COMMENTS ON ADVANCED NOTICE OF PROPOSED RULEMAKING
Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators
76 FR 44512
DOCUMENT NUMBER 2011-18792
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY
INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC. - USA
ASSOCIATION FOR COMPUTING MACHINERY SPECIAL INTEREST GROUP ON COMPUTER-HUMAN INTERACTION

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronic Engineers, Inc. – USA (IEEE-USA), and the ACM Special Interest Group on Computer-Human Interaction (SIGCHI), we are submitting the following comments in response to the Advanced Notice of Proposed Rulemaking on the Department of Health and Human Services (HHS) regulations for research involving human subjects, also known as the Common Rule.

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. The Institute of Electrical and Electronic Engineers, Inc. – USA (IEEE-USA) advances the public good and promotes the careers and public policy interests of 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. (For further information, please visit www.ieeeusa.org.) The ACM Special Interest Group on Computer-Human Interaction (SIGCHI) - www.sigchi.org - is the world's largest association of professionals in the research and practice of computer-human interaction. SIGCHI serves as a forum for ideas on how people communicate and interact with computer systems. Should you have any questions or need additional information, please contact Cameron Wilson, our Director of Public Policy, at 202-659-9711, or at cameron.wilson@acm.org.

Representing computing professionals and researchers, all three groups can address the ANPRM on the Common Rule along two major themes. Like any other research community, we can comment on the appropriate level of oversight for human subjects research in our field. Additionally, we can speak to the proposed rules concerning data security that HHS would rely on to alleviate some of the regulatory burden on researchers.

Human Subjects and Computing Research

A notable percentage of computing research, especially in the subfields of computer networks, computer-human interaction, accessibility and usability, involves human subjects. Certain subfields of computing research did not exist prior to the formation of the Common Rule, and on that basis alone, revisiting the regulations is overdue. Many in the computing community would consider survey and interview research to be of low risk to human subjects in most cases.

Additionally, there are some kinds of computing research where conducting the traditional pre-experiment informed consent procedures would make it difficult to minimize bias in the experiments or to even conduct research at all. When researching activity across computer networks at the transport level, it can be difficult to identify, contact, and obtain consent from human actors in those networks in a timely fashion. If the research is conducted at the application level, consent may be precluded by conditions in the terms of service of the relevant applications.

Data Security for Human Subjects Research Information

The ANPRM indicates that HHS is considering replacing many current oversight practices for certain kinds of research with data security requirements. Such requirements would help minimize the exposure of personal information of research subjects to all but the few researchers that would need to have access to that information. From the ANPRM, Section V:

"a solution we are considering is to mandate data security and information protection standards that would apply to all research that collected, stored, analyzed or otherwise reused identifiable or potentially identifiable information."

Our experience in privacy and security for computing systems and the information stored on them indicates that a mandate of data security and information protection standards would be good practice and we heartily recommend HHS pursue this solution. The relative lack of privacy and security in consumer data systems is part of the reason there have been over half a billion data records breached in over 2,700 publicly reported incidents since 2005.[1] These incidents have included research and medical institutions. Increasing the amount of data stored and accessed will require additional data security and information protection practices. The consequences of a breach of human subjects research information are such that a mandate or some other means of ensuring universal adoption of best practices in data security and information protection is essential.

Recommendations

The following recommendations reflect our answers to the questions in this ANPRM, and our experience with other regulations that influenced computing research. You can find them explained in additional detail in our responses to the questions below.

Make sure regulations do not unintentionally restrict research on anonymity, security and privacy.
Minimizing the re-identification of de-identified data is a worthwhile objective for these regulations. However, such a regulation should not also restrict research on anonymity, privacy or security that would involve de-identifying and/or re-identifying. Consider this a parallel to so-called red team testing of computer systems, where every effort is made to break the system tested to improve it.

Insist on uniform application of data security and information protection rules.
In the course of research, information on human subjects can be transmitted to other parties besides the researchers who were originally subject to these regulations. Transfer to a third party must not reduce the protections accorded to collected information under these regulations.

Allow for means of updating regulations to reflect research results and changes in best practices.
The last major changes to these regulations were twenty years ago. In a young field like computing, new kinds of research and new subfields can emerge in that time. Should this emerging work bring additional risks to human subjects, there needs to be a way to incorporate new findings into existing regulations without taking the time for a major rulemaking. The same is true for changes in best practice in data security and information protection.

Specific Questions

We address specific questions below (the questions are in bold) with particular emphasis on issues arising from uncertainty regarding the state of the art in providing secure and/or anonymized data. Security and anonymity are themselves active research areas, and it is important to remember that what is possible (or not) today can change. Many of the questions in the ANPRM do not directly address this uncertainty. We also want to make sure that issues involving security, privacy and anonymity apply to both data in place and data transmitted over networks.

***Question 1*: Is the current definition of ''minimal risk'' in the regulations (45 CFR 46.102(i)—research activities where ''the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests'')—appropriate? If not, how should it be changed?**

There is another category of research that should be considered as minimal risk – transport-level networking research. This is research using captured packet traces from one or more points in the network to serve as input data for an analysis of network behavior, such as traffic flows between sets of traffic sources and traffic destinations. An example would be attempting to locate network attack source nodes in a Denial of Service or Distributed Denial of

[1] Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach

Service (DDoS) attack with traffic analysis tools. In the case of transport-level networking research, consent is often a logistical challenge. Obtaining pre-research informed consent for network traffic analysis can be difficult. Obtaining consent for research involving social networks may be hindered by terms of service for relevant applications.

In circumstances where consent poses such problems, we recommend, where practical, a post-research debriefing – having the researchers discuss the results and implications of the research with the subjects following the experiments. In some cases, post-identification would require attempts at de-anonymization that would itself create risks. Transit research is an example of research that would be enhanced through a combination of reporting and classifying the research as Excused.

Question 5: **What criteria can or should be used to determine with specificity whether a study's psychological risks or other nonphysical, non-information risks, are greater than or less than minimal?**

The security and anonymity research communities, including the usability components of those communities, are working hard on the need to properly inform research subjects about their work, and are also conducting research in how to better address those needs[2]. As the research community moves forward, the Common Rule requirements should integrate research findings that influence human subjects research processes.

Particularly in security and privacy research, informed consent and traditional practices to mitigate risk can hinder effective research. In these cases, we would recommend that the researchers conduct a post-research debriefing with subjects concerning the research results and implications. This is the current best practice, but as noted above it could change during the Common Rule review process. We recommend that any research on network operations where no data are re-identified be Excused.

Question 6: **Are there survey instruments or specific types of questions that should be classified as greater than minimal risk? How should the characteristics of the study population (*e.g.* mental health patients) be taken into consideration in the risk assessment?**

Computer scientists and network researchers conduct research that can help clear the Internet of spam and malicious content implement specific types of instrumentation to identify, compile, draw, and examine attacks and attackers. Digital criminal networks are an active research area. This research should not be prohibited by protections meant for other subject populations. The logistical difficulties of obtaining informed consent, combined with the large numbers of individuals involved mitigate the potential risk to human subjects. We believe expedited review should be the standard in these cases.

Question 7: **What research activities, if any, should be added to the published list of activities that can be used in a study that qualifies for expedited review?**

Networking research that uses only the information normally and openly transmitted over the network(s) should be subject to expedited review. Depending on the particulars of the project, such research could fall into the Excused category.

For instance, research on digital crime requires interacting with malicious agents. These individuals cannot be subject to informed consent, or the research would be simply impossible. Interactions with criminals and networked components that these parties control is critical to understanding and defeating online criminal threats. Clarification of the many subtleties will change as the criminals' strategies change. This dynamic interaction may be best served by a national discipline-specific body that includes computer scientists, ethicists, and individuals from IRBs. A uniform set of best practices could be created under a framework (informed by the experience of HIPAA), then disseminated to IRBs and researchers. Compliance with such practices would allow this kind of research to be expedited.

Usability research on interactions of networking monitoring, security, and applications should be expedited unless the research involves tests of duress. Research in this category usually focuses on standard use of technology and technical applications.

---

[2] D. Maughan, "An examination of the current state of Ethics in Information and Communications Technology Research", National Science Foundation WATCH Series, Arlington, Virginia 22230, 6 October 2011

Question 11: **What are the advantages of requiring that expedited review be conducted by an IRB member? Would it be appropriate to instead allow such review to be done by an appropriately trained individual, such as the manager of the IRB office, who need not be a member of the IRB? If not, what are the disadvantages of relying on a non-IRB member to conduct expedited review? If so, what would qualify as being "appropriately trained"? Would the effort to make sure that such persons are appropriately trained outweigh the benefits from making this change?**

We see the point of expedited review as ensuring that protocols that appear likely, but not self-evidently, to be low risk are low risk. This requires both IRB and relevant subject matter expertise. Therefore, we do not see IRB membership per se as the salient issue. Rather, the objective should be to ensure that appropriate expertise in both senses is brought to bear on protocols involving topics such as computer networking and security, informational privacy, and digital anonymity. Establishing a sufficiently comprehensive set of subject matter experts who have undergone IRB training to serve as designated reviewers (but not necessarily IRB members) for purposes of expedited review strikes us as the most effective approach to this issue. Alternatively, an IRB member tasked with an expedited review should have the formal option to call upon an appropriate subject matter expert for advice, similar to the current provision that permits an IRB as a whole to do so. Consistent with our view that IRB membership is not really the issue, it also would be acceptable for appropriately trained administrative staff to carry out an expedited review, contingent on their either possessing any necessary subject matter knowledge or being able to call upon an appropriate expert.

Question 12: **Are there other specific changes that could be made to reduce the burden imposed on researchers and their staffs in terms of meeting the requirements to submit documents to an IRB, without decreasing protections to subjects? Are there specific elements that can be appropriately eliminated from protocols or consent forms? Which other documents that are currently required to be submitted to IRBs can be shortened or perhaps appropriately eliminated? Conversely, are there specific additions to protocols or consent forms beyond those identified in this notice that would meaningfully add to the protection of subjects? What entity or organization should develop and disseminate such standardized document formats?**

Some of the necessary documentation does not effectively apply to certain kinds of research. The 'location' of network research is hard to pin down in a conventional geographic sense. As mentioned in answers to other questions, there are certain areas of computer research, such as analyzing computer security behavior, where fully informing human subjects would hinder those subjects from providing unbiased responses.

We recommend that IRBs be willing to review and approve research beyond terms of service based entirely on the risks and benefits of the research.

Question 13: **Given the problems with the current system regarding wide variations in the substance of IRB reviews, would it be appropriate to require IRBs to submit periodic reports to OHRP in the instances in which they choose to override the defaults described in Sections B(1), B(2)(a)(ii), and B(2)(b) above? Should IRBs have to report instances in which they require continuing review or convened IRB review of a study which involves only activities identified as being on the list of those eligible for expedited review? If an IRB that chose to override these defaults was required to submit a report to OHRP, would this provide useful information about any lack of appropriate consistency among IRBs so that clarifying guidance could be provided as needed, or provide useful information to OHRP about the possible need to revise the expedited review list or the continuing review requirements?**

Our answer to question 12 complements question 13, by providing a specific example to be generalized here. In some cases for different computer systems and architectures, there are appropriate bodies to provide recommendations for how to provide clarifying guidance about research beyond terms of service.[3] Evaluation of how different IRBs deviate can serve to inform both the guidance, and in some cases even the IRB about better practices. Similarly

[3] For instance, Tor administers its services through a not-for-profit board. A cooperative standards process is handled for things like cybersecurity research (D. Maughan, http://www.cs.stevens.edu/~spock/wecsr2012/ 3rd Workshop on Ethics in Computer Security Research (WECSR 2012)

network operators may have varying standards in terms of user expectation of privacy, or which networks are more or less resilient.

For example, while Tor – a network technology designed to enhance online anonymity - is supported by a not for profit organization, other organizations may prohibit security or privacy research not in the interest of its users but rather to obfuscate their own failures. In some cases the network operator can be best placed to make evaluations; conversely, terms of service are known to be anticompetitive and not consistently in the interest of users.[4] The combination of recommendations, an ability to override those recommendations, and regular, consistent review is a potent combination for oversight while allowing for flexibility.

Consider two areas of research: deception and anonymity. Because deception is a component of online criminal activity (including credential theft, machine subversion, and fraud) individuals in some categories of computer security research, the subjects must be deceived.[5] The goal in these cases is to understand deception. Similarly, studies of anonymity and privacy require attempts to de-anonymize or identify individuals in datasets whom begin anonymous. The goal is to understand anonymity.[6]

Question 15: **Beyond the expansions under consideration, are there other types of research studies that should qualify for the Excused category? Are there specific types of studies that are being considered for inclusion in these expansions, that should not be included because they should undergo prospective review for ethical or other reasons before a researcher is allowed to commence the research?**

Human-computer interaction research involving usability and accessibility that does not involve physical or psychological stress, sensitive questions of topics, deception, or greater than minimal risk should be Excused. For example, many HCI studies involve asking users about their needs, watching participants use prototype software tools, and surveying them about their opinions and perceptions of these tools. These studies typically involve almost no risk to participants.

Question 16: **Should research involving surveys and related methodologies qualify for the Excused category only if they do not involve topics that are emotionally charged, such as sexual or physical abuse? If so, what entity should be responsible for determining whether a topic is or is not emotionally charged?**

We would support restricting surveys and related methodologies from qualifying for Excused research if emotionally charged topics are involved. That restriction must be linked to an entity that uses a consistent and universal consideration of what emotionally charged topics would be. Such considerations should involve input from researchers and non-researchers to effectively gauge how human subjects might approach particular topics.

Question 17: **What specific social and behavioral research methodologies should fall within the Excused category? Under what circumstances, if any, should a study qualify for the Excused category if the study involves a form of deception (and if so, how should "deception" be defined)?**

Research that has been through one IRB should be Excused at all other institutions. A single institution of record can then provide consistent, timely, risk-minimizing, and informed review.

Research conducted in online settings that reflect observation of public behavior should also fall within the Excused category.

---

[4] Nathaniel Good and Jens Grossklags and David Thaw and Aaron Perzanowski and Deirdre Mulligan and Joseph Konstan, User Choices and Regret: Understanding Users' Decision Process about Consensually acquired Spyware, I/S A Journal of Law and Policy for the Information Society, Summer 2006,

[5] "An Analysis of Underground Forums", Marti Motoyama, Damon McCoy, Stefan Savage, and Geoffrey M. Voelker, *Proceedings of the ACM Internet Measurement Conference*, Berlin, CA, November 2011.

[6] Rui Wang, Yong Li, XiaoFeng Wang, Haixu Tang, Xiaoyong Zhou, Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study. 16th ACM Conference on Computer and Communications Security (CCS'09), Chicago, IL, Nov. 2009 Available: http://www.darkreading.com/securityservices/security/app-security/showArticle.jhtml?articleID=224200457

Risk should be the critical variable in determining excusing, expedited, and full review. For example, deceit needs to be an available research option particularly for computer security. There are studies we cannot do without it. Deceit does not inherently create risk. IRBs should have clear, consistent, risk-based guidance on research involving deception and/or misdirection. This guidance should be informed by the efforts of the security community to define and refine best practice.[7]

Question 19: **Regarding the Excused category, should there be a brief waiting period (*e.g.* one week) before a researcher may commence research after submitting the one-page registration form, to allow institutions to look at the forms and determine if some studies should not be Excused?**

A defined waiting period for all IRBs and researchers would provide needed certainty and clarity in the review process for both researchers and institutions. However, many institutions exhibit highly variable responses. A maximum waiting period should be set as a national standard. Such a waiting period must be shorter than the review period for the Exempt category.

Question 20: **The term "Excused" may not be the ideal term to describe the studies that will come within the proposed revision of the current category of exempt studies, given that these studies will be subject to some protections that are actually greater than those that currently exist. Might a term such as "Registered" better emphasize that these studies will in fact be subject to a variety of requirements designed to protect participants? We welcome other suggestions for alternative labels that might be more appropriate.**

We think the label "Registered" for such research indicates the existence of at least some oversight, and would be appropriate to use instead of "Excused."

Question 21: **Is it appropriate to require institutions holding a Federalwide Assurance to conduct retrospective audits of a percentage of the Excused studies to make sure they qualify for inclusion in this category? Should the regulations specify a necessary minimum percentage of studies to be audited in order to satisfy the regulatory requirements? Should some other method besides a random selection be used to determine which Excused studies would be audited?**

Any audit mechanism must be distributed equally across Excused, expedited, and full review research or the certainty of audit would create a strong institutional bias against allowing research to be Excused. The design of an audit mechanism is important, and we recommend including well designed retrospective audits for studies in any category.

In addition to random evaluations, there can be evaluations based on the distribution of Excused studies across institutions. Institutions with similar research portfolios should be expected to have reasonably similar rates of Excused, expedited, and full review research. Thus in addition to random audits, there may be more frequent audits for those institutions which appear to be themselves at risk of refusing to accept research as Excused or identifying too broad a category of Excused. Such a targeted review may determine (in the second case) that an institution has developed an excellent mechanism for ensuring that all research is registered. Thus in addition to random samples, institutional variable should be taken into account.

Question 22: **Are retrospective audit mechanisms sufficient to provide adequate protections to subjects, as compared to having research undergo some type of review prior to a researcher receiving permission to begin a study? Might this new audit mechanism end up producing a greater burden than the current system? Do researchers possess the objectivity and expertise to make an initial assessment of whether their research qualifies for the Excused category? By allowing researchers to make their own determinations, without prospective independent review, will protections for some subjects be inappropriately weakened? If allowing researchers to make such determinations without independent review would generally be acceptable, are there nonetheless specific categories of studies included in the proposed expansion for which this change would inappropriately weaken protections for subjects? And will the use of a one-page registration form give institutions sufficient information to enable them to appropriately conduct the audits?**

---

[7] See notes 2 and 3.

We believe retrospective audits would be an effective tool to help evaluate an institution's oversight capacity in ensuring that its researchers are taking proper care for research involving human subjects. We would not presume to know whether audits by themselves would be sufficient to provide adequate protection.

Question 23: **Under what circumstances should it be permissible to waive consent for research involving the collection and study of existing data and biospecimens as described in Section 3(a)(3) above? Should the rules for waiving consent be different if the information or biospecimens were originally collected for research purposes or non-research purposes? Should a request to waive informed consent trigger a requirement for IRB review?**

There are categories of research in which informed consent is problematic (network data, anonymity research) or hinders the underlying goal of the study (deception in computer security). These categories can be carefully and narrowly defined so that no IRB review is triggered, or that some kind of modified informed processes (such as a post-research debriefing) would be required. A good guideline is to ensure that data that cannot be de-identified is carefully protected. If a waiver of consent puts such data at risk, additional review is warranted.

Question 24: **The Common Rule has been criticized for inappropriately being applied to—and inhibiting research in—certain activities, including quality improvement, public health activities, and program evaluation studies. Regarding quality improvement, for example, these activities are in many instances conducted by health care and other organizations under clear legal authority to change internal operating procedures to increase safety or otherwise improve performance, often without the consent of staff or clients, followed by monitoring or evaluation of the effects. It is far from clear that the Common Rule was intended to apply to such activities, nor that having it apply produces any meaningful benefits to the public. Indeed, its application to such activities, and requiring IRB review and compliance with informed consent requirements, might have a chilling effect on the ability to learn from, and conduct, important types of innovation. We seek comment on whether and, if so, how, the Common Rule should be changed to clarify whether or not oversight of quality improvement, program evaluation studies, or public health activities are covered. Are there specific types of these studies for which the existing rules (even after the changes proposed in this Notice) are inappropriate? If so, should this problem be addressed through modifications to the exemption (Excused) categories, or by changing the definition of "research" used in the Common Rule to exclude some of these studies, or a combination of both? And if the definition of research were to be changed, how should the activities to be excluded be defined (*e.g.*, "quality improvement" or "program evaluation")?**

We believe the proposed recommendations involving the Excused category would go a long way toward alleviating the concerns within the computing community about the Common Rule being inappropriately applied to certain kinds of computing research. Going forward, emerging subfields in computing that would use research involving human subjects should be addressed as early as possible. Standards efforts should include Common Rule and other ethical guidelines in their work. The new rules should allow such efforts to inform IRBs and related research guidance.

(24 Continued) **Are there some such activities that should not be excluded from being subject to the Common Rule because the protections provided by that rule are appropriate and no similar protections are provided by other regulations? With regard to quality improvement activities, might it be useful to adopt the distinction made by the HIPAA Privacy Rule (45 CFR 164.501(1)), which distinguishes between "health care operations" and "research" activities, defining "health care operations" to include "conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities"?**

We do believe adopting a distinction like the one in the HIPAA Privacy Rule distinguishing between "health care operations" and "research" activities is useful, and applicable to other fields like computing. There are many different kinds of analysis and monitoring of networks that would be more appropriately classified as "network operations" than as "research" activities. We would recommend excusing projects supporting network operations as they would not be focused on the human elements of the network, but on maintaining the health and functionality of that network.

Question 25: **Are there certain fields of study whose usual methods of inquiry were not intended to or should not be covered by the Common Rule (such as classics, history, languages, literature, and journalism) because they do not create generalizable knowledge and may be more appropriately covered by ethical codes that differ from the ethical principles embodied in the Common Rule? If so, what are those fields, and how should those methods of inquiry be identified? Should the Common Rule be revised to explicitly state that those activities are not subject to**

its requirements?

Some methods of inquiry can be covered under an Excused rule to ensure consistent guidelines and activities. The computer security community is struggling to define appropriate standards for the study of anonymity. There is tremendous uncertainty about what the ethical and other appropriate standards for security research should be. Security research has not previously resulted and is unlikely to result in direct harm. The security community is seeking to develop internal standards. Specifically there are ethical requirements for publication and a now-established workshop on ethics in computer security as well as ethical statement requirements in the Internet measurement and the usable security top publication venues. Refining practices into standards with such considerable uncertainty requires expertise in anonymity and security.

However, other fields and methods of inquiry are sufficiently fluid that federal regulations may not be the best means for guiding research involving human subjects. For instance, anonymity research may expose vulnerable people to identification but also find means to prevent the identification of the vulnerable by malicious actors. There is no value in an end to research into anonymity via standards that set rules at a given moment in time and point of scientific knowledge.

Question 28: **For research that requires IRB approval, the Common Rule does not currently require that the researcher always be allowed some form of appeal of a decision (*e.g.,* disapproval of a project). Some institutions have voluntarily chosen to provide appeal mechanisms in some instances, by, for example, allowing the researcher to present the project to a different IRB, or by having it reviewed by a special "appeal" IRB that is composed of members chosen from among the membership of the institution's other IRBs. Should the Common Rule include a requirement that every institution must provide an appropriate appeal mechanism? If so, what should be considered acceptable appeal mechanisms? Should such appeal mechanisms, or different ones, be available for appeals asserting that the investigation is not research, or that the research does not require IRB approval?**

The Common Rule structure can simultaneously ensure higher quality research and superior protection of subjects by including appeals and adding the appeals to the audit process. Currently limitations, errors, or misapprehensions of IRBs can remain uncorrected. Research institutions that are isolated, emerging, or embarking in new arenas may be particularly subject to unduly risk-averse activities. Thus the inclusion of appeal and review can improve the application of the Common Rule, the quality of research, and the national equity of educational and research experiences.

Question 29: **As noted above, IRBs sometimes engage in activities beyond those that are required by the regulations. For example, an IRB might review some studies for the purpose of determining whether or not they qualify for exemption (the new Excused category), or might review studies involving the analysis of data that is publicly available. Would it be helpful, in furtherance of increased transparency, to require that each time an IRB takes such an action, it must specifically identify that activity as one that is not required by the regulations?**

In information science there is a strong bias towards improved information. We support IRBs engaging in such a review of studies. If the revised Common Rule errs, the analysis of these decisions could identify regulatory failures in a timely manner.

Question 33: **How significant are the inefficiencies created by local IRB review of multi-site studies?**

These delays and difficulties are significant. It is a common IRB requirement that an experiment must be reviewed internally before any external participant can be integrated. This requires that integrated interdisciplinary proposals be picked apart, reviewed in pieces, and then brought together for a third review. While each individual IRB's requirements may appear reasonable, it is not uncommon for more than one IRB to require either that the other move first or that the remote IRB must complete review before local review begins. This creates a logically impossible situation. Much energy is expended, by researchers and reviewers, with no benefit for research or subjects.

Adopting the recommendations outlined in our response to question 17 should reduce these inefficiencies.

Question 54**: Will use of the HIPAA Privacy Rule's standards for identifiable and de-identified information, and limited data sets, facilitate the implementation of the data security and information protection provisions being considered? Are the HIPAA standards, which were designed for dealing with**

health information, appropriate for use in all types of research studies, including social and behavioral research? If the HIPAA standards are not appropriate for all studies, what standards would be more appropriate?

It is difficult to respond to this question given that the HIPAA de-identification standards are currently in flux. However, recent research and re-identification incidents cause us to doubt the efficacy of relying on any definitive standard for de-identification. The sufficiency of any de-identification approach is contingent on a number of factors, including data sensitivity, other security controls, and the availability of auxiliary knowledge. Given the steadily growing appreciation of how contextual de-identification is possible, we would prefer to see a standard risk-based process governing de-identification, rather than an absolute standard similar to the current one in the HIPAA Privacy Rule.

***Question 55*: What mechanism should be used to regularly evaluate and to recommend updates to what is considered de-identified information? Beyond the mere passage of time, should certain types of triggering events such as evolutions in technology or the development of new security risks also be used to demonstrate that it is appropriate to reevaluate what constitutes de-identified information?**

As discussed in our response to question 25, research on anonymity often demonstrates new means for re-identifying de-identified information. We would recommend that the treatment of collected information not be limited to discussions of de-identified and re-identified information. Advances in data mining, data aggregation, data re-identification and similar practices should trigger changes in information protection practices.

Standards for anonymity are not static. Federal regulations may not be able to match that pace of change, but research communities can. For example, last year Wang, Wang, Tang and Zhou published a paper that showed that individuals can be identified not only from data but from published papers.[8] The bioinformatics community was responsive and immediately changed the internal disciplinary standards for publication. Anonymity is a moving target. This implies defining risk-based process standards rather than specific de-identification methods and making those risk-based standards sufficiently flexible to respond to advances in research on anonymity.

***Question 59*: Would study subjects be sufficiently protected from informational risks if investigators are required to adhere to a strict set of data security and information protection standards modeled on the HIPAA Rules? Are such standards appropriate not just for studies involving health information, but for all types of studies, including social and behavioral research? Or might a better system employ different standards for different types of research? (We note that the HIPAA Rules would allow subjects to authorize researchers to disclose the subjects' identities, in circumstances where investigators wish to publicly recognize their subjects in published reports, and the subjects appreciate that recognition.)**

Any study where sensitive personal information is collected and analyzed needs strong data security and information protection standards. Because such collection and analysis is not limited to studies involving health information, we recommend applying a strict set of data security and information protection standards to all human subjects research where sensitive personal information (which could include participation in a particular research project) is collected.

***Question 60*: Is there a need for additional standardized data security and information protection requirements that would apply to the phase of research that involves data gathering through an interaction or intervention with an individual (e.g. during the administration of a survey)?**

We are not aware of a need for additional standardized data security and information protection requirements for interactions with individuals.

***Question 61*: Are there additional data security and information protection standards that should be considered? Should such mandatory standards be modeled on those used by the Federal government (for**

---

[8] Rui Wang, Yong Li, XiaoFeng Wang, Haixu Tang, Xiaoyong Zhou , Learning Your Identity and Disease from Research Papers: Information Leaks in Genome Wide Association Study. 16th ACM Conference on Computer and Communications Security (CCS'09), Chicago, IL, Nov. 200 Available: http://www.darkreading.com/securityservices/security/app-security/showArticle.jhtml?articleID=224200457,

instance, the National Institute of Standards and Technology recently issued a "Guide to Protecting the Confidentiality of Personally Identifiable Information.")?

NIST standards in the area of information security would be an excellent resource in determining mandatory standards for data security and information protection. More specifically, such standards should encourage, as general good practice, encryption of identifiable human subjects data at rest and in transit whenever this offers meaningful risk mitigation.

Any PII should be secured when stored through effective minimization of access to that PII, and additional access controls when such data is transported. If PII is placed on removable media, it should be encrypted, should not be stored in clear text, and the media should be tracked and access controlled until the PII is removed from that media. If PII is transported for processing, it should be transported over secure channels.

***Question 62*: If investigators are subject to data security and information protection requirements modeled on the HIPAA Rules, is it then acceptable for HIPAA covered entities to disclose limited data sets to investigators for research purposes without obtaining data use agreements?**

We would recommend including the possibility of disclosing limited data sets for research purposes in the initial data use agreements for HIPAA covered entities. If that is done, and investigators follow data security and information protection guidelines modeled on HIPAA Rules, then disclosure of limited data sets for research purposes would be acceptable, provided the use of those data sets is restricted to the purposes outlined by investigators when requesting the data from HIPAA covered entities.

***Question 63*: Given the concerns raised by some that even with the removal of the 18 HIPAA identifiers, re-identification of de-identified datasets is possible, should there be an absolute prohibition against re-identifying de-identified data?**

An absolute prohibition on re-identifying de-identified data would be counterproductive in computing research. Such a prohibition would remove an important avenue of research on privacy and anonymity of data sets by removing a means – attempting to re-identify data – of testing the success of de-identification practices. However, we consider attempted re-identification to assess the efficacy of de-identification methods to be the only prima facie legitimate purpose for attempted re-identification.

***Question 64*: For research involving de-identified data, is the proposed prohibition against a researcher re-identifying such data a sufficient protection, or should there in some instances be requirements preventing the researcher from disclosing the de-identified data to, for example, third parties who might not be subject to these rules?**

We recommend that any disclosure of de-identified data to third parties be subject to the same rules that applied to the parties collecting the data.

***Question 65*: Should registration with the institution be required for analysis of de-identified datasets, as was proposed in Section II(B)(3) for Excused research, so as to permit auditing for unauthorized re-identification?**

Registration would make it easier for institutions to communicate with researchers changes in best practices in de-identification or other means of assuring data security and information protection. Registration procedures should also note cases of research on re-identification to help distinguish those efforts from unauthorized re-identification.

***Question 66*: What entity or entities at an institution conducting research should be given the oversight authority to conduct the audits, and to make sure that these standards with regard to data security are being complied with? Should an institution have flexibility to determine which entity or entities will have this oversight responsibility for their institution?**

Given that part of the impetus for this revision of the Common Rule standards is an effort to standardize practices across institutions, we recommend that the same entity be given the oversight responsibility in every institution.