HIPAA).

If your data will **not** be shared, please check this box. ☐

16. Will you be using any electronic communications or equipment/devices in the collection of ePHI? Consider if you will you be collecting data via website, electronic surveys, or text messages. Please describe the circumstances. If using a survey, please specify.

HIT SUBMIT BUTTON

FOR USE ONLY BY DSR PANEL
LOG NUMBER :
REVIEWED BY:
DATE:
FOLLOW-UP ACTIONS:
THIS DSR ☐ **MEETS STANDARDS** ☐ **DOES NOT** MEET STANDARDS
NAME: DATE:


KEY
PI action
IRB action
DSR Panel action
Joint action
Data Security Review Process
Questions are answered, and the appendix 'meets standards'
Panel has questions, and contacts PI for more information
Areas are identified that need to be addressed
The PI works with their 'local' IT resources and/or Panel members to address issues
PI submits updated appendix to IRB
Panel reviews updated appendix
PI prepares appendix and sends to IRB
IRB sends appendix to Panel for review
Panel reviews appendix information
Appendix 'meets standards'
Panel has no questions, and appendix 'meets standards'
After the appendix 'meets standards' the panel informs the IRB
IRB takes appendix into consideration
At this time, Panel enters information into DSR database

ROOT CAUSE ANALYSIS

> "There is no lock on the door. Only layers of protection."
> *- U of M researcher*

An important aspect of our project was to look into what was causing or contributing to security violations. We reviewed several years of the HIPAA Incident Log which tracks incidents involving both PHI and ePHI. The log identifies the nature of the violation, and oftentimes has some explanation or background information. Many of the interviews also provided information about what contributes to security violations. Some of the root causes which we identified derive from an IT frame of reference, and some from a research or PI point of view. We believe that we have identified most of the actual or commonly-perceived root causes.

The root causes are presented in graphic form on the following page. They are not listed or sized relative to their frequency or risk level. Please remember the boxes represent the "why", and not the "what" of violations. For clarity we have occasionally given an example of a "what" in parenthesis.

The highlighted boxes are those which we feel are addressed by the recommendations made within this report.

Some explanation of the terminology may be useful:

'Centralization' represents any alternative to having every PI provide IT expertise and support on his/her own. 'Centralization' could be University-wide, college-wide, department support, or other variation.

> "We need to centralize. But locally."
> *- U of M researcher*

The term 'human error' encompasses a fairly wide range of actual activities. For our definition, this is when people are momentarily making bad decisions, or trying to hurry, or placing convenience over security. This would include opening up email attachments sent by unknown persons which can compromise a network or wipe out a hard drive. It includes putting a laptop into a situation where it can get stolen. It includes transposing numbers or letters and electronically sending ePHI to the wrong person. Generally, 'human error' momentarily opens up the opportunity for violations to occur.

'Failure to comply' differs from human error in that it's a more willful avoidance of policies. This would include failure to encrypt a laptop, or creating a password that is all too easily cracked, or sharing passwords. 'Failure to comply' creates extensive timeframes in which violations could occur.

We've labeled as "unable to comply" those factors that act as impediments to PI's having the best security possible. And we don't mean to imply that these factors invariably lead to non-compliance, but they help set the stage. When IT resources are not readily available, when money pressures come to bear, and when PI's are experts in their fields and not in security, the situation is less than ideal.

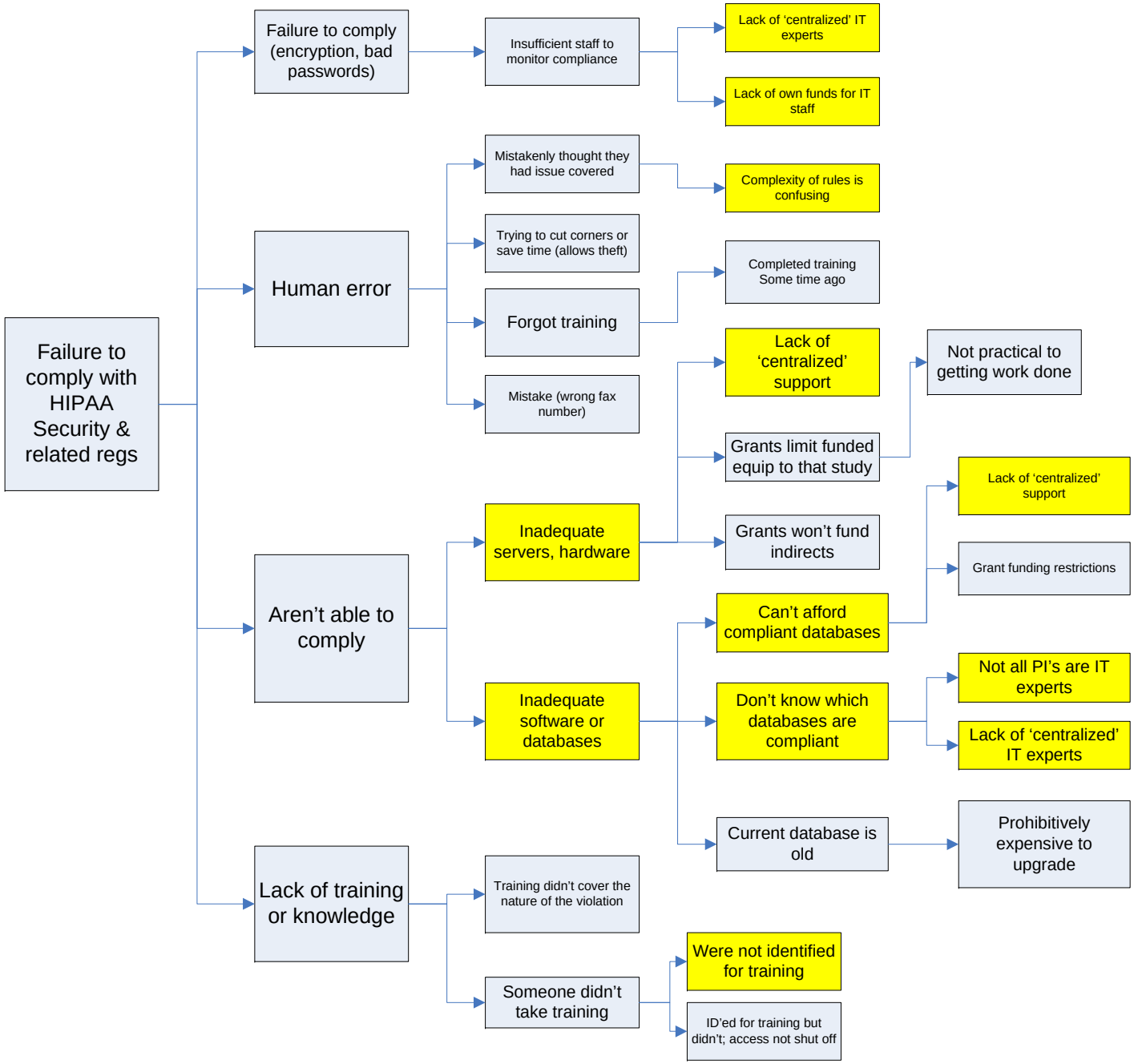
> "We have failed to make it easier to comply."
> - U of M researcher

All University employees are required to complete Security training. Some units in the Academic Health Center (AHC) are considered to be in a designated health care component (HCC) and all staff in these areas need to complete various levels of HIPAA Privacy and Security training. The specific extent of training is based on actual job responsibilities, and this presents an opportunity for someone to be mis-identified for training. There are many areas all across the University whose research is subject to HIPAA, and the Privacy & Security Office works with 75+ Privacy Coordinators in more than 250 units to help make sure the right groups are identified for training. But without University-wide HIPAA training being required, there exists an opportunity for research staff using ePHI to not receive training. If someone does not complete training that has been assigned to them they will get several reminders, but they ultimately risk losing electronic access to certain systems.

> "There are concentric circles of understanding that generally decrease as you go out from the PI."
> *- U of M IT professional*

Our recommendations on the new appendix include listing by x.500 all staff that will be involved in human subject research. This information will then be cross-referenced with training records to ensure that required training is completed.

Our recommendations on the DSR process will do a good deal towards reducing the instances where one is "unable to comply". While financial considerations will obviously still exist, we believe that having pro-active IT assistance will reduce inadequate backups, sub-standard storage, un-secure sharing, inadequate software, and lack of encryption. We believe there will be many instances where professional IT staff will be able to suggest software for which the University has licensing, identify existing secure servers, and assist with performing upgrades.



Highlighting represents those causes addressed to some degree by the recommendations

WEB-BOARD IMPLEMENTATION & COMMUNICATION PLAN

One of the issues that came up during the internal interviews was that researchers often didn't know where to get answers to their technology and security related questions. Among our recommendations is the creation of a web-board, entitled **ask IT.** This vehicle will serve as an opportunity for researchers to ask questions. Questions are submitted online, so they can do this whenever it's convenient for them. In conjunction with the DSR which is initiated by the new IRB appendix, this web-board provides an opportunity for researchers to more easily partner with security experts to resolve their particular issues.

Questions will be submitted and the panel will respond directly to that individual. The resulting Q & A may be edited, and names, departments and other identifiers will be removed prior to posting on the web-board.

The answers will be a consensus of the IT professionals monitoring the web-board and will be the minimal best practices that they all agree to.

The web-board will have questions grouped by general topic, and will also have a keyword search function. Prior to submitting a question, users will be able to see if the question has already been addressed in a manner suitable for their needs.

The archived questions and answers will serve as an ever-expanding information resource which can serve as a low-cost and easily-accessible way to address some issues. Of course, some researcher's problems and resolutions will be highly specific and not well-suited to adoption by others. But we think there is opportunity to make a significant impact on the issues that are currently going unaddressed. And this is a way for things to be addressed even before the more formal DSR is undertaken. Ideally, these two formats will complement one another.

The bank of previous questions should be periodically monitored to ensure accuracy as technology changes. Answers given today may not be applicable in two years --- or less. We suggest that this issue be reviewed after the web-board is in use for some time. Actual workload will be a consideration in deciding if the best way to address this is by individually reviewing older questions, deleting questions with certain keywords, deleting the Q&A on individual topics beyond a certain date, or deleting all content beyond a certain date.

As with our recommendations on the new appendix, we recommend that before rollout the web-board undergo usability testing.

We encourage the administrators of the web-board to be receptive to user's continued feedback, and to be open to making this as user-friendly and user-

useful as the research community indicates. Their needs could change over the years.

Unless the makeup of the panel changes, the questions need to be kept to the narrow scope of computer and technology security as it relates to ePHI under HIPAA and related regulations. A panel of computer experts should not be expected to respond to overall questions about HIPAA compliance. It should not be used as a general computer helpline.

Overview of askIT Web Board Features:

- Central place to ask questions related to data security in human subject research
- Panel of experts to provide responses to questions within 24 to 48 hours (weekends and holidays will be exceptions)
- Forum for posting and sharing of past questions so researchers can use the board as a resource
- Archive of past questions that are searchable by researchers
- Method to track frequency of questions or group according to topic
- Tracking of questions for web-board administrators to review for frequency and patterns that may indicate opportunities for training or pro-active action

Proposed askIT Web Board Launch Timeline:

Fall 2008 Perform usability testing and survey users as to functionality of site in order to make improvements / changes to the draft.

Spring 2009 Launch of beta site to researchers in conjunction with limited roll-out of communication and marketing plan.

Fall 2009 New training and communication pieces reflecting lessons learned from initial beta roll-out in Fall 2008.

Data Security Review (DSR) and askIT Communication Plan Roll-out

- Bookmarks with the askIT logo and site listed on it
- Posters for lab areas promoting the askIT site
- Email campaign for askIT site
- Information at new faculty orientation on new appendix, DSR, and askIT
- Articles and updates in AHC Communications and the U of M Brief

- Article in the Minnesota Daily
- Front page article on the U of M web site
- Information going to, or presentation for, Associate Deans of Research in AHC
- Links off other websites; OVPR, IRB, RSPP, AHC, and others
- HIPAA FAQ post-card for researchers to post in labs, dated so researchers know when to take the card down.

A communication and promotion plan for the rollout of new resources is key to the success and adoption of askIT . Researchers we interviewed directly asked for dated postcards regarding HIPAA FAQs, or "Top Ten Things to Know About HIPAA" so they can post them in their labs at the beginning of the year. These materials need to be visually powerful and also up to date with the askIT header and look so the branding carries through all promotional materials.

The main thrust of all announcements and promotional materials should be that the DSR and askIT are there to help researchers with security. Our interviews revealed that the research community doesn't think this help currently exists, but they want it. Our recommendations are intended to ultimately make less work for them, not more.

Attachment A

University of Minnesota Interviewees

Academic Health Center, Associate Deans for Research

- ***Charles Moldow***, M.D., Medical School
- ***Ann Garwick***, Ph.D. RN, School of Nursing
- ***Srirama Rao***, Ph.D., College of Veterinary Medicine
- ***George Trachte,*** Ph.D., Duluth Medical School
- ***Henning Schroeder***, Ph.D., College of Pharmacy
- ***Joel Rudney***, Ph.D., School of Dentistry

Office of Clinical Research, Academic Health Center

- ***Jasjit Ahluwalia***, MD, MPH, MS, Executive Director
- ***Becky Moen,*** Associate Director
- ***Matt Beecher*****,** Informatics Manager
- ***Nancy Flemmons***, Associate Clinical Specialist
- ***Sue Lowry,*** Info Tech Professional
- ***Laure Campbell*****,** Research Subjects Advocate
- ***Scott Lunos*****,** Research Fellow

Lorrie Awoyinka, Senior Grant/Contract Administrator, Sponsored Projects Administration (SPA)

Kemal Badur, Info Tech Supervisor, CLA

Paul Bernhardt**,** Info Tech Prof, School of Public Health

Eugene Borgida**,** Ph.D., Professor, Psychology

Steve Cawley, Vice President and University Chief Information Officer, OIT

John Crow, Ph.D., Director, Center for Biomedical Research Informatics

Ed Deegan, Director, AHC Academic Information Systems (AIS)

Connie Delaney, Ph.D. RN, Dean, School of Nursing

Josh Fehrmann, Info Tech Prof, Cancer Center

Carol Foth, Education Specialist, Office of the VP For Research

Jonathan Harper, Security Administrator, AHC AIS

John Jensen, Assistant Director, U of M Privacy & Security Office

Moira Keane, Director, Research Subjects Protection Program, IRB

Robert Kvavik, Ph.D., Professor, Associate Vice President, Office of Planning

David Loewi, M.S., Director, Computing Services UMN Morris

R. Timothy Mulcahy, Ph.D., University Vice President for Research

J.M. (Michael) Oakes, Ph.D., Associate Professor, Epidemiology

Kevin Peterson, M.D. MPH, Associate Professor, Family Practice & Community Health

Elizabeth Seaquist, M.D., Professor, Medicine; Director, General Clinical Research Center

Barbara Shiels, J.D., Associate General Counsel

Jessy Thomas, M.S., CCRP, Associate Program Director, Office of Regulatory Affairs

Sarah Waldemar, Assistant Director, Office of Oversight, Analysis & Reporting

Shelly Wymer, Program Director, Office of Measurement Services

HIPAA and Research
Interview Themes

INTERVIEWS	THEMES	Need finformation on HOW to comply	Individual behavior & human error pose significant risk	Want some degree of 'centralization' but also ability provide own	Not the role of the IRB to assess security issues	Range of skill level among PI's & staff	Want assistance in suggesting and/or reviewing security plan	There should be some specific risk assessment	The future of research involves increased sharing and collaboration	(Most) Grants don't pay for IT (equip, upgrades, or staffing)	Show how changes are a benefit to researchers
			x	x				x	x	x	x
										x	
		x		x		x	x				
		x			x		x				
		x	x		x		x				
						x			x	x	x
		x	x	x			x				
				x		x	x			x	x
			x	x	x	x			x	x	x
						x	x		x	x	x
		x			x	x					x
		x	x				x			x	
			x		x						
			x								
		x	x	x	x						x
			x	x	x	x	x	x			x
		x	x	x	x	x	x	x	x		
		x		x	x	x	x	x	x		x
				x	x			x	x		
		x		x		x	x			x	x
					x	x		x			
		x									x

Attachment C

Peer Institution Information

List of institutions:

Penn State

University of Wisconsin-Madison

University of Michigan

Yale University

Johns-Hopkins University

Harvard University

Mayo Clinic

University of California-San Francisco

University of Iowa

The questions:

1. Does your university have established security standards or policies?

2. If so, how are those standards or policies meaningfully enforced?

3. Do you have an IRB or a Privacy Board? Do they play any role in reviewing security plans for clinical research involving ePHI?

4. How do your clinical researchers obtain IT resources? (Are they expected to provide their own professional IT staff, expertise, and resources? Is professional IT staff made available at the college level? At a departmental level?)

What's Inside

IRB home
FAQ HIPAA
General Counsel
AHC Home

PEL WEB BOARD (BETA VERSION)

Knowledgebase Home | Glossary | Favorites | Contact | Login

Welcome to the datasecurity knowledge base / web board. Please ask a question below or search past questions posed to the data security review team. Answers will be returned to you in a prompt manner and archived forfor future searching. Your name will be removed from the question in the archive.

ASK A QUESTION

Search the Knowledgebase

Browse by Category

-- Select Category --

Recent Entries

1. how do i secure my server?
2. Data Security Training and Awareness Collaboration

Most Popular Searches

1. training
2. how do i secure my server

Top Ten Facts about HIPAA and data security postcard mock-up

Bookmark for AskIT website