3108 Fifth Avenue
Suite B
San Diego, CA
92103

Comments of the World Privacy Forum

To: the Office for Human Research Protections, US Department of Health and Human Services; Department of Education; National Science Foundation, and other agencies

Regarding: Federal Policy for the Protection of Human Research Subjects NPRM, Docket ID number HHS-OPHS-2015-0008

Via Federal eRulemaking Portal regulations.gov.

Jerry Menikoff, M.D., J.D.
Office for Human Research Protections (OHRP)
Department of Health and Human Services
1101 Wootton Parkway
Suite 200
Rockville, MD 20852

January 5, 2016

Re: Federal Policy for the Protection of Human Research Subjects, NPRM, Docket ID number HHS-OPHS-2015-000880

The World Privacy Forum welcomes the opportunity to respond to the Department's request for public input on its Notice of Proposed Rulemaking (NPRM) on the Federal Policy for the Protection of Human Research Subjects, Docket ID number HHS-OPHS-2015-000880, 80 FR 53933.[1] The World Privacy Forum is a non-profit public interest research and consumer education group. We have published many research papers and policy comments focused on privacy and security issues. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and many other rapidly evolving areas in the privacy

[1] Original notice: https://federalregister.gov/a/2015-21756

field. We have published significant reports about health data and privacy, including our Medical ID Theft report, the first to bring this topic to public attention, and our Patient's Guide to HIPAA, among others. We have also published significant reports on data analytics, including The Scoring of America, a report more than seven years in its research. You can see our publications, prior comments to HHS, and more information at www.worldprivacyforum.org.

I. General Comments

The NPRM's goal of improving the current system and focusing attention on more risky activities is perfectly reasonable. We recognize that is it easy to say that there should always be more review, but resources for review are scarce. Efficiency in human subjects protection is a reasonable objective. Institutional Review Boards (IRBs) review many more projects today than they should. Our objective in these comments is to make sure that privacy concerns do not get lost while revamping the Common Rule. We do not believe that there is any inherent conflict in making the Common Rule work better while still protecting privacy.

We attempted to tie our comments to questions posed in the NPRM, but this was not always possible. We have given each question a heading for clarity.

II. Informational Risks

The NPRM takes an extremely narrow approach in its description of informational risks. We discuss specifics of these problems in this section of our comments, with suggestions and requests for modernizing and improving the NPRM's shortcomings with respect to informational risk.

First, though, we want to acknowledge that in general the NPRM does a better job of addressing informational risks than the current rule. We agree with the statement (p. 53940), and support it, although we would have used a stronger word than *suggest*.

> "The increase in concern about unauthorized and inadvertent information disclosure, in combination with newer research techniques that increase the volume and nature of identifiable data suggest the need for the Common Rule to more explicitly address data security and privacy protection."

In the preamble, the NPRM states (p. 53938):

> "As technology evolves, so does the nature of the risks and benefits of participating in certain types of research. Many studies do not involve interaction with research subjects, but instead involve, for example, analyzing information obtained from medical records, administrative claims data, education records, criminal justice records, research data shared through data repositories, and existing biospecimens stored in repositories. Risks related to these types of research studies are largely

> informational, not physical; that is, **harms could result primarily from the inappropriate release of information** and not from the research interventions themselves. Nonetheless, those harms can be significant."

The highlighted words illustrate that although improved, the NPRM's view of informational risk is focused mostly on data breaches. This is far too narrow, and respectfully, it is also an outdated approach. This is an important point — informational risk does not just equal the risk of unauthorized access. Risk has changed in ways that would have been difficult to imagine even five years ago. These other significant risks need to be accounted for in the NPRM. We will do our best to outline the most important points of this issue here.

The actual information risks begin with the collection and compilation of the data. The basic compilation of personal information by any record keeper (who may or may not be acting with the knowledge or consent of a data subject) exposes the data subject to an informational risk *regardless of the use and disclosure rules that apply*. While the NPRM correctly mentions data breach, which we support, the NPRM does not mention legal and permissible disclosure of the data through legal and judicial processes.

The NPRM needs to acknowledge that some information disclosures are legal, and yet are still beyond the control of any record keeper. Any litigant or agency with a subpoena and any law enforcement officer with a search warrant may be able to force disclosure of a record, regardless of the record keeper's disclosure policy. Had the records not been compiled in the first place, these risks might not exist. History has proven this point many times; we are not speaking theoretically here.

We note that certificates of confidentiality provide some protection against subpoenas. If the Common Rule required that all research activities that process personal information must have certificates of confidentiality, that might make a mild difference. However, certificates in fact only offer weak protections, so even a certificate helps only somewhat against the basic risks that arise when a researcher collects, compiles, and maintains personal information. Even if the NPRM adopted our previous recommendation for the ANPRM[2] that all research projects must obtain certificates of confidentiality, we would still make the point that compilation of personal data exposes data subjects to a broad and complex array of informational risks regardless of use and disclosure rules.

We think that the final rule needs to take a broader view — and frankly, a more modern view — of the full range of informational risks. We think that it is certainly possible for research to continue and that some of the limitations in the current rule can be eased notwithstanding these risks. The privacy needs of research subjects can be accommodated with modest controls, rules, and procedures. But the controls, rules, and procedures need to be extended past the concept of

---

[2] WPF Comments to HHS on Common Rule ANPRM, October 18, 2011. http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPF_CommonRule_Oct182011fs.pdf.

data breach as the only informational risk. We will discuss this point further in section IV, Minimal Risk of these comments.

III. Identifiability of Biospecimens and PII

> **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 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.

A. Identifiability of Biospecimens

On page 53940, the NPRM states:

> In the future, technologies will facilitate the use and analysis of greater variety and volumes of information, and there is a possibility that it will be increasingly difficult, if not impossible, to make biospecimens fully non-identified.

This future is here or, in the alternative, the future is so close that the Common Rule should assume that all biospecimens are identifiable. Why? The time between amendments to the Common Rule is measured in decades. By the time the federal government next amends the Common Rule, the identifiability of biospecimens will no longer be at issue but a fully-developed reality.

Consider the issue of informational risks. These risks have been present for a very long time, but the Common Rule is just now being changed to address those risks realistically. The same type of trajectory will occur with identifiability of biospecimens. We urged in our comments on the

ANPRM that biospecimens should be assumed to be identifiable, and that the Common Rule be adjusted accordingly.[3]

We repeat the same advice we offered earlier, and urge your consideration of making an update to the language here. If biospecimens are identifiable, then restrictions on use and disclosure that accompany transfers of biospecimens (or data from biospecimens) should control any activities by the recipient that might lead to identification of individuals.

Data use (or specimen use) agreements are likely to offer the best way to establish the terms of sharing. Standard agreements would be a step in providing suitable protections when specimens are used for research in ways not disclosed to or agreed to by the data subject. HHS could provide model agreements to help everyone adopt fair and comprehensive terms.

B. Support for the Definition of Personally Identifiable Information in the NPRM

Regarding the question about shifting to the term *personally identifiable information*, or PII, and using a widely-accepted definition already in use, we support this change. There is value is reusing familiar definitions regarding personal information when possible. In the end, definitions only get you so far. What constitutes personal information sometimes requires some human judgment, and definitions alone will not automatically resolve all questions.

We support the use in the Common Rule of OMB's concept of PII as quoted. It is a decent definition, as good as most, and already in use. There is no reason to reinvent this particular wheel. We note that there are several OMB variations of the definition of PII, this definition has been widely cited and published, and we agree with the choice of this particular definition.

IV. Minimal Risk

The definition of *minimal risk* is significantly deficient in the NPRM because it fails to address what constitutes a minimal informational risk. As a foundational point of the NPRM, this must be corrected.

The NPRM defines minimal risk as follows:

> §____ 102.(j) Minimal risk means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. The Secretary of HHS will

[3] WPF Comments to HHS on Common Rule ANPRM, October 18, 2011. http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPF_CommonRule_Oct182011fs.pdf.

> maintain guidance that includes a list of activities considered to involve no more than minimal risk. This list will be re-evaluated no later than every 8 years based on recommendations from the Federal departments and agencies and the public.

First, the focus of the definition seems to be on risks from **physical or psychological** examinations or tests. There is no hint that the definition even covers **informational risks**. This is a major shortcoming, and ties in with the deeply outdated view of informational risks in other sections of the NPRM.

It is not clear how or if the Common Rule's concept of minimal risk applies to informational risks. The risks to privacy *ordinarily encountered in daily life* are significant, poorly understood, and often hidden from the view of data subjects. This last comment relates only to commercial activities and not to risk posed by government surveillance.

Current debates over the use of information about Internet or cell phone users illustrate the point. Regular news reports highlight novel and often-secret data collection methods used by commercial companies in the pursuit of consumer profiles, more effective advertising, or increased profits.[4] Studies show broad gaps in popular knowledge about privacy.[5] Current debates in Congress and state legislatures provide additional evidence of the need for better privacy rules.

Whether the privacy risks *ordinarily encountered in daily life* is a fair standard for measuring informational risks in research is extremely doubtful. **Researchers should be held to higher standards than apply today in the unregulated marketplace for consumer data.** In other words, researchers should not behave like commercial data brokers such as Acxiom, Experian, and others. Most commercial participants not subject to the Common Rule can collect, compile, use, disclose, and sell consumer data without legal restriction. The abundance of health data has

---

[4] See, e.g., Center for Digital Democracy, *Examination of Online Direct-to-Consumer Prescription Drug Promotion* (2011) (Comments to Food and Drug Administration) ("Ongoing tracking and targeting of health users across the digital marketing system is a major concern not only for patient privacy, but also because such data is used to better hone campaigns designed to influence consumers in a myriad of ways. Health marketers strive to harness the data collection and analysis capabilities of online advertising in order to foster greater demand for prescription drugs. Unfortunately, little information is currently provided on what is being collected from users of health-related sites and how such data are used."), at http://www.centerfordigitaldemocracy.org/sites/default/files/FDAComments062711final.pdf.

[5] See Chris Jay Hoofnagle et al, *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* (2010) ("42 percent of young Americans answered all of our five online privacy questions incorrectly. 88 percent answered only two or fewer correctly. The problem is even more pronounced when presented with offline privacy issues – post hoc analysis showed that young Americans were more likely to answer no questions correctly than any other age group."), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. In other words, young and old alike did poorly on the test of privacy knowledge.

changed the equation where HIPAA-covered entities hold all of the data. The current wild west of consumer data is not a useful model for assessing research risks.[6]

Ongoing debates over the proper scope of the Fourth Amendment provide some lessons. A commonly used test to assess when privacy should fall under the protections of the Fourth Amendment comes from a concurring opinion in a seminal Supreme Court decision.[7] Under the test, a *reasonable expectation of privacy* exists if (1) a person has exhibited an actual (subjective) expectation of privacy; and (2) that expectation is one that society is prepared to recognize as reasonable. When this test is satisfied, a government search or surveillance activity that violates the reasonable expectation of privacy falls under the Fourth Amendment. The scope and applicability of the Fourth Amendment is not an immediate concern in the human subjects context.

The Fourth Amendment privacy test based on expectations is not much different from the standard in the Common Rule because both rely upon what is ordinarily encountered, routine, or expected. This brings us to the point. A well-recognized problem with the reasonable expectation of privacy test is the "silent ability of technology to erode our expectations of privacy."[8]

That is precisely the problem if the standard for minimal risk in the existing rule applies to informational risks. What is happening on the Internet and elsewhere is changing and eroding expectations of privacy. The judicial *expectation of privacy* test is now widely criticized for its lack of any real objective or fixed standard. No matter how the Fourth Amendment is interpreted by the courts, we need to do better in the research context. We cannot allow the *anything goes* practice of commercial Internet advertisers to affect standard for research conduct.

Researchers and IRBs cannot tell from the largely unchanged definition whether or how the standards apply to informational risks. Even though the NPRM's preamble offers a comment on this point (and a comment on this issue accompanying the final rule is the **minimum** change that we request on this issue), the existing definition leaves researchers without any idea how to apply the *ordinarily encountered in daily life* to informational risks.

Readers may simply conclude that the informational risks of any given research project are minimal because "everybody is on Facebook" anyway. Are risks minimal if I make data on Facebook available only to friends? What about friends of friends? Researchers could also draw conclusions about informational risk because some technology companies already collect a wide

---

[6] See WPF's Congressional testimony regarding this issue: *Testimony of Pam Dixon before the Senate Judiciary Committee, Data Brokers — Is Consumers' Information Secure?* November 3, 2015 http://www.judiciary.senate.gov/imo/media/doc/11-3-15%20Dixon%20Testimony.pdf, and *Testimony of Pam Dixon before the Senate Commerce Committee, What Information Do Data Brokers Have on Consumers?* http://www.worldprivacyforum.org/wp-content/uploads/2013/12/WPF_PamDixon_CongressionalTestimony_DataBrokers_2013_fs.pdf.

[7] *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[8] See, e.g., Paul Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 Iowa Law Review 553, 573 (1995).

variety of data, from online data, to sensor data in watches, cars, and other devices, and even cell phone data. For example, some mobile phone health apps collect telephone call meta data and SMS text meta data.[9] Over time, rich health data from many novel sources will become abundant, well beyond the constraints of HIPAA, which will change the norms of how the data is viewed in terms of its accessibility and risk.

The activities that modern companies — from search engines to social media to telecom companies to car companies — undertake to collect and monetize consumer data are not standards that should apply to human subject research. Human subject research needs a higher and clearer standard. Without clearer guidance, we worry that a researcher might, for example, take note of the many websites where patients publicly and knowingly share their personal medical history and decide that a research project poses relatively fewer privacy challenges and therefore the projects must be okay. It is too easy for someone who wants to use another person's data to find a justification if the standard is vague and too flexible. That is what bothers us about the minimal risk standard as applied to personal information.

To summarize, the issue is not whether there is minimal informational risk. When there is PII, there is informational risk. There must be privacy and security policies that address the risks involved. Minimal risk may not be a meaningful threshold test for informational risk. No finding of *minimal risk* based standards found in ordinary life should exempt any research project with PII or potentially identifiable data from formally considering and addressing informational risks.

We want to make it clear that assessing informational risks is harder because of rapid changes in personal information processing by industry and by government. We want to emphasize three points in particular.

First, the basic compilation of personal information by any record keeper (who may or may not be acting with the knowledge and consent of a data subject) exposes the data subject to an informational risk *regardless of the use and disclosure rules that apply*. We expand on this point elsewhere in these comments.

Second, researchers and IRBs are not necessarily able to make assessments of informational risks. The online world changes so fast and requires so much attention that any casual observer will be left behind. Most researchers simply do not have the time or the skills to keep up with developments.

---

[9] See for example, Ginger.io, a mental health app.The privacy policy states (excerpt) "All such collected data (collectively, "User Interaction Data ") may include how and when you use your mobile device for communications with others, including mobile phone and text use, and your location and speed of movement while you use your mobile device. Such User Interaction Data may also include, but is not limited to, call information, SMS information (see Safeguards below), location samples, accelerometer samples, smartphone actions, and smartphone screen-time related to, or resulting from, your use of the Services." https://ginger.io, accessed Jan. 5, 2016.

Third, even information that may seem innocuous can be analyzed and used in a way that harms individuals. WPF issued a report recently on consumer scoring, which is one aspect of the market for consumer data.[10] The report – *The Scoring of America* -- documents the range of personal information already being used in the marketplace today, and how its analysis impacts consumers.

As we discuss consumer scores, keep in mind that we are not talking primarily about credit scores subject to regulation under the Fair Credit Reporting Act. The credit score is regulated, but the thousands of the rest of the scores in use today are not. New and "big data" is being used to replace the regulated data and provide proxies for the same information.

These data elements below are available for and used in hundreds or thousands of consumer scores. The list was compiled from multiple sources, and intensively sourced and researched. It is not just a list of ideas or words, it represents real data points being sold routinely about real people.

Demographic Information:

- Age
- Age range
- Date of birth
- Education
- Exact date of birth
- Gender
- Marital status
- Home ownership
- Own or rent
- Estimated income
- Exact income
- Ethnicity
- Presence of children
- Number of children
- Age range of children
- Age of children
- Gender of children
- Language preference
- Religion
- Occupation - category of occupation

[10] World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (April 2014), http://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

- Examples: Beauty (cosmetologists, barbers, manicurists) civil servants, clergy, clerical/ office workers, doctors/physicians/surgeons, executives/administrators, farming/ agriculture, health services, middle management, nurses, professional/technical, retail service, retired, sales, marketing, self-employed, skilled/trade/machine operator/laborer, teacher/educator.
- Occupation - title of occupation
- Military history
- Veteran in household
- Voter party
- Professional certificates (teacher, etc.)
- Education level reached or median education

Sensor and bio data:

- Biometric data (iris scan, voice prints, fingerprints, faceprints, etc.)
- Sensor-generated data (bio-sensor data from fitness and health devices and apps)

Contact Information:

- Full name
- Email address
- City
- State
- ZIP
- ZIP + 4
- Home Address
- Land-line phone
- Social IDs / social media handles and aliases
- Mobile phone number
- Carrier
- Device type
- Email address

Vehicles:

- Vehicle make, model and year
- VIN
- Estimated vehicle value
- Vehicle lifestyle indicator
- Model and brand affinity
- Used vehicle preference indicator

Lifestyle, Interests and Activities data (including medical):

- Antiques
- Apparel (women, men & child)
- Art
- Average direct mail purchase amounts
- Museums
- Audio books
- Auto parts, auto accessories
- Beauty and cosmetics
- Bible purchaser
- Bird owner
- Books
- Book purchases - plus types. (Mystery, romance, religious, etc.)
- Book clubs
- Career
- Career improvement
- Cat owner
- Charitable giving indicators:
- Charitable donor by type of donation (religious, health, social justice)
- Charitable donor by ethnicity or religion (Jewish donors, Christian donors, Hispanic donors)
- Charitable donor by financial status (wealthy donors)
- Children or teen interests
- Fashion and clothing (Multiple: sports, high fashion, shoes, accessories, etc.)
- Collectibles
- Collector
- Christian families
- Computer games
- Computers
- Consumer electronics (Many categories, including electronic fitness devices)
- Dieting and weight loss
- Telecommunications and mobile
- Dog owner
- Investing
- DVD purchasers
- Electronics - home, computing, office, other
- Empty nester
- Expectant parents
- Frequent mail order buyer
- Frequency of purchase indicator
- Getting married
- Getting divorced
- Gun ownership

- Health and beauty
- Health and medical: for example, Allergies, Alzheimer's disease, angina, arthritis/ rheumatism, asthma, back pain, cancer, clinical depression, diabetes, emphysema, erectile dysfunction, epilepsy, frequent heartburn, gum problems, hearing difficulty, high blood pressure, high cholesterol, irritable bowel syndrome, lactose intolerant, ulcer, menopause, migraines/frequent headaches, multiple sclerosis, osteoporosis, Parkinson's disease, prostate problems, psoriasis/eczema, sinusitis/sinuses.
- High-end appliances
- Home improvement
- Household consumer expenditures — many categories.
- Jewelry
- Magazine subscriptions
- Mail order buyer
- Mobile location data (some analytics companies)
- Movies - attendance / collector
- Musical instruments
- Music
- New mover
- New parent
- Online and continuing education
- Online purchasing - many categories
- Parenting
- Pets - other
- Plus size clothing purchase
- Political affiliation
- Recent home buyer
- Recent mortgage borrower
- Retail purchasing - many categories.
- Science-related
- Sexual orientation
- Social media sites likely to be used by an individual or household, heavy or light users
- Spa
- Sports interests: (large category, these are examples)
- Birdwatching
- Equestrian
- Exercise and fitness
- Gardening
- Golf
- Fishing
- Outdoor interests - hiking, camping, climbing
- Swimming, diving, snorkeling
- Spectator Sports
- Stamps/coins

- Yoga
- Television, Cable, Satellite/Dish
- Travel: Vacations, domestic and/or international
- Purchase of international hotel or air flights
- Frequent flyer
- Types of purchases indicator
- Veteran in household
- Vitamins
- Volunteering

Financial and Economic – Property and Assets data:

- Estimated income
- Estimated household income
- Home value
- Length of residence
- Payment data: 30, 60, 90-day mortgage lates
- Purchase date
- Purchase price
- Purchase amount
- Most recent interest rate type
- Most recent loan type code
- Sales transaction code
- Most recent lender code
- Purchase lender code
- Most recent lender name
- Purchase lender name
- Fuel source
- Loan to value
- Purchase interest rate type
- Most recent interest rate
- Purchase interest rate
- Pool or spa
- Home - year built
- Air conditioning
- Boat ownership
- Plane ownership
- Motorcycle ownership
- Commercial assets or business ownership

Financial and Credit data:

- Bankruptcy

- Beacon score
- Credit score - actual
- Certificates of deposit/ money market funds
- Estimated household income ranges
- Income producing assets indicator
- Estimated net worth ranges
- IRAs
- Life insurance
- Low-end credit scores
- Mutual funds/annuities
- Summarized credit score or modeled credit score by neighborhood
- Payday loan purchaser
- Number of credit lines
- Tax liens
- Card data:
- Card holder - single card holder
- Range of new credit
- Debit or credit card present in household
- Card holder - brand (Discover, Visa, Mastercard, etc.)
- Card holder - type (Gas, bank, premium, luxury, prepaid, etc.)
- Frequent credit card user
- New retail card holders
- Underbanked or "thin file"
- Stocks or bonds
- Average online purchase
- Average offline purchase[11]

We reproduce this long (and yet still incomplete) list of data categories to illustrate our point about the range of consumer data bought and sold every day in the commercial marketplace. The WPF scoring report focuses on the use of consumer data for consumer scoring, but lists reflecting each specific category of data are also available for purchase in many other ways. For example, list brokers offer to break down their lists by offering "selections" from the entire list. You can buy a list of individuals by category but limited by age, ethnicity, zip code, medical diagnosis, and many more characteristics.

The result is that any isolated individual characteristic – whether someone has children or credit cards; golfs or fishes; collects stamps or coins; or has a dog – may affect an individual's score. The score may determine whether and how that consumer participates in the economic marketplace for goods and services. Few are likely to think that owing a dog is especially private information. However, that single characteristic may determine whether a particular consumer score is 79 or 80, and that score will determine if the consumer sees an ad offering better job, if

[11] Id. at 33-38.

the consumer can board an airplane without special screening, or whether that consumer's child receives a solicitation to apply to a good college.

Largely unregulated either by the Fair Credit Reporting Act or the Equal Credit Opportunity Act, new consumer scores use thousands of pieces of information about a consumer's past to predict how the consumer will behave in the future. It can also be used to research a large variety of medical issues of interest to medical researchers. Issues of secrecy, fairness of underlying factors, use of consumer information such as race and ethnicity in predictive scores and human research, accuracy, and the uptake in both use and ubiquity of these scores are key areas of focus. Proprietary algorithms make decisions about all of us, and there is no transparency to any consumer scoring activity other than credit scoring. Those engaging the consumer scoring activities collect their data from any available source.

We dare say that most of you responsible for reading these comments are unaware of consumer scoring and the consumer scoring algorithms that result. If you do not know and cannot evaluate these ongoing commercial practices using personal data, how do you think that researchers and IRB members will be able to make decisions about informational risks? How will researchers use these newly available and largely unrestricted data streams? We note that the data streams we refer to are for the most part identifiable and include large amounts of PII.

We do not suggest that the difficulty of the task or the broad commercial and governmental usage of personal information means that any personal information processing necessarily entails more than minimal risk. We do not reject the concept of minimal informational risk. However, we suggest that informational risks are too easy ignored or overlooked, especially by researchers happy to avoid IRBs.

A. Our recommendations to improve the NPRM regarding minimal risk:

We understand that informational risk is a substantial issue that requires a lot of thought. We have researched and thought about this issue for more than a decade. Here are our recommendations for you to consider.

We recommend that:

1. The definition of minimal risk should include the words *informational risk*;
2. The preamble to the final rule should discuss the problem of assessing informational risk in mild detail to provide guidance on the issue; and that
3. The guidance from the Secretary of HHS regarding minimal risk should also discuss informational risk.
4. We also recommend that changes in the consumer data marketplace require updating of minimal risk guidance more frequently than every 8 years. We suggest 3 or 4 years as an alternative, with public consultation an essential element of the Secretary's review.

V. Damaging to financial standing, employability, educational advancement, or reputation (question 11)

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?

Section ____.101

> (b) The following categories of activities are excluded from this policy, and no procedural, recordkeeping, or other requirements of this policy apply to the activities other than the conditions specified for the relevant category or categories:
> (i) Research, not including interventions, that involves the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) uninfluenced by the investigators, if at least one of the following criteria is met:
>
> > (A) The information is recorded by the investigator in such a manner that human subjects cannot be identified, directly or through identifiers linked to the subjects;
> > (B) Any disclosure of the human subjects' responses outside the research 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; or
> > (C) The research will involve a collection of information subject to the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 et seq.; research information will be maintained on information technology that is subject to and in compliance with section 208(b) of the E-Government Act of 2002, 44 U.S.C. 3501note; and all of the information collected, used, or generated as part of the research will be maintained in a system or systems of records subject to the Privacy Act of 1974, 5 U.S.C. 552a.

Our comments focus on (B) with respect to judgments about the effect on disclosure of a data subject's risk of civil or criminal liability or the subject's financial standing, employability, educational advancement, or reputation.

The question we raise is how can a researcher make the necessary judgments about liability and effect on an individual? We recognize that in some cases, the judgments are simple and an exclusion may be readily justified.

We observe that the standard in the NPRM calls for an assessment of the consequences of any *disclosure of the human subjects' responses outside the research*. This may not be the best standard to use. One general goal is to protect research data against other uses. If that goal is

accomplished, then using the consequences of a data breach as a test may be misplaced, although for legally mandated access through subpoenas, warrants, or court orders, the consequences of extra-research disclosures may still be relevant.

In general, we see two types of problems. First, in some cases, issues of civil or criminal liability can be difficult for lawyers to bring forward successfully. The NPRM leaves it to each researcher to make the judgments, whether the judgments entail simple decisions or hard ones. Even identifying potentially relevant legal principles and statutes can be difficult. Applying those principles and statutes can be legitimate subjects for law school exams under the right factual circumstances. For example, a researcher might erroneously conclude that records cannot be subpoenas because of the non-existent "researcher's privilege." How do we know that the researcher made a judgment based on a correct and current view of the law?

We think that the standard for this part of the exemption should be a bit higher and a bit clearer. The exemption should be allowed only if in the researcher's reasonable and documented judgment, the researcher finds no basis to believe that any civil or criminal liability could attach if a human subject's response were shared outside the research. If there is any question whether civil or criminal liability could attach, then the exemption should only be allowed after proper consultation with a lawyer and a review (possibly expedited) of the lawyer's judgment by an IRB. Leaving an interested party (a researcher) to make a complex legal judgment beyond that researcher's expertise is a poor idea. Researchers are no better than the rest of us in finding a justification for a self-serving conclusion.

Second, the standard of *damaging to the subjects' financial standing, employability, educational advancement, or reputation* calls for an incredibly broad and challenging judgment. In the section of our comments where we discuss minimal risk, we detailed how virtually any personal characteristic may be used by consumer scoring algorithms to make determinations about an individual. Will the fact that an adult reads at the 5th grade level damage that individual's reputation or employability? Will a research conclusion that an individual is red-green colorblind, not adept at math, or reads at a fifth grade level affect employability? Will the determination that an individual is left-handed or is on a diet affect that individual's opportunities in the economic marketplace? The consumer scoring report that we cited documents that almost any characteristic can affect a consumer score and how that consumer will be treated by the government or by a commercial company. The Scoring of America report documented this type of data flow indisputably in 2014, and the data usages of this type have grown even stronger since that time.

The judgments here are different than the legal judgments called for by the other part of this standard. The judgment will often require considerable knowledge of how personal information is collected, used, and shared in the commercial and governmental arenas. We suggest that the average researcher, like the average individual, is likely to have little of that knowledge and that the marketplace for commercial exploitation of personal data has expanded greatly since the standard in question was first promulgated years ago.

We do not mean to suggest that nothing can pass the test. Many activities will collect personal information that would have no use outside of the research. In some cases, however, it will be difficult to tell. Given the size and scope of the consumer data marketplace, we think that few people (and even fewer researchers) can make the requirement judgment offhand. We think that a researcher should be obliged to make and document a short but diligent search to determine if there is a commercial use for the personal data collected for the research project. Otherwise, the standard will result in another uneducated, casual, and self-serving judgment that will always come out in the researcher's favor.

The common theme to our two suggestions is *documentation*. The simple way to provide the documentation is by extending the NPRM's proposal for a decision tool for exempt projects to cover excluded projects as well. A researcher should be required to use a decision tool in order to qualify for exclusion of a project from the Common Rule. The tool would allow a researcher to decide in a formal way if a project qualifies for exclusion because risks are low. The tool we envision would differ somewhat from the tool proposed for exempt projects because the standards are different.

We also propose that if a researcher seeking exclusion responsibly uses the results of the exclusion decision tool (revisiting the issue if the research changes over time) and retains the documentation, that researcher should have an appropriate degree of liability protection (a safe harbor) for any excluded activities properly described in the decision tool. Essentially, we propose for excluded projects the same type of safe harbor that the NPRM envisions for exempt projects. Even if the creation of a formal safe harbor is not adopted, the creation of a voluntary decision tool for excluded projects would still be valuable to guide researchers in making legal judgments that they have no specific training to do and for making informational risk judgments that are hard for anyone to do.

HHS should be tasked with publishing an excluded project decision tool after receiving public comment. All of the commercial marketplace information that we included in this section of our comment would be relevant to a project decision tool. For legal issues, updates to a decision tool could be occasional, perhaps only when legislation or court decisions establish new standards. For information activities, the consumer data marketplace and technology change so rapidly that updates to a decision tool might be appropriate every few years, perhaps every two or three years.

VI. Exclusion for Research Subject to the Privacy Act of 1974 (question 14)

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?

§ ____.101(b)(2)

> (C) The research will involve a collection of information subject to the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 et seq.; research information will be maintained on information technology that is subject to and in compliance with section 208(b) of the E-Government Act of 2002, 44 U.S.C. 3501 note; and all of the information collected, used, or generated as part of the research will be maintained in a system or systems of records subject to the Privacy Act of 1974, 5 U.S.C. 552a.

We focus these comments on the exemption for records maintained in a Privacy Act of 1974 system of records. Does the Act provide enough protections for research subjects? The answer is no. The Act's disclosure controls are not appropriate for any research activity.

The Act authorizes disclosures from every system of records to law enforcement agencies at all levels, to the Courts, to the Congress and under other circumstances. 5 U.S.C. § 552a(b). Further, every agency can and has defined routines uses authorizing other disclosures as they see fit, often with little regard for the vague statutory standard. Agencies have widely abused the authority to define routine uses, but this is not the place to argue over that. Many agencies have agency-wide routine uses authorizing broader disclosure to law enforcement than the Act itself allows, disclosures to find parents who owe child support, disclosures to almost anyone in the event of a data breach, and many more. Some agency record systems have dozens of routine uses.

Would any IRB approve a project that proposed to allow disclosure to law enforcement of records that could be used against research participants? The premise of the exclusion of activities subject to the Privacy Act of 1974 is that the Act provides the necessary protections for data subjects. It does not. A general purpose privacy law covering the broad range of federal agency activities has little bearing on research activities for which a much higher degree of confidentiality is appropriate. In implementing the Act, agencies took the easy route of defining more allowable disclosures than are appropriate. Allowing those disclosures for research would make a mockery of research privacy.

We recommend that ____.101(b)(2)(C) be dropped entirely. The Privacy Act of 1974 is not a meaningful research privacy law.

VII. Exclusion for Public Sources (question 16)

16. 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?

Section ____.101

> (b) The following categories of activities are excluded from this policy, and no procedural, recordkeeping, or other requirements of this policy apply to the activities other than the conditions specified for the relevant category or categories:
>
> *****
>
> (ii) Research involving the collection or study of information that has been or will be acquired solely for non-research activities or were acquired for research studies other than the proposed research study, when either of the following two criteria is met:
> (A) These sources are publicly available, or
> (B) The information is recorded by the investigator in such a manner that human subjects cannot be identified, directly or through identifiers linked to the subjects, the investigator does not contact the subjects, and the investigator will not re-identify subjects or otherwise conduct an analysis that could lead to creating identifiable private information.

Our first point has to do with publicly available sources of personal information. We do not know what the term *publicly available* means. Is information posted on a hospital's Facebook page publicly available? Is it not available if you are not a member of Facebook, and someone else has posted it? What if the information is on Facebook but it is "locked down," and only available to friends? Or to friends of friends? What if the information was leaked and posted to a public Internet page? What if the information was the subject of a security breach and is not available to anyone willing to pay ten cents a name for it? What if information is posted on a public Internet site but is also maintained by a federal agency that is not permitted to disclose it by law? What if the information is on a public court docket in Anchorage, Alaska, but you must travel a long distance to Anchorage to see the information? What if the information can be purchased from a commercial data broker? What if the information was publicly available last year but is no longer available today? What if the information is not available in Europe (where the Right to be Forgotten is enshrined in law) but can be retrieved by a search engine in the US?

We submit that the term *publicly available* provides little guidance to researchers. Each researcher will interpret the words differently and in the researcher's own self-interest. The NPRM should either provide clearer guidance or limit the term to public registers or other specifically identified official public sources.

We have a better view of the other provision quoted above. We generally support the notion of allowing an exclusion for data that is not identifiable with suitable protections against re-identification. However we want to complain about this language: "if the investigator will not re-identify subjects." What does "will not" mean? Does it mean that the investigator has no plans to re-identify subjects? Agrees not to re-identify subjects? Will never re-identify subjects

without a court order? Will *never* re-identify subjects under any circumstances? We do not know what it means.

We suggest this language as an alternative: ***and the investigator agrees by virtue of relying on this provision to exclude research from the Common Rule not to re-identify subjects or otherwise conduct an analysis that could lead to creating identifiable private information unless required to do so by court order.*** This language defines a realistic duty for researchers rather than making a vague prediction about what researchers will or will not do.

VIII. Exclusion for HIPAA (question 23)

23. Public comment is sought regarding to what extent the HIPAA Rules and HITECH adequately address the beneficence, autonomy, and justice aspects for the collection of new information (versus information collected or generated in the course of clinical practice, e.g., examination, treatment, and prevention). Should this exclusion be limited to data collected or generated in the course of clinical practice? If additional data collection is allowable, should it be limited to what is on the proposed Secretary's list of minimal risk activities (discussed in more detail below in II.F.2 of this preamble)?

Section ____.101(b)

> (iv) Research as defined by this policy that involves only data collection and analysis involving the recipient's use of identifiable health information when such use is regulated under 45 CFR parts 160 and 164, subparts A and E, for the purposes of "health care operations" or "research" as those terms are defined at 45 CFR 164.501 or for the purpose of "public health activities" as described under 45 CFR 164.512(b).

The rationale for this exclusion is that the HIPAA Privacy Rule already covers these activities. This exclusion suffers from the same problem as the proposed exclusion of research subject to the Privacy Act of 1974. In both cases, the privacy law that supposedly justifies the exclusion has standards that are wholly unsuitable for research. We do not propose to list all of HIPAA's flaws here, but we will point out the worst one. HIPAA allows any covered entity to disclose any or all PHI in its possession to any national security agency (e.g., the CIA, NSA, FBI, and more) without a warrant and <u>without a request</u> from the agency. 45 CFR § 164.512(k)(2).

Is this a privacy rule that should apply to any research activity? It is inconceivable that any IRB would ever agree to allow a research project to make this type of disclosure. Yet if the Common Rule defers to HIPAA, then any research activity by a covered entity covered by the exclusion will be allowed to disclose all research PHI to the CIA for any reason at any time. HIPAA privacy standards are suitable, at best, for records in the health care treatment and payment systems. The privacy standards are not suitable for research activities.

Note that we would not say the same thing with respect to the HIPAA security rule. We find that rule generally meets best practices, and researchers would do well to follow the HIPAA security rule.

We have a small technical concern here as well regarding this language: "Research as defined by this policy that involves only data collection and analysis involving the recipient's use of identifiable health information when such use is regulated under 45 CFR parts 160 and 164…" The words "such use" are not as clear as they might be. The use and disclosure of PHI for research is regulated to some extent under HIPAA because HIPAA regulates covered entities. HIPAA does not regulate third party recipients, including those who obtain PHI under HIPAA's research disclosure provision. If the researcher works in a covered entity and conducts an activity that remains subject to HIPAA, then that researcher is likely subject to the HIPAA privacy and security rules. Not all researcher/recipients are subject to HIPAA. Indeed, most are not. The potential ambiguity here results from the two classes of recipients, one subject to HIPAA and one not.

We think that the language may be clear, but we cannot convince ourselves that there isn't an ambiguity here. The language would be clearer if it said "***when any use or disclosure of PHI by such recipient is regulated…***". Addressing this problem would not resolve our other comment. We would prefer to drop the HIPAA exclusion entirely.

IX. Research Conducted in Established or Commonly Accepted Educational Settings (questions 34-35) (FERPA)

Section ____.104

> (d) The following categories of exempt human subjects research generally involve a low-risk intervention with human subjects, must be recorded as required in paragraph (c) of this section, and do not require application of standards for information and biospecimen protection provided in § ll.105 or informed consent. Only paragraph (d)(2) of this section allows for the collection and use of biospecimens:
> (1) Research conducted in established or commonly accepted educational settings when it specifically involves normal educational practices. This includes most research on regular and special education instructional strategies, and research on the effectiveness of or the comparison among instructional techniques, curricula, or classroom management methods that are not likely to adversely impact students' opportunity to learn required educational content in that educational setting or the assessment of educators who provide instruction.
>
> 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 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?
> 35. Public comment is sought on whether the privacy safeguards of § ll.105 should apply to the research included in § ll.104(d)(1), given that such research may involve risk of disclosure of identifiable private information.

First, we observe with respect to FERPA, as we commented above regarding the Privacy Act of 1974 and HIPAA, that the student privacy law does not include disclosure limitations that would be appropriate for a research project. Relying on FERPA and the Protection of Pupil Rights Amendment as a proxy for privacy protection for research projects is inappropriate. Operational privacy laws that apply to institutions that have broader missions than research are not sufficient to protect the privacy interests of research subjects.

Second, we see no reason why notice of a research project should not include sufficient information about the project to enable a parent to make an informed decision. The notice should:

1. Include the research purpose,
2. Identify all of the researchers by name, title, and qualifications,
3. Describe the privacy protections (including the length of time identifiable records will be maintained, rights of access and correction, any allowable uses and disclosures, and how the parent may pursue a complaint about the research).
4. Notices should be sent by postal mail or by email if a parent agreed in advance to receive email notices from the school.

In a school context, it is especially important to strike a balance that includes robust notice that includes the opportunity for a parent to refuse to allow a child's information to be used in a research project if the research activity uses identifiable records or asks the child to participate in any research-related activities.

Third, we repeat that privacy safeguards under FERPA do not work well for research, and it is essential that the privacy safeguards in section ____.105 apply. Researchers are not likely to provide adequate privacy or security measures unless mandated.

Finally, if information about a student is lost, misused, or leaked, the information could haunt that student for the rest of his or her life. Because the consequences for data misused are greater

for children, it is appropriate to demand stronger protections. We do not express an opinion whether this class of research should be exempt, but if it is exemption is proposed, then the lack of IRB oversight should mean that researcher must comply with appropriate privacy and security standards.

X. **New exemption for public benefit or service program (questions 51 and 52)**

§ ____.104

> (d) The following categories of exempt human subjects research generally involve a low-risk intervention with human subjects, must be recorded as required in paragraph (c) of this section, and do not require application of standards for information and biospecimen protection provided in § ll.105 or informed consent. Only paragraph (d)(2) of this section allows for the collection and use of biospecimens:
> ****
> (2) Research and demonstration projects that are conducted or supported by a Federal department or agency, or otherwise subject to the approval of department or agency heads, and that are designed to study, evaluate, or otherwise examine public benefit or service programs, including procedures for obtaining benefits or services under those programs, possible changes in or alternatives to those programs or procedures, or possible changes in methods or levels of payment for benefits or services under those programs.
>
> 51. Public comment is sought regarding what should constitute notice for purposes of this exemption category. Given the many different types of data that would be covered by this provision (e.g., data from private entities used for social or behavioral science research, government records for which laws already establish standards for notice, and data publicly available for harvesting from the internet), would it be possible to develop a uniform ''notice'' requirement? What type of notice, in terms of its dissemination and scope, should be considered to meet this requirement of the proposed exemption? With regard to the dissemination of the
> notice, should the notice requirement be permitted to be fulfilled through a general public notice, not specifically directed to individuals who are potential research subjects, such as the notice allowable under the Privacy Act? Would a prominent notice posted in all clinics or other relevant public places where information will be collected be acceptable? Should each individual whose data could be used receive their own notice, such as is required of direct treatment providers covered by the HIPAA Privacy Rule? With regard to the content of the notice required by this proposed exemption, what kind of information should be included in the notice, such as the types of research that might be conducted, privacy safeguards, contact information, etc.?
> 52. Public comment is sought on whether, on the other hand, prior notice is necessary.****

Providing notice of privacy rights and use of PII is, admittedly, a difficult challenge across the entire privacy spectrum. Privacy notices are seemingly everywhere, and people rarely read them or understand them. Research by Chris Hoofnagle of Berkeley Law, among other research, shows that people misinterpret the mere presence of a privacy policy, thinking erroneously that a privacy policy means that data is not disclosed. Sadly, that is rarely what a privacy policy says.

There is no simple way to overcome these realities. However, we make two points. First, some people will read notices, and notices may be more likely to receive attention from consumer advocates, reporters, and legislators. Since there will be no IRB oversight, we have to live on the hope of oversight from others. A notice is one important element of any oversight activity, and the notice should be as widely available as possible (e.g., posted publicly on a website).

Second, privacy notices are not just for data subjects. The notices benefit those who process data (no matter what the sphere of activity) in two ways. There is a great benefit in requiring a data controller to develop a notice and decide what the privacy policy is and especially what the limits of use and disclosure are. This is a valuable exercise that often results in better understanding of privacy and of the actual needs of the data controller who writes the notice. In addition, those engaged in the data processing enterprise (again, no matter what the sphere of activity) benefit from a notice because it tells the allowable types of processing. This may be especially important when those using data are from removed from those who wrote the original notice. If a researcher eventually asks "what did we tell individuals we would do with their data?", the notice provides the answer in a consistent way.

How to provide the data subject the notice? This is hard to prescribe. All methods have good and bad features. For a public benefit program, the notice should be provided in the same way that individuals are told about the essential information about the nature of the program and the program's benefits.

XI. Audits (question 33)

§____.104 Exempt research

> (c) Federal departments and agencies shall develop a decision tool to assist in exemption determinations. Unless otherwise required by law, exemption determinations shall be made by an individual who is knowledgeable about the exemption categories and who has access to sufficient information to make an informed and reasonable determination, or by the investigator or another individual at the institution who enters accurate information about the proposed research into the decision tool, which will provide a determination as to whether the study is exempt. If the decision tool is used, further assessment or evaluation of the exemption determination is not required. An institution or, when appropriate, the IRB, must maintain records of exemption determinations made for research subject

> to the requirements of this policy for which the institution or IRB exercises oversight responsibility. These records must include, at a minimum, the name of the research study, the name of the investigator, and the exemption category applied to the research study. Maintenance of the completed decision tool shall be considered to fulfill this recordkeeping requirement.
>
> 33. Public comment is sought regarding the value of adding an auditing requirement.
>
> We support some type of audit requirement. We have made the point several times in these comments that the draft rule puts researchers in a position where they have a conflict of interest. They must evaluate something to determine if what they do is excluded or exempted from the Common Rule. Unless there is some oversight of that determination, we fear that researchers, like other humans, will too often decide that what is in their personal interest is right.

We do not propose that every decision be audited. First, researchers should be required to file with the IRB the completed decision tool. If allowed to keep the tool on their own, we fear that the needed records will too often be "lost." Second, we recommend that IRBs audit a percentage of projects for which the researcher determined that the project is either excluded or exempted. Audit should be relatively simple to complete, and in many universities with appropriate degree programs, the work can be assigned to students. A required audit rate of 5% should be sufficient to put rigor in the system.

We also suggest that any researcher found to have abused the decision tool and improperly exempted or excluded a project should be barred for at least a year from undertaking any other exempt or excluded project.

XII. Sensitive Information

§ ____.105

> e) The following categories of exempt human subjects research allow for the collection of sensitive information about human subjects, must not involve biospecimens, must be recorded as required in paragraph (c) of this section, and require application of standards for information and biospecimen protection provided in § ll.105:

This is one of several places in the NPRM where the proposal relies on the concept of sensitive information. It is a very difficult term because it has no clear or universal definition. Information that is not "sensitive" in one context is "sensitive" in another. For example, a home address may not be sensitive for most people, but it may be for police officers, jurors, victims of domestic violence, and others. Gender is not sensitive information for most individuals, but it may well be highly sensitive for transgendered individuals at various times in their lives. Other fairly routine

information elements may not be sensitive in ordinary activities, but that same information may allow identify thieves to access a bank account or obtain credit in someone else's name. A genetic ailment may be sensitive to one individual while another posts the information on the Internet for all to see. This conversation has been long-discussed within Congress and the Federal Trade Commission in the non-HIPAA-covered health data arena. Almost no progress has been made, and there is a growing understanding that sensitive information is simply not possible to define in a cleanly-cut regulatory framework.

We think that it is hopeless to try to define sensitive information. In fact, many policy discussions around sensitive data have begun to move away from this concept. The work of Dr. Helen Nissenbaum about context and privacy sparked much thought, and has provided a foundation for a shift in thinking about this issue. See for example, *A Contextual Approach to Privacy Online*, http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf.

We are concerned about the reliance here on sensitive data because if researchers and IRB are left to apply the term, the result will be a welter of overlapping and conflicting results. The best approach is to treat **all personal information as worthy of the same level of privacy protection, except where a statute provides otherwise.** We realize that this initially appears to be a more difficult road for researchers; however, after much consideration and more than a decade of conducting research on this issue, we have come to the conclusion that in the end it is actually much cleaner and simpler for covered entities to apply the rule to all data. This policy will become more important over time as data sources increase, along with increase in access to novel data sources by researchers which may contain fields that could be found to have intriguing correlations or causation that ends up being sensitive in one way or another.

XIII. Consent

§___.105

> (c) Limitations on use, release, and disclosure. Unless otherwise required by law, institutions and investigators shall use or release biospecimens or use or disclose identifiable private information collected or maintained for research only:
> (1) For human subjects research regulated by this policy;
> (2) For public health purposes;
> (3) For any lawful purpose with the consent of the subject; or ***

We do not normally object to disclosure of personal information with a data subject's consent. However, the language here is too open ended. Consider the following types of consent:

> • A general consent allowing a marketing company to collect personal information.
> • A consent authorizing a life insurance company to obtain health records about an individual.

• A consent authorizing the federal government to obtain records in connection with an application for a security clearance.
• A consent authorizing a health insurance company to obtain any or all information about an individual's health care, condition, or treatment.
• A consent allowing an employer to obtain health information for use in an employee wellness program.

All of these consents are either so broad or so value that records maintained for a research project could fall within the scope of the consent form. The language in the draft rule – for any purpose with the consent of the subject – is simply too unlimited. Worse, the draft rule obliges ("will use or disclose") a researcher to disclose records without any discretion.

We suggest that a consent from the individual be valid only if it expressly mentions the research project that maintains the records. Otherwise, a researcher would be obliged to honor any general consent and to disclose records to any party. If a safety value is necessary, it is that the researcher can always disclose a record to the data subject, who in then free to use or disclose the record as the data subject sees fit.

For some types of research, researcher object to sharing records with a data subjects, and some laws recognize this objection and allow the withholding of records. Why should the Common Rule have a policy that mandates disclosure of records to anyone with consent? There is a failure here to connect several disparate elements of research record disclosure that needs more attention.

XIV. Privacy and Security

§ ____.105 Protection of biospecimens and identifiable private information.
(a) In General. Institutions and investigators conducting research that is subject to this policy, or that is exempt from this policy under § ll.104(e) or (f), involving the collection, storage, or use of biospecimens or identifiable private information, shall implement and maintain reasonable and appropriate safeguards as specified in paragraph (b) of this section to protect biospecimens or identifiable private information that they collect, obtain, receive, maintain, or transmit for research. The safeguards shall reasonably protect against anticipated threats or hazards to the security or integrity of the information or biospecimens, as well as reasonably protect the information and biospecimens from any intentional or unintentional use, release, or disclosure that is in violation of paragraph (c) of this section. IRB review of the safeguards required by this section is not required, except to the extent required by § ll.104(f)(1).

We strongly support a policy that requires all researchers covered by the Common Rule or exempt from the Common rule to maintain reasonable and appropriate safeguards. We are comfortable allowing the Secretary of HHS to develop the safeguards. Safeguards must address

both privacy and security. Every research project that maintains personal information should have a privacy policy and should be required to follow specific security practices most appropriate for the nature of the project.

XV. IRB Members

> §____.108 (a) In order to fulfill the requirements of this policy each IRB shall:
>
> (2) Prepare and maintain a current list of the IRB members identified by name; earned degrees; representative capacity; indications of experience such as board certifications or licenses sufficient to describe each member's chief anticipated contributions to IRB deliberations; and any employment or other relationship between each member and the institution, for example, full-time employee, part-time employee, member of governing panel or board, stockholder, paid or unpaid consultant;

We support this provision. We recommend that each IRB be required to post the list of IRB members with all of the information described in §____.108(a)(2) on a website accessible to the public.

XVI. Elements of Informed Consent

> §_____.116(a)
> (9) One of the following statements about any research that involves the collection of identifiable private information:

We recommend that the following statement be included as a required element of informed consent:

> The collection, maintenance, and compilation of any personal information about you create a risk to your privacy. As long as the researcher maintains your personal information, the information may be lost or stolen, acquired by the government, or obtained by anyone else using a subpoena or other form of lawful process. The risks here may be small, but the risks are real. These risks remain as long as anyone involved with the research maintains information that identifies you.

XVII. Waiver of Informed Consent

> (f)(1) Waiver or alteration of consent. An IRB may approve a consent procedure that does not include, or that alters, some or all of the elements of informed consent set forth above, or waive the above requirements to obtain informed consent, provided the IRB finds and documents that:

****

(iv) The waiver or alteration will not adversely affect the rights and welfare of the subjects

The required finding here should be that the **collection, maintenance, and use of personal information** will not adversely affect the rights and welfare of the subjects.

XVIII. Conclusion

Thank you for the opportunity to comment on the NPRM. The Common Rule stands as one of the most important outgrowths of what we have heard some researchers call the "Nuremberg Code Era." It is crucial to get it right, and to ensure that updates protect the legacy of the rule's philosophical and ethical foundations. In considering the NPRM as a whole, we have concern about how sensitive information is positioned in the rule, as well as concern about using the Privacy Act and other regulations as potential constraints for human subject research.

The Rule revisions that concern us the most, however, rest in the issue of informational risks. We urge HHS to take another look at this issue with an eye to the recent research that documents how informational risk has substantively changed. We are not in a time any longer where there are simply online and offline risks, or sensitive information risks versus marketing data risks. The lines have blurred and the data has been fused — financial, health, online and offline are merged, and it has gone even further than that. Now we have merging of online, offline, device, location, and biosensor and other kinds of sensor data, all of which provide a rich stream of new data with many uses for human subject research. HHS has the chance to get in front of this issue with this NPRM, we encourage the agency to take this opportunity to do so.

We stand ready to answer any questions, or help in any way.

Respectfully submitted,

Pam Dixon
Executive Director,
World Privacy Forum