

Issues Raised by ANPRM Regarding Secondary Uses of EHR Data
for Research Purposes

Introduction/Framing

- The ANPRM focuses on potential changes to the Common Rule, which governs most federally funded health care *research*. Although HHS expresses a desire to harmonize the research provisions in both the Common Rule and HIPAA (and the ANPRM proposes to adopt some of HIPAA's standards), the ANPRM does not propose any changes to provisions of HIPAA.
- The issues raised by human subjects research are very complex, and in the short time period available to submit recommendations that could be helpful to HHS in resolving some of the issues raised in the ANPRM, there is not sufficient time for the Policy Committee to get up to speed on, and thoughtfully weigh in on, all of the issues.
- However, the Policy Committee has issued recommendations regarding privacy and security protections for information in EHRs that could be helpful to HHS in resolving some of the issues raised by the ANPRM. Consequently, we are limiting our focus to the policies surrounding the use of data in EHRs initially collected for treatment purposes and also used secondarily for evaluations, assessments, and reports. The lack of comment on some aspects of the secondary use of data for research, such as the elements of informed consent and the circumstances justifying waiver of consent, should not be interpreted as support or disagreement with the ideas in the ANPRM.
- In seeking to weigh in on the issues raised in the ANPRM, we seek to build on the following previous recommendations of the Tiger Team (taken verbatim from the letter approved by the Policy Committee in August 2010):

Core Values

- The relationship between the patient and his/her health care provider is the foundation for trust in health information exchange; thus providers are responsible for maintaining the privacy and security of their patients' records.
- Patients should not be surprised about or harmed by collections, uses or disclosures of their information.

Recommendations on Fair Information Practices and on Consent:

- All entities involved in health information exchange should follow the full complement of fair information practices when handling personally identifiable health information.
- When the decision to disclose or exchange a patient's identifiable health information is not in control of the provider (or the provider's organized health care arrangement (OHCA)), patients should be able to exercise meaningful consent to their participation.

Draft Straw Recommendations

I. Question 1 – For provider entities¹ using EHR systems, what uses of data constitute “research” and therefore should be subject to regulation under the Common Rule

Background/Framing

- The Common Rule currently exempts research using existing EHR data from requirements for IRB review if the data does not identify individual subjects. The ANPRM proposes to retain this exemption from IRB review² – but to require prior consent for any research using identifiable data (research done with a limited data set or with HIPAA de-identified data would not require consent).
- Technology enhances the ability to conduct assessments of health care quality, safety and effectiveness; technology also enhances the ability of providers to effectively treat patients and improve population health.
- One of the goals of HITECH is the creation of a learning health care system. Consequently, providers and health care organizations should be expected to use data in EHRs to optimally treat patients and evaluate the quality and effectiveness, including the comparative effectiveness, of the care they provide -- and to share the results.

¹ We recognize that the scope of entities involved in federally funded research is quite broad and includes entities not directly impacted (or covered by) ONC or HITECH programs (for example, health plans, pharmaceutical manufacturers, research institutions, etc.). Based on our experience and expertise, we are confining this recommendation to provider entities; however, HHS should consider applying it to others involved in the research enterprise where it would be appropriate to do so.

² Instead, HHS is proposing to require researchers to file a brief one-page summary of the research with the IRB or research office.

- Although the ANPRM intends to provide greater flexibility for research activities, more clarity regarding which data activities constitute “research” could help remove real or perceived obstacles to important endeavors. Current rules (both the Common Rule and HIPAA) define “research” as activities designed to develop or contribute to “generalizable knowledge.” Since the creation of a learning healthcare system will depend on more widespread dissemination of the results (in a way that safeguards individual privacy) of treatment interventions and evaluations of the health care system, characterizing research as any evaluative activity that contributes to the “generalizable knowledge” may no longer serve the interests of either patients or providers.
- The use of EHR systems creates new technological opportunities to improve treatment of patients and to evaluate the quality, safety and effectiveness of that care. We are concerned that the potential treatment of such activities as “research” could limit these activities.

Draft Recommendations:

1. The use of a provider entities’ EHR data for treatment purposes or to evaluate the safety, quality and effectiveness of prevention and treatment activities should not require consent or IRB approval or registration. Such activities should not be considered “research” but instead should qualify as treatment and operations if conducted by, or on behalf of (such as by a business associate), a provider entity.
 - a. This exemption should apply even if the results are intended to, or end up being, publicized or more widely shared (i.e., contribute to generalizable knowledge).
 - b. Consent should not be required to access EHR data for these purposes, even if the data does not qualify as either a limited data set or de-identified data; however, provider entities should always use the minimum necessary amount of data to accomplish these activities (including removing patient identifiers when it is not necessary to identify individual patients).
 - c. Examples of activities the Tiger Team agrees should be covered by this recommendation (not intended to be an exclusive list):
 - i. The use of EHR data to improve care provided to patients (such as by evaluating the effectiveness of care).
 - ii. Early detection of patient safety issues through identification of patterns of adverse events.
 - iii. Evaluation of interventions designed to improve compliance with existing standards of care and outcomes

- (e.g. interventions that reduce the rate of hospital-acquired infections)
- iv. Monitoring individual clinicians and professional staff for adherence to existing standards of care and existing treatment protocols; data comparisons of outcomes.
 - v. Outreach efforts intended to increase patient compliance with existing standards (e.g. vaccinations, cancer screening tests).

We have attached some comments we received from care providers that offer examples of activities they believe should be considered to be treatment and operations and not “research.”

2. Consistent with the Tiger Team’s previous recommendations, the above exemption should apply only when the provider entity (or OHCA) retains oversight and control over decisions regarding when their identifiable EHR data is used for quality, safety and effectiveness evaluations.
 - a. This recommendation is based on previous Tiger Team/Policy Committee recommendations that recognize that patients place their trust in their health care providers with respect to stewardship of their health information. Consequently, when the provider entity (or the OHCA) that the patient trusts no longer has control over decisions regarding access to patient identifiable data, the patient should have meaningful choices regarding whether or not his or her identifiable information is part of such an arrangement.
 - b. This exemption should be interpreted to allow provider entities (or OHCAs) to collaborate and share identifiable information for treatment purposes or to conduct quality, safety and effectiveness assessments, as long as the entities remain in control over decisions regarding how their EHR identifiable data is to be accessed, used and disclosed.
 - c. Entities should follow the full complement of fair information practices in using identifiable data for these purposes, including (but not limited to) being transparent with patients about how their data is used for treatment and quality, safety and effectiveness evaluation purposes, using only the minimum amount of data needed to accomplish the particular activity, and protecting the data with security measures that are commensurate with the risks to privacy).

Question II – Application of fair information practices

Background

- The focus of the ANPRM is primarily on when consent should apply to the secondary use of EHR data for research purposes.

- However, consent is but one element of fair information practices, the framework that typically is applied to uses of potentially sensitive information.
- Overreliance on consent can inappropriately shift the burden for protecting privacy onto patients.
- ONC has adopted an articulation of fair information for its programs (the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information).
- Although ONC doesn't regulate research per se; however, to the extent that ONC programs are providing incentives for the adoption of EHRs, which will provide a rich source of data for potential research), it makes sense for the Tiger Team/Policy Committee to provide its perspective on "private and secure" uses of this data, including for research.
- Probably, most patients won't understand the difference between a "covered entity" and a "research entity", but will expect the same privacy and security standards applied to their data.

Draft Recommendations:

3. Research entities should also be required to adopt policies and/or best practices that follow the full complement of fair information practices, regardless of whether or not a patient's consent is required to be obtained.
 - For example, researchers should limit the amount of information collected to what is necessary to perform the research, limit the number of people who have access to the data for research purposes to those performing the research, and adopt and adhere to specific retention policies with respect to the data (and return or destroy the data upon the expiration of the retention period).
 - As another example, researchers should be required to adopt basic security protections consistent with the privacy risks associated with inappropriate exposure of the data. We applaud the ANPRM for recommendation that researchers be required to adopt basic security protections.