epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Comments of

THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

to

DEPARTMENT OF HEALTH AND HUMAN SERVICES

[Docket ID: HHS-OPHS-2015-0008]

Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators
Notice of Proposed Rulemaking

January 6, 2016

By notice published September 8, 2015, the Department of Health and Human Services ("HHS") and fifteen other federal departments and agencies seek public comment on "proposals to better protect human subjects involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) reduce the discretion of researchers to make subjective determinations of privacy risks to research subjects; (2) oppose the exclusion of research activities involving human subjects from Common Rule coverage; and (3) urge HHS to solicit additional comments after issuing the decision tool for exemption determinations, the broad consent form, and the data security standards of §___.105.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, freedom of expression, and democratic values.[2] EPIC's Advisory Board includes leading experts in law, technology, and

[1] Notice of Proposed Rulemaking, 80 Fed. Reg. 53,931 (Sep. 8, 2015) [hereinafter "Common Rule NPRM"].
[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.

public policy.[3] EPIC continually advocates for health information privacy rights and deidentified patient data.

EPIC has previously expressed concern about proposed changes to the Common Rule.[4] In comments to the Department of Health and Human Services in 2011, Professor Latanya Sweeney, Director and Founder of Harvard University's Data Privacy Lab, Data Privacy Researchers, and EPIC urged the Department of Health and Human Services not to adopt standards that would weaken the privacy rights implicated by the Common Rule.[5] We warned that medical privacy standards for deidentification were "gravely inadequate" and urged support for stronger techniques of deidentification.

In *IMS Health v. Sorrell* (2011), EPIC filed an amicus brief on behalf of 27 technical experts and legal scholars, as well as nine consumer and privacy groups, arguing that the privacy interest in safeguarding medical records is substantial and that the "de-identification" techniques adopted by data-mining firms do not protect patient privacy.[6] EPIC also submitted comments to HHS on the privacy implications of proposed amendments to the HIPAA Privacy Rule related to gun control and mental health records.[7] In *FAA v. Cooper*, a case involving government disclosure of an individual's HIV status, EPIC filed an amicus brief asserting that the government should not be allowed to avoid liability by asserting that it caused only mental and emotional harm when it intentionally and willfully violated the Privacy Act.[8]

EPIC has also submitted comments to the Presidential Commission for the Study of Bioethical Issues concerning issues of privacy with regard to human genome sequence data.[9] EPIC commended the Commission for recognizing the privacy implications associated with human genome sequence data, but also set out specific recommendations to safeguard the genetic information of individuals.

EPIC offers these comments to the Department of Health and Human Services to protect the privacy and autonomy of human subjects.

---

[3] EPIC, *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html.
[4] See generally, EPIC *Privacy and the Common Rule,*
https://epic.org/privacy/privacy_and_the_common_rule.html
[5] Latanya Sweeney PHd et al., *Comments on Common Rule Advanced Notice of Proposed Rulemaking*, Docket No. HHS–OPHS–2011–0005
(Oct. 26, 2011), *available at* https://epic.org/apa/comments/EPIC-et-al-Common-Rule-Cmts.pdf.
[6] Amicus Curiae Brief of EPIC, *Sorrell v. IMS Health Inc.*, No. 10-779 (S.Ct. Mar. 1, 2011), *available at* https://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf.
[7] EPIC, *Comments on HIPAA Privacy Rule and the National Instant Criminal Background Check System*, (June 7, 2013), *available at* https://epic.org/apa/comments/EPIC-HHS-HIPAA-Privacy-Rule.pdf.
[8] EPIC, *FAA v. Cooper*, https://epic.org/amicus/cooper/.
[9] EPIC, *Comments on Issues of Privacy Access With Regard to Human Genome Sequence Data*, (May 25, 2012), *available at* https://epic.org/privacy/genetic/EPIC-Human-Gene-Seq-Data-Comments.pdf.

I. Overview

EPIC supports the goals of this notice of proposed rulemaking ("NPRM") to clarify informed consent procedures and ensure Common Rule protection for biospecimen research regardless of identifiabilty. Transparency in biospecimen research is important to maintaining public trust in science and health care professionals.[10]

However, the NPRM repeatedly places research interests ahead of the privacy and autonomy of human subjects and fails to appreciate the unique privacy risks present in today's data-driven society. The Common Rule must do more to ensure respect for persons, one of the three key principles of medical research ethics identified in the Belmont Report.[11]

The patient interest in protecting the privacy of personal medical information is widely recognized. "A majority of adults express discomfort (42 percent) or uncertainty (25 percent) with their health information being shared with other organizations— even if . . . [their] name, address, [date of birth, and social security number] were not included."[12] One out of every seven adults "would hide something from their doctor if they knew their information would be shared," even with guarantees that their names, addresses, dates of birth, and social security numbers stay secret.[13] Another third "would consider hiding information."[14] Over 90% of Americans want to determine which companies and government entities can see their health information.[15] Moreover, individuals have an "interest in the uses to which data sets that include their data is put, even if they are not personally identified by researchers."[16]

---

[10] Rebecca Skloot, *Your Cells. Their Research. Your Permission?*, NEW YORK TIMES (Dec. 30, 2015), available at http://www.nytimes.com/2015/12/30/opinion/your-cells-their-research-your-permission.html?_r=0.

[11] Department of Health, Education, and Welfare, National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*, 44 Fed. Reg. 23,192, 23,193 (Apr. 18, 1979), available at http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html [hereinafter "The Belmont Report"].

[12] California Healthcare Foundation, *Consumers and Health Information Technology: A National Survey*, 26 (2010), *available at* http://www.chcf.org/publications/2010/04/consumers-and-health-information-technology-a-national-survey.

[13] *Id*. at 25.

[14] *Id*.

[15] Patient Privacy Rights/Zogby International Poll, Nov. 23, 2010, *available at* https://patientprivacyrights.org/2010/11/new-patient-privacy-poll/. *See also* William M. Tierney (MD) Sheri A. Alpert (MPA, PhD), Amy Byrket (AS, PMP), Kelly Caine (PhD), Jeremy C. Leventhal (MS), Eric M. Meslin (PhD), and Peter H. Schwartz (MD, PhD), Provider Responses to Patients controlling Access to their Electronic Health Records: A Prospective Cohort Study in Primary Care, 30 J. Gen. Internal Med. Supplement 1, 31–37 (2014), *available at* http://link.springer.com/article/10.1007%2Fs11606-014-3053-0.

[16] Anita Allen, *Privacy and Medicine*, Stanford Encyclopedia of Philosophy (2009), *available at* http://plato.stanford.edu/entries/privacy-medicine/.

a. The NPRM Fails to Adequately Address Privacy Risks

As a general matter, the NPRM's focus on calibrating the level of oversight to the level of risk involved in a research activity does not account for potential privacy risks. As the Council for Big Data, Ethics, and Society's stated, "[i]t is no longer reasonable to claim that either the prior existence or the publicness of a dataset is a reasonable proxy for minimal informational risk posed by the data contained therein."[17] Moreover, privacy-related risks are particularly challenging to assess, as the nature of a single piece of seemingly innocuous data can become highly sensitive when paired with other information. Granting researchers the discretion to assess complex privacy risks with little oversight or guidance poses unreasonable risk to human subjects.

Allowing investigators to determine whether an activity is "low risk" is a subjective judgment with virtually no oversight. The NPRM proposes to exclude certain research involving identifiable private information that the researcher determines "would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation." §_.101(b)(2)(i)(B). Information that appears meaningless in one context could be highly sensitive or damaging to another's.[18] Moreover, a scientific researcher who does not also possess a legal background is not in a strong position to determine what could place an individual at risk for legal liability.

b. The NPRM Proposed Exclusions and Exemptions Weaken Privacy Protections and Oversight

EPIC opposes the exclusion of any research activity involving human subjects from the Common Rule. All human subject research activities should be subject to data safeguards, informed consent requirements that respect the autonomy and dignity of the human subjects, and reviewed by an independent, disinterested party. Likewise, exempting certain research activities from Common Rule protections also leaves human subjects at greater risk of harm to their autonomy and privacy because many of these activities would otherwise be unregulated.

As noted in the NPRM, "[d]esignating certain research fully outside of the bounds of the Common Rule means that investigators are self-determining whether their own research is covered by the law."[19] This is particularly problematic with respect to the proposed exclusion of activities that are deemed "low-risk" under NPRM at §___.101(b)(2).

Exemptions and exclusions for certain identifiable information cannot be justified by an assumption that it is inherently "low-risk." This highly subjective determination ignores the

---

[17] Council for Big Data, Ethics, and Society, *Letter on Proposed Changes to the Common Role*, 4, *available at* http://bdes.datasociety.net/wp-content/uploads/2015/12/BDES-Common-Rule-Letter.pdf (last visited Jan. 5, 2016).

[18] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford University Press, 2010).

[19] Common Rule NPRM at 82.

reality of big data research and the risks imposed by correlative research,[20] and would be inconsistently applied.

c. The NPRM Fails to Provide the "Terms or Substance" of Key Proposed Revisions

Where an agency engages in a proposed rulemaking, the Administrative Procedure Act requires notice that includes "either the terms or substance of the proposed rule or a description of the subjects and issues involved." 5 U.S.C. § 553(b)(3). The agency has requested numerous comments on provisions without providing the "terms or substance" of the specific proposals. Specifically, the NPRM requests comments on a "decision tool" for exemption determinations that has not been developed yet; a broad consent form that is not provided or described; and data security standards that have yet to be formulated.

The agency's failure to provide details of key proposals in the NPRM is particularly problematic with respect to the proposed "decision tool" that would automate determinations of whether a research activity qualifies for exempt status from various Common Rule protections. The NPRM repeatedly requests public comment on whether the decision tool would be reliable, whether researchers should be able to use the tool themselves, and what other information should be documented in addition to what is provided via the decision tool. The public has been given only vague suggestions as to the form and substance of this decision tool, which apparently has not yet been created and may be released in multiple forms by multiple agencies.

It is unreasonable for HHS to frustrate substantive public comment on this central proposal. Accordingly, the agencies must reissue the NPRM to solicit public comments on the decision tool, consent form, and data security standards. Otherwise, it is unlawful for the agency to issue a final rule without this information. To allow for reasonable public participation in the rulemaking process, agencies "must provide sufficient factual detail and rationale for the rule to permit interested parties to comment meaningfully."[21]

II. EPIC Responses to NPRM Questions for Public Comment

a. Definition of "Identifiable Private Information"

Question 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). The Office of Management and Budget's concept of PII refers to information that can be used to distinguish or trace an individual's identity (such as their name, social security number, biometric records, etc.) alone, or when*

[20] *See id*.
[21] *Am. Farm Bureau Fed'n v. U.S. E.P.A.*, 984 F. Supp. 2d 289, 333 (M.D. Pa. 2013) *aff'd*, 792 F.3d 281 (3d Cir. 2015) (quoting *Fla. Power & Light Co. v. United States,* 846 F.2d 765, 771 (D.C.Cir.1988)). *See also Time Warner Cable Inc. v. F.C.C.*, 729 F.3d 137 (2d Cir. 2013).

combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. It is acknowledged that replacing "identifiable private information" with "PII" would increase the scope of what is subject to the Common Rule. However, the practical implications of such an expansion, other than the need to ensure that the data are security stored and otherwise protected against disclosure, may be minimal. Public comment is requested on the advantages and disadvantages of such a change.

EPIC Response: The current definition of "identifiable private information" and the modifier of "may be readily ascertained" is out-of-date and should be revised. The phrase "Personally Identification Information" (PII) is routinely used in privacy law, policy, and professional ethical codes.[22] It should be adopted here. The simplest definition of PII is information that identifies or could identify a particular person. EPIC favors this definition.

The Office of Management and Budget ("OMB") definition of personally identifiable information provides a useful exposition but it is not of itself a useful definition.[23]

EPIC opposes the adoption of HIPAA standards of identifiability, as noted in comments to the 2011 ANPRM.[24]

b. Proposed Exclusion of Activities from the Common Rule

Question 9. *Public comment is requested on the extent to which covering any of these activities under the Common Rule would substantially add to the protections provided to human research subjects.*

EPIC Response: EPIC opposes the proposed exclusion of certain human subject research activities from the Common Rule. This proposal would undermine individual dignity and autonomy, and it would create significant new privacy risks for participants in excluded research. As EPIC explained in the overview, under these new exemptions, (1) researchers would not be required to inform participants in a wide range of research activities of the purpose of the research or obtain participant consent; (2) researchers would not be required to protect

---

[22] *See, e.g.*, Nat'l Conf. State Legislatures, *Security Breach Notification Laws* (2015) (listing data breach notification laws triggered by breach of PII enacted in forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands), *available at* http://www.ncsl.org/research/telecommunications-and-informationtechnology/security-breach-notification-laws.aspx. *See also* Christopher Wolf, *Envisioning Privacy in the World of Big Data, in Privacy in the Modern Age: The Search for Solutions* 204, 207 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015) ("Personally identifiable information ('PII') is one of the central concepts in information privacy regulation.").

[23] Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies* (May 22, 2007), *available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.*

[24] Latanya Sweeney PHd et al, *Comments on Common Rule Advanced Notice of Proposed Rulemaking*, 10, Docket No. Docket ID number HHS–OPHS–2011–0005 (Oct. 26, 2011), *available at* https://epic.org/apa/comments/EPIC-et-al-Common-Rule-Cmts.pdf.

participants' privacy or confidentiality, and (3) researchers could potentially use and disclose so-called "low-risk" identifiable private information without limitation.

The person in the best position to assess whether information is "low risk" is the subject, not the researcher. But because, under the NPRM proposal, the subject would not be required to give informed consent or even be notified that research was taking place, she would be unable to calculate the true risk of participation. The Belmont Report underscores this conclusion: "To show lack of respect for an autonomous agent is … to withhold information necessary to make a considered judgment, when there are no compelling reasons to do so."[25]

At a minimum, Common Rule coverage of all human subject research activities would remove some of the subjectivity and guesswork from complicated privacy risk assessments. Self-determination and lack of accountability or review presents potential for abuse. These risks would be mitigated by Common Rule documentation requirements and IRB review.

Question 10. *Public comment is sought on whether this exclusion should only apply to research activities in which notice is given to prospective subjects or their legally authorized representatives as a regulatory requirement. If so, please comment on what kind of information should be included in the notice such as the research purpose, privacy safeguards, contact information, ability to opt- out, etc. Would requiring notice as a condition of this exempt research strike a good balance between autonomy and beneficence?*

EPIC Response: EPIC opposes the exclusion of any human subject research activity from compliance with the Common Rule. However, should this exclusion remain in the final rule, effective notice would provide some greater protection for subject autonomy than no notice at all.

The notice should inform subjects of the purpose of the research, the institution conducting the research, who the results could be shared with, whether results will be recorded and/or disclosed in a personally identifiable format, the privacy and data security safeguards in place, contact information, and the ability to opt-out of the specific research activity as well as secondary research uses of the information provided.

Question 11. *Public comment is sought regarding whether it is reasonable to rely on investigators to make self-determinations for the types of research activities covered in this particular exclusion category. If so, should documentation of any kind be generated and retained?*

EPIC Response: EPIC opposes the exclusion of human subject research activities from the Common Rule. The ability of investigators to make self-determinations of exempt status, particularly whether the information collected is not damaging pursuant to 101(b)(2)(i)(B), is problematic. See EPIC response to Question 9 for additional explanation.

[25] The Belmont Report at 23,193.

Question 14. *For activities captured under the third element of this exclusion, do the statutory, regulatory, and other policy requirements cited provide enough oversight and protection that being subject to expedited review under the Common Rule would produce minimal additional subject protections? If so, should the exclusion be broadened to also cover secondary analysis of information collected pursuant to such activities?*

EPIC Response: EPIC regularly calls attention to the numerous shortcomings of the Privacy Act.[26] Most obviously, the Privacy Act failed to safeguard the privacy of the 21 million individuals whose records maintained by the Office of Personal Management were breached during the past year.[27] EPIC recently urged Congress to modernize the federal law, arguing that "[g]iven increased public concern about government data security, a recent decision of the Supreme Court, and the OPM breach, Congressional action to strengthen the Privacy Act of 1974 is long overdue."[28] In light of the need to update the federal Privacy Act, existing law does not provide sufficient oversight and privacy protections for human subjects of research activities; compliance with robust Common Rule data safeguards and confidentiality requirements must fill this gap.

Question 15. *Public comment is requested on the extent to which excluding any of these research activities from the Common Rule could result an actual or perceived reduction or alteration of existing rights or protections provided to human research subjects. Are there any risks to scientific integrity or public trust that may result from excluding these research activities from the Common Rule?*

EPIC Response: Allowing researchers to self-determine that a given research activity is "low risk" and thus requires no compliance with Common Rule protections is a serious reduction of existing rights and safeguards for human subjects. See EPIC Comment to Question 9 for additional explanation.

Question 22. *Public comment is requested on whether the protections provided by the HIPAA Rules for identifiable health information used for health care operations, public health activities, and research activities are sufficient to protect human subjects involved in such activities, and whether the current process of seeking IRB approval meaningfully adds to the protection of human subjects involved in such research studies.*

EPIC Response: EPIC opposes the exclusion of research activities involving human subjects from Common Rule compliance, even where such activities may be covered by HIPAA as proposed in the NPRM at §___.101(b)(2)(iv).

---

[26] Letter from EPIC to Rep. Bob Goodlatte and Rep. John Conyers, Jr., U.S. House of Reps. Comm. on the Judiciary (Sep. 16, 2015), *available at* https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.

[27] OPM, *Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident* (Sep. 23, 2015), available at https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

[28] *Id*. at 6-7.

In comments to HHS in 2011,[29] Professor Latanya Sweeney, Data Privacy Researchers, and EPIC urged the Department of Health and Human Services not to adopt standards that would weaken the privacy rights implicated by the Common Rule. Specifically, we stated that "[a]pplying the HIPAA Privacy Rule standards for de-identification to research broadly in an attempt to protect against the information risks described in the [Advanced Notice of Proposed Rulemaking] is poorly understood and all evidence suggest the HIPAA standards are gravely inadequate." We discussed in detail the following inadequacies of the HIPAA standards:

> [HIPAA's] lack of accountability and transparency in data sharing, the seeming lack of enforcement in light of the large number of allegations, HHS' own lack of demonstrated use, the proposed changes to the HIPAA Privacy Rule itself, the lack of a standard for its statistician provision, its lack of fitness to other kinds of data, including other forms of medical data beyond field-structured data, and the adverse impact that could result on sharing commercial data with researchers.[30]

c. Proposed Exemptions

Question 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.*

EPIC Response: Because the exemption tool has not been released or described with any specificity, it is impossible to provide a substantive response to this question. It is not difficult to imagine the possibility of a misguided researcher manipulating answers to achieve a desired outcome. Such a possibility would certainly reduce public trust. HHS must release the decision tool for substantive comments prior to finalizing any NPRM proposals.

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

EPIC Response: EPIC would support an auditing requirement to ensure that the decision tools are used ethically and impartially, and to ensure that exemption determinations are made consistently. Audits must also verify that these determinations are made with appropriate consideration of privacy risks.

Question 34. *Public comment is sought on whether this exemption category should only apply to research activities in which notice that the information collected will be used for research purposes is given to prospective subjects or their legally authorized representatives as a regulatory requirement, when not already required under the Privacy Act of 1974. If so, comment is sought on what kind of information should be included in the notice, such as the research purpose, privacy safeguards, contact information, etc. Comment is also sought on how*

---

[29] Latanya Sweeney PHd et al., *Comments on Common Rule Advanced Notice of Proposed Rulemaking*, Docket No. Docket ID number HHS–OPHS–2011–0005 (Oct. 26, 2011), *available at* https://epic.org/apa/comments/EPIC-et-al-Common-Rule-Cmts.pdf.

[30] *Id*. at 4.

such a notice should be delivered, e.g., publication in a newspaper or posting in a public place such as the school where the research is taking place, or by individual email or postal delivery. Note that other requirements, such as those of the Family Educational Rights and Privacy Act (FERPA) or the Protection of Pupil Rights Amendment, may also apply. Would requiring notice as a condition of this exempt research strike a good balance between autonomy and beneficence?

EPIC Response: Given the educational context of this exemption, participation of student subjects is largely mandatory. Thus, consent cannot sincerely be implied from participation and notice would not cure the lack of subject autonomy.

The stated NPRM goal of this proposal is "to retain an exemption for a considerable portion of education research."[31] However, in light of increasing collections of student data and corresponding threats to student privacy, it is important that Common Rule protections remain in place.

Question 35. *Public comment is sought on whether the privacy safeguards of §__.105 should apply to the research included in §__.104(d)(1), given that such research may involve risk of disclosure of identifiable private information.*

EPIC Response: Meaningful privacy safeguards must apply to this research, particularly in light of the growing threats to student privacy. However, because the NPRM does not include specific information about the privacy safeguards of §_.105, EPIC can offer only speculative commentary as to whether the forthcoming safeguards will be adequate. If the privacy safeguards of §_.105 are modeled on the HIPAA standards, these measures will not be adequate. See EPIC Response to Question 22 for additional discussion of HIPAA.

Question 39. *Public comment is sought on whether this exemption category should only apply to research activities in which notice is given to prospective subjects or their legally authorized representatives as a regulatory requirement. If so, comment is sought on what kind of information should be included in the notice, such as the research purpose (if authorized deception is not utilized), privacy safeguards, contact information, etc. Would requiring notice as a condition of this exempt research strike a good balance between autonomy and beneficence?*

EPIC Response: EPIC opposes this proposed exemption, which fails to consider any potential privacy risks as criteria for qualifying activities and furthermore would exempt these activities from compliance with privacy safeguards under the Common Rule.

However, should this exemption be retained in the final rule, providing notice is preferable to leaving subjects uninformed and unaware. Respect for a human subject's autonomy and dignity requires at least basic awareness of the type of research being conducted and how the results may be used and disclosed. The concept that participation is implied consent when a purported

[31] Common Rule NPRM at 111.

subject has no idea how his information will be used undermines respect for persons and their autonomy.[32]

Question 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.*

EPIC Response: Because the NPRM provides no description of any potential decision tool for exemption determinations, substantive commentary on this question is limited. However, EPIC supports additional administrative review and documentation for all uses of exemption decision tools. Oversight of researchers or independent decisionmaking is particularly important to the proposed research activities at §__.104(d)(3). According to the NPRM, "benign interventions would be brief in duration, harmless, painless, not physically invasive, not likely to have a significant adverse lasting impact on the subjects, and it would be required that the investigator has no reason to think the subjects will find the interventions offensive or embarrassing."[33] The determination of whether a research activity is "offensive or embarrassing" is subjective and fact-specific; interested parties and automated algorithms are ill-suited for the task.

Question 45. *Public comment is sought on whether the proposed exemption regarding the use of educational tests, survey procedures, interview procedures, or observation of public behavior (§__.104(e)(1)) should be applied to research involving the use of educational tests with children and whether it should also be applied to research involving the use of survey or interview procedures with children. If so, for research involving children, should the permissible survey or interview topics be limited in some way?*

EPIC Response: The exemption proposed at §__.104(e)(1) should not be extended to children. As specifically noted in the Belmont Report, "Respect for persons incorporates at least two ethical convictions: first, that individuals should be treated as autonomous agents, and second, that persons with diminished autonomy are entitled to protection."[34] This principle compels the greatest amount of protection to children who are subjects of research.

d. Informed Consent

Question 60. *What topics should be addressed in future guidance on improving the understandability of informed consent?*

EPIC Response: EPIC appreciates the efforts in the NPRM to improve the informed consent process for individuals. Future guidance should clarify that informed consent should specifically address potential informational harms and privacy risks. The data security safeguards protecting

[32] The Belmont Report at 23,193.
[33] Common Rule NPRM at 125.
[34] The Belmont Report at 23,193.

the research data should also be disclosed. Given the rise in health care data breaches, whether a researcher employs adequate security measures is an important factor to consent.

e. Broad Consent for Secondary Research

Question 61. *Public comment is sought on whether broad consent to secondary research use of information and biospecimens collected for non-research purposes should be permissible without a boundary, or whether there should be a time limitation or some other type of limitation on information and biospecimens collected in the future that could be included in the broad consent as proposed in the NPRM. If a time limit should be required, is the NPRM proposal of up to 10 years a reasonable limitation? Would a limitation related to an identified clinical encounter better inform individuals of the clinical information and biospecimens that would be covered by a broad consent document?*

EPIC Response: EPIC supports limits on information and biospecimen collection in the future that is subject to the broad consent previously provided. EPIC supports the limitation suggested in the NPRM that would limit broad consent to "(1) clinical information and biospecimens already existing at the institution at the time broad consent was sought, and (2) clinical information and biospecimens collected as part of an identified clinical encounter."[35]

f. Waiver of Informed Consent

Question 70. *Public comment is sought on the proposed prohibition on waiving consent when an individual has been asked to provide broad consent under §__.116(c) and refused. In particular, how would this prohibition on waiving consent affect the secondary research use of identifiable private information? If an individual was asked to provide such consent, should the absence of a signed secondary use consent be considered a refusal? Does this prohibition on waiving consent for the secondary use of identifiable private information create a disincentive for institutions to seek broad secondary use consent and instead seek a waiver of consent from an IRB? Under what circumstances, if any, would it be justified to permit an IRB to waive consent even if an individual declined or refused to consent?*

EPIC Response: EPIC strongly supports the prohibition of overriding an individual's refusal to consent to unidentified future research uses of identifiable private information and biospecimens. Broad consent should be treated as an opt-in, not an opt-out, requirement for secondary research. Thus, the default presumption should be that an individual's failure to affirmatively agree constitutes a refusal of broad consent. A presumption of consent or the ability to override an individual's refusal to consent would seriously disrespect personal autonomy and dignity.

g. Definition of "Minimal Risk"

Question 79. *How often should the Secretary's list of minimal risk activities be updated? Should advice be solicited from outside parties when updating the list?*

[35] Common Rule NPRM at 183.

EPIC Response: EPIC supports retaining the current rule permitting expedited review only if the reviewer makes a separate determination that the research activity does not involve more than minimal risk. EPIC also urges modification of the definition of minimal risk in the context of informational or privacy risks. As witnessed by increasingly frequent reports of high-profile data breaches, significant privacy risks are "ordinarily encountered in daily life." §___.102(i). To fulfill the NPRM's stated goal of increasing privacy protections for human subjects, a heightened standard must be applied to informational and privacy risks.

Additional Comment on Data Protection Obligations

EPIC also urges the agency to develop, in the context of proposed revisions to the Common Rule, clear guidance on the data protection obligations associated with the collection and use of personally identifiable information in the medical research context. Modern privacy law is based on the view that those who collect and use personal information have a serious ongoing obligation to the data subject that are broadly described as "Fair Information Practices."

Conclusion

In conclusion, EPIC urges HHS to include provisions in the Common Rule that account specifically for informational and privacy risks, and which reduce the discretion of researchers to make subjective risk determinations in this context. EPIC further urges HHS not to exclude research activities involving human subjects from Common Rule coverage, which would increase privacy risks for human subjects. EPIC urges HHS to solicit additional comments on the NPRM proposals after issuing detailed descriptions of the decision tool for exemption determinations, the broad consent form, and the data security standards of §___.105. Finally, EPIC urges the agency to establish clear data protection standards for the collection and use personally identifiable information in the medical research context.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Fellow