To: The Department of Health and Human Services, Office of the Secretary, and Food and Drug Administration

Regarding the Notice of Proposed Rulemaking: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, Docket ID number HHS–OPHS–2015–0008

Via Regulations.gov

January 6, 2015

The Electronic Frontier Foundation (EFF) appreciates the opportunity to comment on the Notice of Proposed Rulemaking (NPRM) on human subjects research protections that appeared in 80 Federal Register 53931 (September 8, 2015). We mostly address privacy issues raised by the NPRM.

Summary
We appreciate the NPRM's effort to impose greater privacy and security protections overall, but remain extremely concerned. With respect to biology and medicine, the NPRM overemphasizes research at the expense of human subjects' privacy and autonomy, and robust informed consent mechanisms are necessary (though not sufficient). Perhaps the most glaring problem in the proposed Rule is its weak update of the ethical practices around biospecimens. The NPRM correctly recognizes that the current Rule's failure to require informed consent for secondary research performed on "non-identified" biospecimens is a serious problem given that biospecimens containing DNA are not only identifiable in theory, but more likely to be identifiable as a practical matter, given the rise of genetic databases. See generally https://www.eff.org/deeplinks/2012/12/rapid-dna-analysis; https://www.eff.org/deeplinks/2011/07/fbis-next-generation-identification-database. Unfortunately, the updated Rule would implement its informed consent requirement via a broad consent for future research, under which any such research would be "exempt" research that would not require annual continuing review by an institutional review board (IRB). We seriously question this approach.

I. HIPAA Privacy Rule Exception

Section ____.101(b)(2)(iv) exempts activities covered under HIPAA, and Question 24 of the NPRM asked whether "additional or fewer activities regulated under the HIPAA Privacy Rule should be included in this exclusion." 80 FR 53953. This exemption should be removed, or at the very least narrowed significantly to not exclude "research" as contemplated by the HIPAA Rules. *See* 80 FR 53952-53.

This exemption rests on the false assumption that the existing statutory regime is up to date ethically and constitutionally. The mistake of deferring to outdated and insufficient privacy protections also appears when discussing §____.101(d)(2), describing HIPAA and other Federal rules as containing "appropriate privacy, confidentiality and security safeguards." 80 FR 53958.

As the Supreme Court reaffirmed recently in *Riley v. California*, 134 S. Ct. 2437 (2014) and *United States v. Jones*, 132 S. Ct. 945 (2012), changes in technology and societal expectations often outpace static federal protections. Until *Jones*, individuals lacked any Fourth Amendment "reasonable expectation of privacy" when in public, such as while driving on public roads; until *Riley*, entire smartphones could be searched "incident to arrest" without a search warrant. Therefore, even if HIPAA or other federal privacy statues and regulations have not yet been found to violate a backwards-looking constitutional minimum, they are not designed to bear the kind of burden that this forward-looking ethical rule would put on them.

The Belmont Report principles require more, and any rule based on the principles in the Belmont Report must not abdicate privacy merely because some other statutory regime could conceivably meet some ethical or constitutional minimum.

The Common Rule cannot merely assume that existing law adequately considers the modern importance of respecting patients' autonomy and privacy. An inherent weakness of HIPAA is that its Privacy and Security Rule only applies to "covered entities" and their business associates. When treatment providers and other entities subject to HIPAA disclose data to, for example, state government entities for public health purposes, such data is no longer protected by HIPAA unless the government entity is already subject to HIPAA. *See generally* https://www.eff.org/issues/public-health-reporting.

Furthermore, as we noted in our 2011 comments on the ANPRM, advances in re-identification seriously challenge the value of de-identification, and the technical debate over the arms race between de-identification and re-identification continues. *See, e.g.*, Arvind Narayanan & Edward W. Felten, *No silver bullet: De-identification still doesn't work* (July 9, 2014) http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf. Especially because of the current "big data" and "open data" trends, we repeat our previously expressed concern: "An important aspect of this problem is that re-identifiability is a function of both the putatively de-identified data set and other available data. Thus, it may be impossible to know if data is effectively de-identified, as a dataset that is de-identifiable today may become identifiable tomorrow, after more information is available."

II. Technological Advancement Supports More Fine-Grained Consent

HHS asserts that because of "big data" and algorithms, "when there are appropriate privacy protections in place, the balance between respect for persons and beneficence should come out in favor of facilitating the research, including not requiring informed consent in many instances." 80 FR 53976. In our view, this approach flies in the face of the Belmont Report principles.

It is true that advances in data storage and analysis make research easier now than before, but it also makes it much easier to attach permissions and consent to specimens and to enforce these limitations on consent. HHS cannot merely claim the benefits of big data on the research side without acknowledging the parallel impact it has had on the first Belmont principle of "respect for persons".

First, computational and data-storage advances have increased the ease with which researchers can receive, track, send, and enforce fine-grained consent on the same databases they will be manipulating to perform their research.

Second, this ease of data transfer has had a paradigm-shifting impact on the ability of entities to aggregate deep databases on individuals—the disclosure of which have much more of an impact on patient privacy than the disclosure of databases did in the past. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1704 (2010). As the White House Big Data Review team stated: "The advent of more powerful analytics, which can discern quite a bit from even small and disconnected pieces of data, raises the possibility that data gathered and held by third parties can be amalgamated and analyzed in ways that reveal even more information about individuals. What protections this material and the information derived from it merit is now a pressing question." EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 34 (2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Finally, more than two Belmont Report principles are relevant to the discussion. The third principle requires the consideration of justice, and "big data" analysis can exacerbate hidden biases while its underlying databases often fail to adequately reflect the preferences of historically disadvantaged groups. *See* Big Data: A Tool for Inclusion or Exclusion? FTC REPORT 28, 27 (Jan. 2016), *https://www.ftc.gov/reports/big-data-tool-inclusion-or-exclusion-understanding-issues-ftc-report*. This approach reflected in the NPRM is an example of when "overreliance on the predictions of big data" results in "not thinking critically about the value, fairness, and other implications of the[] uses of big data" on those historically marginalized by society and human subject researchers. *See id.* at 31.

III. Broad Consent

You requested comment on "the value to the public and research participants of being asked their permission for research use of their data and biospecimens." 80 FR 53965. We believe there is immense value in ensuring that individuals give fine-grained, un-coerced, informed written consent for secondary analyses of each specific biospecimen. We are gravely concerned about any rule permitting innumerable and/or perpetual secondary analyses of biospecimens merely after receiving blanket consent for future secondary uses that fall below a threshold of "identifiable".

As noted above, the current Rule does not require informed consent for secondary research performed on "non-identified" biospecimens. By contrast, the proposed Rule would require "informed consent for the use of stored biospecimens in secondary research (for example, part of a blood sample that is left over after being drawn for clinical purposes), even if the investigator is not being given information that would enable him or her to identify whose biospecimen it is." 80 FR 53936.

Unfortunately, the updated Rule would implement this requirement via a broad consent for future research, under which any such research would be "exempt" research that would not require annual continuing review by an IRB. We seriously question this approach. First, broad consent to future research is arguably the least meaningful form of individual consent. The human

subject will not know what the future biospecimen research entails, how it will affect him or her, how the biospecimen or research data will be shared, or which biospecimens they can expect to provide in the time period that this consent is presumed valid for.

Second, while genomic-related research and technology is of great potential benefit, its rapid evolution also presents significant risk and uncertainty to privacy and social control, especially given the increasing use by law enforcement and government of genetic identification. And quite apart from the concerns about government access, use or disclosure of genetic data raises ethical and privacy issues for individuals in the employment and other private-sector contexts. IRBs are a primary mechanism for ethical oversight of research involving human subjects, in partnership with government bodies such as the National Institute of Health's Office for Human Research Protections. Thus, IRBs represent a critical venue for ongoing debate and implementation of ethical norms in the context of concrete proposed research. Exempting this category of research from IRB review undermines this entire oversight process for an area that we expect will present enormous ethical problems as it evolves. Review should at a minimum require specification, evaluation and public disclosure of de-identification protocols.

Even if individual IRBs are satisfied that an individual public researcher is not running a secondary analysis that will allow a person to be identified, this would create a regime in which blanket consent attaches to a series of identifiable specimens and permits innumerable tests so long as they each fall below a uniformly-defined identifiability bar. Trusting individual IRBs to consider whether an individual test is one test too far is unrealistic. Furthermore, different individuals will have different reasonable preferences about which kinds of tests are too invasive of their privacy and when the cumulative effect of individual tests has crossed their individual threshold of comfort.

Therefore, we urge you to reject any notion of "broad consent" unless it is limited to cover only the biospecimen taken at that time, allows human subjects to opt into specific kinds of research while opting out of others, and permits patients to set their own time limit on how long each specimen can be used. The current formulation does not strike the proper balance and violates patients' autonomy rights. Given a sufficiently comprehensible and comprehensive list of the kinds of research proposed, a member of the public could choose to offer absolute broad consent, but should also be permitted to offer targeted broad consent for only certain kinds of secondary research on certain biological specimens limited after a certain period of time elapses.

A. Burden of Individual Tracking

The NPRM does not sufficiently explain why it believes that "individual tracking" of test subjects is too burdensome. This assertion appears on 80 FR 53974 as an explanation for why the NPRM finds blanket broad consent sufficient, and does not require researchers to track individual specimens and how they are tested. ("[I]t was determined that limiting the scope of the broad consent in this manner would be very difficult to implement and would require rigorous tracking on an individual-subject basis. Therefore, this proposal was not included[.]") Claiming that this requirement would be "difficult to implement" is factually questionable, and even if it were burdensome, this burden must be balanced against the added respect for individual autonomy that such a tracking system would bring.

i. The Burden of Tracking

Many of the "problems" of tracking specimens disappear if consent is sought after each specimen collection instead of at the beginning of a 10-year period. But even if not, the tracking problems could be addressed easily by requiring the researcher to attach a unique identifier that accompanies any biological specimen used for secondary research. The HIPAA Privacy Rule, for instance, permits a covered entity to assign to, and retain with, the de-identified health information, a code or other means of record re-identification if that code is not derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. This is minimally burdensome, and would require either hosting an API (Application Program Interface) that distributes which permissions attach to a particular specimen of a particular individual when queried, or adding additional columns to a properly encrypted/protected/handled database that is sent along with the specimens.

Implementing a tracking system that would enable an individual—or a representative of the public like a state attorney general—to determine who has their specimens and for which purpose would make it much easier to solve many of the other allegedly burdensome problems the NPRM identifies. For example, if the specimens may only be used if the researcher reports which specimens they are using and which information they intend to extract, then the researcher can query the database for fields that record a more fine-grained consent for secondary research. An individual could therefore offer consent for only certain kinds of experiments, and could require that information to be received by researchers before they undertake any experiments. And before a person undertakes research on the specimen, they could be required to confirm that their study fits into the permission granted from the human subject, and to check with the original specimen-collecting researcher to confirm that the cumulative information gathered from the tests will not surpass the human subject's individual de-anonymization threshold.

More fundamentally, even if individual tracking turns out to be a burden on researchers, that is not sufficient to totally ignore the value a tracking process can have on respect for an individuals' wishes. The NPRM notes that this is burdensome, and then fails to perform a balance as to whether this burden is justified. 80 FR 53974. Surely some burdens are justified under the principles in the Belmont Report, and (given the large increase in autonomy that the NPRM admits better tracking would create) *id.,* the decision to list *no* "Non-quantifiable Costs" in Table 24 (summarizing the estimated benefits and costs of obtaining consent to secondary use of biospecimens) is a strong indication that this decision was unsupported by the evidence on the record. 80 FR 54021.

ii. Already Tracking Some Information

Presumably, some information would already be sent along with the specimen (like the date of collection and the date of broad consent) in order to enforce the proposed 10-year limit. 80 FR 53974 (Question 60 asking for input on 10-year time-limit proposal). If the date and information about the consent given is already recorded directly on the specimen label, then all a tracking system would require would be a unique identifier leading to more information about the consent written on the same label. A researcher could then use this information to look up the specimen in the accompanying spreadsheet sent with the specimen, or could access an API (maintained online either by the researcher, their institution, or some centralized agency) that will return what

specific secondary research consent the individual who provided the specimen gave and which tests have already been performed on this specimen.

iii. Aggregating Tests' Impacts on Patient Privacy

This tracking would also help solve one of the other major problems this NPRM elides. Again, Question 61 asks "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."

It is imperative that the concept of informed consent for secondary research reflect society's knowledge that individual tests can produce measurements that—when aggregated—can lead to identification. More specifically, this can permit either the public or researchers to associate the subject with biological, biographical, and behavioral facts that the subject might expect to remain private.

An IRB—when reviewing a proposed test—should be aware of all of the tests proposed and performed on a particular specimen, and on all specimens linked to the broad consent given, so that the IRB can know the history of this individual's specimens and assess whether this proposed research will tip the scales.

IV. Review of Exclusion Determinations

Questions for public comment 27-33 concern the NPRM's proposal for policing the boundary between exempt and non-exempt activities. 80 FR 53956-57. Although §___.101(c) does announce that the department or agency head retains the final judgment as to whether "a particular activity is covered by this policy"—presumably under all of §___.101(b)—this section is far too deferential to both the researcher and the department/agency head.

Our primary concern here is to preserve meaningful oversight, which we believe requires after-the-fact accountability. The NPRM must lay out a more substantive process mandating more than one level of appeal/review by a human in all but the most clear-cut examples. Because this is a uniquely dispositive decision, in order to provide certainty that the department or agency head actually considers the "ethical principles of the Belmont Report" HHS should consider whether to include in the Common Rule a sanction or private cause of action against the researcher and the department or agency head for erroneously granting an exemption.

Question 27 asks "how likely it would be that institutions would allow an investigator to independently make an exempt determination for his or her own research without additional review by an individual who is not involved in the research and immersed in human research protection e.g., a member of the IRB Staff." But likelihood is the wrong question. The correct question is—if *any institution* might allow this non-IRB-reviewed process, how can human subjects be protected?

It is extremely likely that—absent an explicit prohibition—some institution will trust an investigator to report their own activities and choose what to report to the funding

department/agency. Deciding to exclude this prohibition because HHS assumes it will not be violated often enough ignores the history and purpose of the Common Rule. Why assume compliance? Why not set it as a minimum requirement—the violation of which is punishable? Any institutions that fall below this threshold—which HHS apparently believes is an important safeguard—will then be in violation of the Common Rule. Any parties who in any event would have required IRB (or a similar) review of this exemption determination will not be impacted at all. Therefore, if this review is as straightforward as the NPRM seems to believe, then the only danger the requirement imposes falls on those institutions that take an inordinate risk.

Questions 28 asks for public comment on "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." If the tool does anything but approve the most obvious cases, the answer is yes. The only way to catch those who will "contrive his or her responses" is to build review by humans into the system in all but the most obvious cases. The NPRM should reflect this preference, and state clearly that the automated system will only be useful for screening out the easy cases.

Even if not all of these decisions are reviewed, HHS should designate some subsets that definitely are reviewed. For example, we believe that the proposed Rule should contain an explicit guarantee that a person makes the following in-or-out decisions on a record that permits meaningful review (some of which are discussed in more detail in IV.A and IV.B *infra*):

- Whether an activity is epidemiological research or a public health surveillance activity. *See* 80 FR 53949.
- What are "related analyses" under the Intelligence Surveillance Activity exception. *See* 80 FR 53950.
- Whether a particular proposed activity falls is one of the permitted "related analyses" in this Intelligence Surveillance Activity exception. *See id.*

For all but the easiest cases, even if HHS drafts a uniquely comprehensive and thoughtful tool for eliciting responses, there will be ways of describing research that evade any automated tool detection. Language is fungible. Cases based solely on the interpretation of statutory or regulatory language routinely go through administrative review and two lower levels of Article III courts before they land at the supreme court and elicit sharply divided decisions. *Cf. Nat. Fed. of Indep. Bus. v. Sebelius*, 132 S. Ct. 2566 (2012) (determining that individual mandate was a "tax" under the Constitution, but was not a "tax" under the Anti-Injunction Act). An individual investigator reviewing an online automated form will have the opportunity to respond to even the best formulated questions with answers that are not false, but which will evade revealing the relevant information that would trigger review.

Therefore, as for Question 33, the proposed audit requirement would be a necessary but insufficient component of a review process that adequately reflects the balance required by the Belmont Report. 80 FR 53957.

A. Intelligence Surveillance Activity Exemption

One of the more problematic exemption-decisions will be about whether an activity is an intelligence surveillance activity under §____.101(b)(1)(vi). Oddly, the NPRM does not seek

public comment addressing this particular exemption. *See* 80 FR 53950. This determination should be subjected to a particularly stringent review process because of these agencies' long histories abusing human subjects through creative interpretation of their mandates. *See Project MKULTRA, The CIA's Program of Research in Behavioral Modification: Joint Hearing of Select Comm. on Intelligence and Subcomm. on Health and Sci. Research of S. Comm. on Human Resources*, 96th Cong. 69-72 (1977) (Appendix A), http://www.nytimes.com/packages/pdf/national/13inmate_ProjectMKULTRA.pdf; *see also* Memorandum from John C. Yoo, Office of Legal Counsel, U.S. Dep't of Justice to William J. Haynes II, General Counsel of the Department of Defense, *Re: Military Interrogation of Alien Unlawful Combatants Held Outside the United States*, (Mar. 14, 2003), https://www.aclu.org/files/pdfs/safefree/yoo_army_torture_memo.pdf.

As a preliminary concern, the NPRM claims to be "codify[ing] the current interpretation of the Common Rule." 80 FR 53950. It is unclear to us what authority supports this claim. This was not apparent from the ANPRM, and is not identified in the NPRM. Second, if HHS believes that this authority justifies the exemption, it should identify the reasoning it found persuasive when deciding to codify the existing interpretation. At present, it is doubtful that this claim is supported by the record.

The NPRM includes "surveillance activities and related analyses" in the exemption, and HHS should offer more guidance as to what the undefined "surveillance activities" refers to, and what "related analyses" will qualify for this proposed exemption. They apparently must be "related" to "surveillance activities," but this offers practically no limitation to an intelligence community with a history of expansively interpreting limited exemptions. There should be a discussion, a representative list, or at a minimum a modifier added here to give future courts or administrative law judges some sort of applicable standards to apply if a dispute arises.

In addition, the NPRM should clarify that the exemption only applies to biospecimen analysis if the biospecimen was collected for that particular use, and by a "defense, national security, or homeland security authority solely for authorized intelligence, homeland security, defense, or other national security purposes." 80 FR 53950. As presently written, the language appears to potentially allow for the "use" of a biospecimen that was "collected" by a different agency, "collected" for a different purpose, or both.

This is especially problematic given that HIPAA's national security exception currently permits doctors, hospitals, and any other "covered entity" to disclose individual health information "to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act" without patient authorization. 45 C.F.R. § 164.512(k)(2); *see* https://www.eff.org/issues/national-security-and-medical-information.

HHS should clarify that the NPRM language only allows for an exemption if a listed agency collected *and* used the biospecimen for a specific covered purpose, or for multiple purposes defined *ex ante* the collection. It would be perverse indeed for the updated Common Rule to quietly facilitate the creation or expansion of a permanent intelligence community biospecimen bank.

B. Public Health Surveillance Exemption

We are also concerned with the public health surveillance exemption under §____.101(b)(1)(v). Although this exemption is more fully fleshed out than the intelligence surveillance activity exemption, it still has significant problems.

This exemption permits for data collection that would enable public health authority to predict a public health outbreak. The NPRM should include explicit limitations on which kinds of data can be collected before the activity falls outside of this exemption and an IRB is required. Currently the NPRM asserts that the difference between "epidemiological research" and "public health surveillance" can be determined by analyzing "the purpose or context in which the investigation is being conducted and the role of the public health authority." 80 FR 53949. This should explicitly include an instruction to examine the kind of data being gathered, and should note a presumption that an activity is "epidemiological research" if it collects non-specimen data that correlates—or would be expected to correlate—to sensitive biographical/biological and lifestyle attributes.

V. Disclosure of Surprising Results to Human Subjects

Section ____.104(f)(2) demonstrates that the NPRM prioritizes receiving benefits from secondary research on biospecimens too strongly over considering the interests of the human subjects who provided that biospecimen. Specifically, if exempted research comes up with a surprising result that would be of interest to an individual, there is no IRB or federal review mandated to determine whether those who were studied to discover this information should be able to directly benefit from this information.

HHS justifies this by deciding that the IRBs and federal agencies do not have any special expertise in determining whether information is sufficiently important and useful to justify reaching out and informing people that their specimens were still being analyzed. *See* 80 FR 53967. HHS claims that the IRBs' decisions would create unjust "variability," 80 FR 53967, but this assumes that IRB review duplicates the researcher's original decision process, and ignores the positive benefits of the process of memorializing and justifying one's decisions to an impartial observer.

Given the positive benefits of implementing a tracking system as discussed above, the minimal logistical and monetary cost of this implementation, and the ease with which a researcher could track down the identity of a human subject if necessary, the Belmont Report principles favor requiring a researcher to present results to a reviewer to determine when it is necessary to spread some of the research's benefit back to those generous enough to provide consent for the tests. As we noted in our ANPRM comments, "A significant segment of the public harbors a deeply rooted mistrust of medical research. They do not trust physicians and scientists to be open and honest with them. They fear that the privacy of their medical records will not be respected. They believe that someone somewhere is making a lot of money off of drugs and biological products that were developed using pieces of tissue from people who now are entitled to a piece of the profits. *The Immortal Life of Henrietta Lacks* speaks to that skepticism, and above all is the vivid testament of how the Lackses feel they've been treated by physicians, researchers, journalists,

and corporations." Dale Keiger, *Immortal Cells, Enduring Issues*, Johns Hopkins Magazine (June 2, 2010), http://magazine.jhu.edu/2010/06/immortal-cells-enduring-issues/

VI. Minimally Invasive Procedures Exemption

Question 56 asks for comment on whether there should be an exemption for biospecimens collected through minimally invasive procedures. 80 FR 53967-68. As it stands, this proposal is under-defined and would leave many troubling questions unaddressed. For example, there is no definition of which 'procedure' is relevant and when the analysis begins. Specifically, after an invasive surgery, is swabbing or sampling of the leftover tissue an invasive procedure? Does it matter that the surgery was necessary?

Regardless, it would be a grievous error to create such an exemption. The relevant dangers reflected in the Belmont Rule's respect for individual autonomy include learning too much about an individual, not merely the invasion of an individual's body. Human beings shed cells everywhere, and it is already true that biospecimens are collected with non-invasive procedures, such as saliva from drinking glasses or sweat and skin cells from the arms of a chair.

If a minimally or non-invasive procedure has minimal privacy implications, then IRB review will be easily passed or the process will be expedited or exempted. Physical invasiveness is not a proxy for the genetic and other informational privacy issues raised by biospecimen research.

VII. Observation of Public Behavior

The exemption allowing for non-reviewed studies of public behavior so long as the information is properly anonymised lacks a sufficient definition of what behavior is "public." According to the NPRM it includes behavior that is visually or auditorily recorded, but does not explain fully when a behavior is sufficiently public as to fail to garner any protection under the NPRM. For example, behavior disclosed to a specific third party should not be considered public merely because it occurs on the property of that third party, or because it is a necessary condition to accessing a good provided by that third party or another third party.

For example, information disclosed to Internet Service Providers including requests for pages and documents to be sent to a particular IP address should not be considered public merely because they are not occurring in a single physical place in one person's home. This is true even if tools can be developed to observe this—and only this—information from a "public" place that the information happens to pass through on its way to a destination.

Respectfully submitted,

Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109