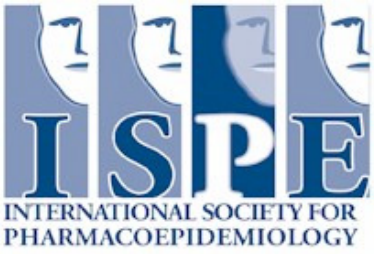

RESPONSE TO

Docket Number: HHS–OPHS–2011–0005

Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators

Submitted by the

International Society for Pharmacoepidemiology

October 20,2011

We applaud the work done by the Office of Science and Technology Policy and DHHS in drafting revisions to the "Common Rule," as research has changed significantly since its last revision in 1991.

Members of ISPE have many years of experience advancing public health by conducting research on the safety and efficacy of medical interventions including drugs, devices, vaccines, and biologics. Much of this research is based on the analysis of health insurer and electronic health record (EHR) data, both of which are collected for non-research purposes. Thus, ISPE is well positioned to point out that there is no alternative to the use of such data, and without access to such data, researchers will be severely limited in their ability to conduct studies designed to safeguard and improve public health.

In pharmacoepidemiology, we often have to evaluate whether specific rare conditions are associated with use of a specific medication. We typically use health insurance claims data or EHR data because, with a rare condition, we need to have information on many thousands of people exposed to the drug in question to achieve valid results. To conduct these types of studies, we apply rigorous methods to determine which individuals were dispensed a specific medication and then evaluate whether they were diagnosed with the rare condition at some time in the future. These studies require knowledge of the timing that the medication was used and when the illness was diagnosed, i.e., we need to have the exact dates for each transaction to ensure that the medication was used before the illness was diagnosed.

With the increasing use of EHRs in the United States that contain the results of laboratory tests, we have the potential to conduct much more complex studies than we are able to do presently using only health insurance claims data. However, the drawback of using EHR data is that it typically represents care that was provided by just one of the individual's health care providers, not from all of the clinicians the individual sees. To evaluate the entirety of individual's medical history—all diseases and medications—we will have to link the individual's medical data from the provider's EHR with the individual's health insurance. To perform the correct linkage between EHR data and health insurance data, individual identifiers such as name, birth date, and address are needed. According to Table 1 of the ANPRM, identifiable information that will be used for future research will require consent at that time that the initial data is obtained. If consent were required for such studies, it is certain that this would 1) reduce the available sample size in settings where sample sizes are already barely sufficient to detect a relation between the medication and rare disease with needed precision and 2) bias the population under study. One can envision certain subpopulations that will be more likely or less likely to refuse consent, such as the elderly or severely ill, thus potentially introducing bias and resulting in incorrect study findings. We discuss these issues in more detail below.

General comments:

As a professional society, ISPE is most concerned about the proposed requirement for written informed consent for data that is collected for non-research purposes, but may also be used for future research. Under the proposed rule, consent would have to take place at the time and point of data collection, i.e., in the

clinical setting. This is a concern because written consent obtained at the time and point of care could only be very general because of the unknown specifics of future research, and as such, consent cannot be informed. We believe that such a requirement for written consent of future use of secondary data is not practical or possible, and will essentially halt all health care research using large datasets of health insurer claims and electronic health records.

The ANPRM also suggests an opt-in or opt-out process for future use of data collected for non-research purposes. Not only is an opt-in or opt–out process difficult to implement, but the resulting data will be incomplete and potentially biased. The incompleteness and/or bias that occurs because individuals choose not to allow their data to be used for research will have serious implications for study validity and generalizability. Individuals would be making decisions to opt-in or opt-out without the information needed to make informed decisions about possible future uses of the data. The research questions, which arise in the future, and for which that particular dataset might provide some of the answers, cannot be known at the time of initial data collection. Thus, the participating individuals would be forced to make the opt-in or opt-out decision based on little or no information about future research use of the dataset.

The ANPRM is considering mandatory standards of data security for *all* data collection, storage, and usage, with the level of security calibrated to the level of identifiability of the information, with identifiability based on the HIPAA Privacy Rule. The HIPAA Privacy Rule has a strict standard for complete de-identification, requiring either the removal of 18 specified identifiers or certification by a statistical expert that the risk of identification is very small. We believe that patient data can be equally protected by the Common Rule, which evaluates identifiability according to whether the subject's identity is "readily ascertainable" by investigators conducting research. Applying the less flexible HIPAA Privacy Rule to all research activities will cause significant research and IRB burdens, with little advantage over the Common Rule in protecting patient privacy.

Likewise, strong data security practices are preferred to requiring adherence to the HIPAA Security Rule for all research. With passage of the 2009 HITECH Act, privacy and security protections under HIPAA were broadened in scope to provide stronger patient data safeguards to now encompass not only covered entities, but all business associates of covered entities. Because HIPAA breach notification standards, i.e., when there is a release of protected health information, incur significant penalties and notification practices, the costs and technological requirements for putting HIPAA security standards in place is unreasonable and too costly if applied to all types of research. Thus, the HIPAA Security Rule intended for protected health information (PHI) in the clinical care situation should not apply to research where the informational risks can be mitigated by other means.

For health care research that relies on PHI, HIPAA has not had a beneficial effect on privacy protections.[1,] Evidence suggests that HIPAA has hampered research, primarily because of its impact on recruitment

[1] (http://www.iom.edu/Reports/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research.aspx).

practices for clinical trials[2] and penalties for privacy breaches that have negatively impacted data access and data sharing. Because HIPAA has not had a beneficial effect for protecting privacy in health research but has actually been detrimental, we believe that all research using data arising from health care encounters should be exempted from HIPAA requirements.

Although the ISPE supports the prohibition of re-identification of de-identified data, we note that there may be certain public health activities in which the benefit of re-identification outweighs its risks, for example if severe poisonings or deaths occur that might be attributable to a suspected drug tampering or manufacturing problem. The ANPRM should include the flexibility of re-identification in specific, compelling situations with proper IRB oversight.

Response to specific questions

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

As discussed above, ISPE contends that it should be permissible to waive consent for all research involving the study of existing, de-identified data, and that this poses minimal risk. Not doing so will impede public health research, especially research assessing the safety and effectiveness of medications used in populations.

We also point out that there are sufficient differences between existing data and biospecimens that these two should not be combined in future rulemaking.

[2] Wilson JF. Health Insurance Portability and Accountability Act Privacy Rule causes ongoing concerns among clinicians and researchers. Ann Intern Med 2006; 145: 313-316.

Question 45: Under what circumstances should future research use of data initially collected for non-research purposes require informed consent? Should consent requirements vary based on the likelihood of identifying a research subject? Are there other circumstances in which it should not be necessary to obtain additional consent for the research use of currently available data that were collected for a purpose other than the currently proposed research?

Question 46: Under what circumstances should unanticipated future analysis of data that were collected for a different research purpose be permitted without consent? Should consent requirements vary based on the likelihood of identifying a research subject?

The ISPE membership is concerned that there be any requirement for informed consent for future use of data initially collected for non-research purposes. We do not believe it is possible to obtain INFORMED consent for future use of data.

As discussed above, the only way to obtain informed consent for use of health data from clinical settings is to have individuals provide consent at the time of their clinical encounter, which would be time-consuming, add to medical care costs, and would be uninformed because the potential uses of the data will not be known at the time of signing.

Question 53: In cases in which consent for future research use is not obtained at the time of collection, should there be a presumption that obtaining consent for the secondary analysis of existing biospecimens or identifiable data would be deemed impracticable, such that consent could be waived, when more than a specified threshold number of individuals are involved? (SACHRP provided the Secretary with recommendations on this issue.\81\) If so, what threshold number should constitute impracticability? Is the number of potential human subjects the only measure of impracticability?

Although the ISPE membership believes that consent should be waived presumptively for secondary research of de-identified data, the threshold that one might set for waiver of informed consent (for practicability reasons) would be completely arbitrary. As such, we do not believe it is practical or appropriate to have threshold standards based on the number of patients.

Question 59: Would study subjects be sufficiently protected from informational risks if investigators are required to adhere to a strict set of data security and information protection standards modeled on the HIPAA Rules? Are such standards appropriate not just for studies involving health information, but for all types of studies, including social and behavioral research? Or might a better system employ different standards for different types of research?

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

The ISPE membership believes that data security is critical and necessary to protect the privacy of study subjects in all types of studies. However, we believe that application of HIPAA standards, with its 18-point strict de-identification standards, is not cost-effective in protecting the privacy of study subjects while permitting needed research to be conducted. As we have described above, the Common Rule can be used as a basis for protecting data, and would welcome additional data protection standards, such as data encryption, that might be suggested by the Office of Human Research Protection. This is preferred, given the complexities, costs, and negative effects on research that would occur if HIPAA security protections were the standard for research uses of all data.