Association for Computing Machinery (ACM)
ACM US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

January 6, 2016

Office for Human Research Protections
Department of Health and Human Services
1101 Wootton Parkway, Suite 200
Rockville, MD 20852

Re: Public comment on the Notice of Proposed Rulemaking on the Federal Policy for the Protection of Human Subjects, Docket ID HHS-OPHS-2015-0008

Dear Office for Human Research Protections:

Thank you for the opportunity to comment on the proposed revisions to the current regulations for research involving human subjects, known as the "Common Rule." Federal Policy for the Protection of Human Subjects, Notice of Proposed Rulemaking (NPRM), 80 Fed. Reg. 53931 (Sept. 8, 2015), Docket ID HHS-OPHS-2015-0008. We appreciate the efforts by the federal agencies to strengthen protections for research subjects and to provide greater clarity for researchers conducting valuable research. We provide general comments and responses to specific questions given in the NPRM.

With more than 100,000 members, ACM (Association for Computing Machinery) is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. These comments were developed by the ACM U.S. Public Policy Council (USACM), which serves as the focal point for ACM's interaction with the U.S. government in all matters of U.S. public policy related to information technology. The membership of the ACM U.S. Public Policy Council is comprised of computer scientists, educators, researchers, and other technology professionals. We have experience with privacy, security, data mining, and machine learning algorithms that are used to extract patterns and understanding from large datasets. ACM U.S. Public Policy Council statements represent the views of the Council and do not necessarily represent the views of the Association.

General Comments

The ACM U.S. Public Policy Council supports the overall goals of the NPRM and welcomes the updating and modernization of the Common Rule. The proposed changes to the Common Rule have the potential to streamline research processes while maintaining appropriate protections for sensitive information. We are supportive of the goal of better addressing the complexity of balancing privacy and autonomy concerns with the greater societal value of scientific research.

- **Computing Research Involving Human Subjects**

Computing professionals conducting behavioral, analytic, and clinical studies in the United States, generally do so pursuant to the guidance of the Common Rule. A notable percentage of computing research, especially in the subfields of computer security, information assurance, computer networks, computer-human interaction, accessibility, and usability, involves human subjects.

- **Exemptions**

We are particularly pleased with the discussions of the excluded and exempt categories, including the streamlined processes for determinations of exemptions. These changes will simplify the behavioral research studies conducted by some computer scientists. The proposed online tool for exemption certification has the potential to provide needed standardization to exemption processes. The single institutional review board (IRB) proposal for multisite studies deserves strong support as a tool for reducing the expense of oversight while improving the consistency of protections in larger research efforts. The required posting of consent forms also is a useful measure for improving access to information by human subjects.

The majority of researchers will not have expertise in computer security. Identifying security certifications or best practices might both improve security and clarify oversight requirements. Specific recommendations could include both technologies and product security certifications, as well as organizations that are so certified, or organizations that will issue such certifications. Although this is a significant challenge, trends in secure outsourcing, security as a service, and cloud computing might ameliorate researchers' burdens in ensuring security.

- **Principles**

Keeping in mind the goals of this NPRM are to help enhance and streamline processes, reduce inefficiencies, eliminate ambiguity, and create a more meaningful IRB process, our general responses to the NPRM proposals and specific questions are guided by the following principles:

- **Apply a functional approach to data information protection**: Overall, regulations focusing on the implications of data usage, access, and disclosure bring advantages over a regulatory focus on specific technologies, materials in an artifact, and specific phenomena. A functional and behavioral regulatory approach could provide greater flexibility to integrate information from different sources, use new technologies, and deliver effective data privacy and security information management strategies over time. Further, a functional approach could provide agencies with a greater ability to exercise oversight to protect and advance data privacy protections as new forms of research, data management, and technologies emerge. Consideration should be given to the function of the regulated technologies and practices, including how and where they are used, and what can be done with them. This approach is applicable similarly to non-digital artifacts that yield data, such as biospecimens. Our responses below specifically apply the functional and behavior regulatory approach to questions regarding biospecimens and the data derived from them; such data frequently are digital data handled by biospecimen data management software and services.

- **Balancing potential harms and benefits of re-identification of data:** The regulations should provide flexibility to allow for the consideration of the harms and benefits of re-identification of data and the related implications for human subjects, researchers, and societal goals. Re-identification is the process by which anonymized data are turned back into personal data through matching techniques. We support oversight mechanisms to ensure protection of the

identity and privacy of human subjects by preventing the release of re-identified data, as appropriate. However, it is also important to consider the potential benefits for valuable research and societal goals. There are public benefits when researchers work on data identifiability projects, even when they do so without the express consent of the data custodians. We see research on data identifiability and re-identification as being very similar in spirit and mechanism to research on computer security vulnerabilities that advance the goals of online safety and improved secure and trustworthy systems.

- **Degree of risk of data reidentifiability**: Both the risk of data reidentifiability and the resulting consequences are matters of degree rather than all or none. Although some data might always be completely identifiable, other data might be identifiable only for some of the individuals involved, and then only perhaps with a level of uncertainty. The ability to identify an individual may also change with advances in algorithmic techniques and as more external data about individuals become available. Thus, technological developments and an increased ability to aggregate data across more data sources could increase the future risk of data reidentifiability. IRBs and notices to subjects should take this increase into account. Further, the best practices of IRBs will need to adapt as technology evolves.

- **Proportionality of data reidentifiability**: Since regulations need to balance risks and benefits, the decision rule should provide approaches for IRBs to determine an acceptable risk or rate of re-identification. In some cases, a risk of 5% may be acceptable, while in other cases, the acceptable risk may be 1 in 100,000. Public policies and attitudes towards privacy may evolve, particularly for new types of data. Regulatory processes guiding data protection and limitations on use should consider these proportionality issues whenever possible, including ongoing review and revision processes that accommodate evolving technologies and perceptions.

Responses to Specific Questions

2. Would providing a definition of biospecimen be helpful in implementing this provision? If so, how might the definition draw a line between when a biospecimen is covered by the Common Rule, and when processing of biological materials (e.g., to create a commercial product used for treatment purposes) has sufficiently altered the materials so that they should not be subject to the regulations? Would only covering biospecimens that include nucleic acids draw an appropriate line?

It does not seem beneficial to regulate biospecimens specifically and solely; rather, it would be beneficial to regulate the data derived from biospecimens. Drawing on the principle of preferring function over form, we advise the discussion of biospecimens, as well as other categories, in terms of their functional implications, as opposed to their specific nature. For example, many concerns about biospecimens arise from the need to protect sensitive health information such as familial relationships or disease risk factors. These concerns are independent of whether the sensitive information came from a biospecimen, a sensor, or a questionnaire.

New technologies are decreasing overall costs for genetic sequencing. Further, greater digital storage capacity is allowing individuals to obtain a digital copy of their personal genome sequences on portable mobile storage devices. With these advancements and more individuals accessing and managing their data using cloud-based platforms, we may see the advent of widespread personal genomes stored and managed by individuals. If individuals enrolled in a genomic study would authorize researchers to electronically access their sequenced genome, no physical samples would be exchanged.

3. To what extent do the issues raised in this discussion suggest the need to be clearer and more direct about the definition of identifiable private information? How useful and appropriate is the current modifier ''may be readily ascertained'' in the context of modern genomic technology, widespread data sharing, and high speed computing? One alternative is to replace the term ''identifiable private information'' with the term used across the Federal Government: Personally identifiable information (PII).

Concrete definitions can reduce ambiguity and, consequently, uncertainty. The selection of terms used elsewhere, such as personally identifiable information (PII), can also reduce complexity, particularly for researchers who might be working in contexts such as health data where HIPAA and other regulations are already in place.

However, identifiability is not a simple all or none condition that can be definitively assigned to each datum about an individual. Some data are identifiable only in sufficient volume, while others are identifiable only in combination with other items, including where each datum, on its own, may be unidentifiable. Still, others might be identifiable only with a certain level of uncertainty for a subset of associated individuals. Finally, innovations in both de-identification and re-identification techniques might lead to the point where data are identifiable.

After identifiability has been assessed and documented, the rule should allow for considering the potential risk-benefit tradeoffs of each use. One might accept much more data sharing and casual security protections for data needed for an important public good. Also, policy leaders might accept a high re-identifiability risk in research involving human subjects for high-priority studies. Flexible policies that tolerate identifiability risks should consider the individual concerns and societal benefits, as well as potential conflicts. Such considerations seem appropriate topics for IRB reviews.

Voluntary consents from human subjects defining allowable releases also could reflect the degree of re-identifiability the human subjects are willing to allow. Some individuals might accept some degree of risk of re-identifiability, whereas others may feel that one in a million is too high.

Consideration also should be given to the impacts to individuals who may be unintentionally impacted by the research activity. For example, research studies of massive open online courses (MOOCs) may adversely impact the experiences of nonparticipating individuals. As we know correlations exist, nonparticipants may also have identifiability concerns, for example, with respect to characteristics.

8. Public comment is requested on whether the parameters of the exclusions are sufficiently clear to provide the necessary operational guidance, or whether any additional criteria or parameters should be applied

Excluding from review low-risk research that is subject to other independent controls would streamline the process of obtaining approval for low-risk human subject research.

28. Public comment is sought regarding whether an investigator would be able to contrive his or her responses to the automated exemption decision tool in order to receive a desired result i.e., an exempt determination, even if it does not accurately reflect the research activities.

The answer to this question will depend to a certain extent on both the design of the digital tool and the workflow for its use. We assume that this automated exemption decision tool will consist of some number of data entry fields and forms that would identify the researcher and capture the details of the study, possibly via some decision trees involving different questions associated with each exemption type. These questions would be answered via data entry fields that might involve fixed responses, such as yes/no or category selection, constrained responses, such as dates and numeric fields, and/or unstructured text.

Human-computer interaction research and user interface design guidelines suggest that there is a tradeoff between structured input of fixed and constrained responses and unstructured free text. Familiar graphical user interfaces can use checkboxes, radio buttons, and validated fields for structured input, reducing the chances for error and increasing confidence in provided answers. Text input fields are needed for any descriptive details that cannot simply be described by numbers, categories, or other structured choices. Free-text input is harder to process. Although natural language processing tools might be used to extract some details, such tools are imperfect at best. Generally, human review is needed to interpret free text. However, unstructured text likely will be necessary to understand the details of the methods, setting, goals, and risks, if any, associated with a study.

Structured inputs in the exemption determination tool would likely be highly susceptible to manipulation, as users could simply experiment with different combinations in order to accomplish the desired results. The unstructured textual descriptions of study details would likely be irrelevant to any such manipulation, as the text would be beyond the scope of automatic interpretation. Without manual review, contrived responses to such fields will be a very real possibility.

If such an automated exemption decision tool is allowed, we recommend the following procedures to help provide transparency and accountability:

- Record and archive the researcher's answers
- Make the researcher's answers public after publication
- Audit the submissions
- Provide for significant penalties and sanctions to discourage false claims

29. Public comment is sought on whether it would be more appropriate for some of the exempt categories than others to rely on the exemption determination produced by the decision tool where investigators themselves input the data into the tool, or whether there should be further administrative review in such circumstances.

Reliance on the automated exemption decision tool should be calibrated in terms of risk. For example, the category of educational tests, survey procedures, interview procedures, or observations of public behaviors is proposed to be exempt if disclosure of responses would not "be damaging to the subjects financial standing, employability, educational advancement, or reputation." Although the tool might capture some structured data that would help characterize the type of data and the extent of associated risks, these risks are inherently subjective. Determination of the magnitude of the risk will likely require an unstructured text description that would require external review. Decision-tree logic in the tool might help identify those submissions that will need this review.

30. Public comment is sought regarding whether relying on the exemption determination produced by the decision tool where investigators themselves input the data into the tool as proposed would reduce public trust in research.

Transparency and voluntary disclosure might help minimize damage to public trust as related to research and IRB approval and review methods. Public trust could be enhanced by having information about the decision process and its management in the automated exemption decision tool publicly available online. Public information also could include the details of any procedures for manually reviewing or auditing exemption determinations.

31. Public comment is sought regarding how likely it would be that institutions would rely on such a decision tool to provide a safe harbor for an investigator making a determination that the proposed research qualifies for an exemption, or whether developing such a tool would not be worthwhile, and whether institutions would be able to adequately manage exemption determinations without the use of the decision tool.

It may be possible to design an automated tool that would simplify the process, providing a decision-making form of triage that might classify projects in terms of the exemption category and possible levels of risk. This might simplify matters for IRBs, allowing them to more effectively identify areas in need of review and thereby increasing the efficiency of the process. Such triage capabilities might be based on specific, well-defined criteria for risks, data types, etc., with recorded answers informing the subsequent review and supporting transparency.

Many institutions already have online tools for IRB protocol submissions. Although these tools can expedite both submission and review, implementation and maintenance on a per-institution basis might be inefficient. To the extent that the proposed exemption determination tools might support convergence on shared frameworks and thereby reduce expenses for institutions, development of these automated online tools could be worthwhile.

32. Public comment is sought regarding what additional information should be required to be kept as a record other than the information submitted into the decision tool, for example, a study abstract, the privacy safeguards to be employed, or any notice or consent document that will be provided.

Records should be kept of all details provided, including the names of the researchers leading the project, the funding source, descriptions of the work, and any assertions made regarding privacy, security, or exemption categories. If any reviews or audits are conducted, they should be detailed as well.

33. Public comment is sought regarding the value of adding an auditing requirement.

An auditing requirement could allow IRBs to check the submitter's claims about the proposed research study. Automated tools might not accurately reflect the desired logic and could lack the common sense and domain expertise needed for sufficient quality control assurance. To maintain quality, institutions and the government should conduct some random inspections of the submitter's claims and the decisions that the automated tools make.

40. Public comment is sought regarding what improvements could be made to the language describing the type of interventions in this exemption category so as to make clear what interventions would or would not satisfy this exemption category.

The description of benign interventions currently provides narrow examples of activities, such as where a research subject "is asked to read materials, review pictures or videos, play online games, solve puzzles, or perform cognitive tasks." If examples are provided, it could be beneficial to generalize the research activity as "using software on a computing device (e.g., playing a game, reading an ebook, or using a mapping application)."

41. Public comment is sought on whether it is reasonable, for purposes of this exemption, to rely on the exemption determination produced by the decision tool where investigators themselves input the data into the tool, or whether there should be further administrative review in such circumstances.

The proposed automated exemption decision tool suggests the possibility of a spectrum of determination and review processes. These processes might range from an almost entirely manual process whereby each application is reviewed by an administrator, as is currently the case in many institutions, to a fully-automated process involving an investigator's use of the tool with no further review. Intermediate possibilities might involve auditing of some subset of projects.

Please see also our answers to Questions #29 and #33 above.

43. Public comment is sought on the concept of requiring such minimum safeguards and limitations on disclosure, as well as whether the requirements of the proposed § ll.105 would constitute a broadening of IRB responsibilities rather than a streamlining of the implementation of responsibilities

that many IRBs already adopted. If an institution does view this as an inordinate broadening of responsibilities, does the institution currently have in place alternative mechanisms for ensuring data security and participant privacy in a research context? Suggestions for alternative approaches to meeting public expectation that federally sponsored research safeguard their data and protect privacy are sought during this public comment period.

Data security and safeguards are challenges for IRBs, research institutions, and individual researchers. The Common Rule and associated guidance should encourage the development of environments and tools certified as providing appropriate safeguards. Certification of such tools would assure that they meet the requirements for which the tool was certified, such as releasing data according to specified security and privacy rules. Although definitions of appropriate safeguards and a certification process would still be necessary, the decreased uncertainty associated with the choice of a known, certified provider could help IRBs proceed more quickly and confidently, and reduce investigators' burden of secure data management. Many approaches exist to safeguard and protect data in a research context. Among the approaches, the regulations should consider the growing use of hybrid or fully cloud-enabled environments. Although security issues still exist for cloud-enabled environments, they also can provide security protections through ongoing professional management of the network, assets, security reviews, and oversight of information security, vulnerabilities, and threats.

44. Public comment is sought regarding whether the proposed Rule's information security requirements for biological specimens and identifiable private information are highly technical and require a level of expertise not currently available to most IRBs. Do these security requirements unrealistically expand IRB responsibilities beyond current competencies?

Systems and data security issues are known to be challenging, even for trained professionals. Although IRBs might ideally be able to call on institutional information technology support staff for guidance, such expertise may not be readily available. Any requirements that IRBs consider security concerns in more depth might require additional expertise and staffing. Certification of processes and providers, including by third-party vendors, might reduce some of this burden. The regulations should consider the growing use of hybrid or fully cloud-enabled environments; see also the response to Question #43.

Given the pace of technological advancements, it would be prudent to conduct reviews more frequently than the suggested term of eight years.

74. Is mandated single IRB review for all cooperative research a realistic option at this time? Please provide information about the likely costs and benefits to institutions. Will additional resources be necessary to meet this requirement in the short term? Should savings be anticipated in the long run?

The current requirements of per-institution review can result in significant inefficiencies, particularly for complex protocols that evolve over time. Transitioning to a mandated single IRB review for cooperative research could bring benefits. For individual researchers and multisite teams, a single review could reduce overhead costs, reduce delays associated with reviews, and improve the capacity to conduct multisite research. For IRBs and regulators, a centralized IRB review process could improve efficiencies

of reviews and administrative functions. Further, it could help identify unanticipated problems commonly shared across sites and incentivize cooperation among institutions and researchers. Joint reviews also could help avoid duplication of effort, thereby resulting in possible cost savings in the long run.

If a mandated single IRB review for all cooperative research is adopted, single IRB policies and regulations should clearly indicate the roles, responsibilities, and documentation procedures associated with single IRB reviews. Such guidance would help assist researchers, institutions, and IRBs involved in cooperative research better understand the single IRB.

75. What areas of guidance would be needed for institutions to comply with this requirement? Is there something that OHRP could do to address concerns about institutional liability, such as the development of model written agreements?

Model written agreements; clarification of roles and responsibilities of both the IRB of record and other participating IRBs; advice on ensuring that concerns of cooperating IRBs are addressed by the IRB of record; and other descriptions of recommended practices and policies would all be helpful. Descriptions of preferred practices with respect to adverse event reporting would also be of interest. Specifically, in the event of an adverse event, would researchers be expected to report the incident to their own institution, to the institutional home of the IRB of record, or to both?

Thank you again for the opportunity to comment on the proposed revisions to the federal policy for research involving human subjects. The staff and members of the ACM U.S. Public Policy Council are available if you have questions or would like additional information about the issues raised in this public comment.

Sincerely,

Eugene H. Spafford, Ph.D.
Chair, U.S. Public Policy Council (USACM)
Association for Computing Machinery

Harry Hochheiser, Ph.D.
Chair, Accessibility Committee
U.S. Public Policy Council (USACM)

Brian Dean, EMBA, PCI QSA, CIPP, CISA, PCIP PCI
Chair, Privacy Committee
U.S. Public Policy Council (USACM)