August 4, 2015

The White House
Attn: Stephanie Devaney
Project Manager of the Precision Medicine Initiative,
White House Office of Chief of Staff
1600 Pennsylvania Avenue Northwest
Washington, DC 20500

Re: Precision Medicine Initiative:
Proposed Privacy and Trust Principles

Dear Ms. Devaney:

The Health Law Section of the American Bar Association (the “Section”) respectfully submits the following comments on the Proposed Privacy and Trust Principles (“Proposed Principles”) issued by the Precision Medicine Initiative interagency working group, including the White House Office of Science and Technology Policy, the Department of Health and Human Services Office for Civil Rights, and the National Institutes of Health (the “Interagency Working Group”).

The views expressed herein are presented on behalf of the Section.1 No government attorneys or government professionals participated in the drafting or submission of these comments. These comments have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the American Bar Association. The views expressed in these comments should not be

1 The comments were initially prepared by a working group of the eHealth, Privacy and Security Interest Group of the Health Law Section (the “ABA Working Group”). Contributors to these comments from the Working Group were John R. Christiansen, George J. Annas, H.P. Bose, Hillary Noll Kalay, Melissa L. Markey, Suchisimita Pahi, Dennis M. Peffley, Nancy L. Perkins, Sheila Sokolowski, Mark Thush and Christine Burke Worthen. In addition, ABA Health Law Section members Robyn Shapiro and Tom Dowdell served as reviewers of the Working Group’s work and participated in the preparation of the final comments. The final comments were approved by the Section’s Council on August 4, 2015. Although members of the Section who participated in the preparation and review of these comments have clients that may be affected by the Proposed Principles and the Precision Medicine Initiative, if and when final Privacy and Trust Principles relating thereto are adopted, no such member has been engaged by a client to participate in the drafting or submission of these comments.
construed as representing the policy or views of any government employee who is a member of the Section, its Council, or the ABA Working Group.

I.      Background on the American Bar Association Health Law Section

The American Bar Association is the largest voluntary professional association in the world. The Section, with nearly 9,000 attorney members, is the voice of the organized healthcare bar within the ABA. Its members represent clients in all aspects of the healthcare industry, including physicians, institutional providers, teaching and research organizations, managed care organizations and other third-party payors, governmental healthcare programs and regulatory bodies, pharmaceutical companies and device manufacturers. Accordingly, the Section believes that it brings a broad and unique perspective to the challenges associated with health information privacy, security, sharing and use, and research administration issues.

II.      Comments on the Proposed Principles

The Precision Medicine Initiative (“PMI”) is an ambitious, nationwide research program that will include one million or more volunteers (“Participants”) in its research population (“PMI Cohort”). According to the White House Fact Sheet: President Obama’s Precision Medicine Initiative (“PMI Fact Sheet”), the principal goal of the PMI is to “pioneer a new model of patient-powered research that promises to accelerate biomedical discoveries and provide clinicians with new tools, knowledge, and therapies to select which treatments will work best for which patients.”

One of the fundamental assumptions of the Proposed Principles is that Participants will “voluntarily contribute diverse sources of data – including medical records, genomic data, lifestyle information, environmental data, and personal device and sensor data [‘Participant Data’].” Other sources of Participant Data may be added over time.

It does not appear that the type of information architecture to be used to receive, maintain, process and share Participant Data and research results has been defined. The Data Sharing, Access and Use principle provides for

Multiple tiers of data access—from open to controlled—based on data type, data use, and user qualifications . . . to ensure that a broad range of interested communities can utilize [PMI Cohort] data while ensuring that privacy is safeguarded and public trust is maintained.

There is no additional discussion of the types of community which might have access to data. One of the assumptions of the Proposed Principles is that Participants will be provided with access to “their own medical information,” including research data. Otherwise, while there are references to “other data users” (or “other authorized data users”) the only type of data user identified is researchers, which are included by implication. There is also no description of the types of data which may be made available (for convenience, “PMI Data” in these comments).
According to the PMI Fact Sheet the PMI “will leverage existing research and clinical networks[.].” Likewise, the White House anticipates that the PMI “will call on academic medical centers, researchers, foundations, privacy experts, medical ethicists, and medical product innovators to lay the foundation for this effort[.]”

A. Definitions

One issue in the interpretation of the Proposed Principles is the lack of clarity in some key terms. It is understandable that a novel project like the PMI would use terms in novel ways, or even require some new terminology. At the same time, the inclusion of definitions of some key terms would be helpful in interpreting the final Principles.

In particular, we recommend definitions for the following terms:

- **PMI Cohort.** The Proposed Principles use the term “PMI cohort” both as if it refers to the population of Participants, which is consistent with the typical usage of the term “cohort,”[2] and as if it refers to the governing body of the PMI.[3] We recommend that “PMI Cohort” be defined in terms of the population of Participants, as we do in these comments, and a separate definition or definitions be provided for the PMI governing body.

- **Participant Data.** This would be a useful term to refer to the personal data contributed by or on behalf of a Participant, to distinguish it from other types of information subject to governance under the PMI. This term is used for convenience in these comments.

- **PMI Data.** This would be a useful term to refer to data which is made available by PMI policy, to researchers and other authorized data users. As contemplated by the Proposed Principles, there are likely to be multiple types of PMI Data, available for different purposes to different types of users. This term is used for convenience in these comments.

Other defined terms would also be useful for interpretation purposes, including terms defining different types of authorized use (e.g. “Research,” “Health Care,” “Participant Request,” etc.), authorized user types (e.g. “Researcher” and “Clinical Care Provider”),

---

[2] See, e.g., “Respecting Participant Preferences” sub-principle 1: “In order for the PMI cohort to be broadly inclusive . . . .” Cf. the Agency for Healthcare Research and Quality definition of “Cohort Study:”

Definition: A clinical research study in which people who presently have a certain condition or receive a particular treatment are followed over time and compared with another group of people who are not affected by the condition.

Example: For example, the Women’s Health Initiative is a cohort study that collects information from a group of older women who are followed over several years.

different types of participating organizations (e.g. “Research Site,” “Health Care Facility,” and perhaps such categories as “Data Services Provider”), and so on. Use of defined terms would also simplify and help ensure consistency in the development of policies, guidelines and agreement documentation.

B. Governance

No specific governance infrastructure is described in the Proposed Principles, but an infrastructure involving both a central authority and participation by and representation of key stakeholder groups is articulated. This infrastructure would provide for compliance with applicable laws and PMI requirements by researchers and other data users, Participant communications management, and analysis of potential research-related risks to individuals, families and communities.

1. Policy Development and Implementation

The proposed Governance principle contemplates a policy development and implementation process, but does not articulate mechanisms. One model which might be considered is the Data Use and Reciprocal Support Agreement (“DURSA”) developed for purposes of the Nationwide Health Information Network (“NHIN”) initiative, a model which is still used in many health information exchange arrangements.

The DURSA model involves a multi-party agreement under which each participating party enters into the DURSA, establishing various obligations intended to enable that party to exchange health information with other participating parties in a trustworthy fashion. One of the DURSA obligations is compliance with the policies and decisions of the “Coordinating Committee,” made up of key Federal agency and stakeholder representatives. The DURSA also contemplates establishment of at least one advisory “Technical Committee.”

The DURSA is not a perfect model, and it is by no means recommended that it be adopted without substantial analysis and adaptation to PMI needs and goals. Nonetheless, it is a model of a policy-driven governance structure based on voluntary stakeholder agreement which is worth considering for PMI governance.

Under such a model, policies and procedures would be developed principally by committees or working groups targeting various project issues and needs. This effort might usefully be started by forming groups assigned to the different Principles, as long as it is recognized that there will be overlap and substantial interplay between the assignment areas, and there are mechanisms to ensure coordination, information sharing and the avoidance of “siloes.”

Policy development committees or groups should include stakeholders affected by the issues, as well as relevant subject matter experts. Policies would be subject to review and approval by the central governing body, preferably subject to a stakeholder comment period. Approved policies would be binding upon stakeholders, as part of their contractual obligations. It would also be highly appropriate to provide guidance and perhaps education to stakeholders and users to ensure their understanding of policies and obligations.
2. **Establishment of Governance-Level Security Program**

The Proposed Principles recognize the importance of security. However, we recommend that security be expressly incorporated into Governance to ensure that security issues are given the executive-level support necessary to ensure compliance with security obligations, and that adequate funding is provided for security implementation.

In particular, in order to implement an effective security program there should be a standing committee, working group or team that reports to, and is perhaps represented on, the central governing body. Executive understanding of security needs and commitment to adequate security is well-known to be essential to effective security.4

This is particularly important for a project like this, which is likely to have a relatively high public profile and will be collecting and generating sensitive personal information as well as commercially valuable new data. Some of this information, as the Proposed Principles recognize, might also be used maliciously, to attempt to stigmatize individuals or communities. This means that PMI information and systems must be considered, in security terms, a highly valuable asset which is by the same token likely to be seen as a valuable target for malicious or profit-seeking persons.

The recent and unfortunately continuing spate of large and small information system breaches makes it clear that information assets like this are under constant threat from malicious or profit-oriented persons, ranging from “lone wolves” to criminal enterprises, various types of activist groups and state-based “cyberwarriors.” At the same time, constantly changing technologies lead to constantly emerging vulnerabilities as well as opportunities for new security strategies.

A dedicated security team, including both representation of key stakeholder categories and highly experienced subject matter experts, will be essential to identifying, helping develop and maintaining appropriate safeguards. This team would provide oversight for the administration of information systems directly involved in hosting PMI Cohort and other PMI data and guidance to participating organizations and users, and provide leadership for security breach response.5

The National Institute of Standards and Technologies (“NIST”) maintains important expertise and a library of valuable publications in this area. However, we recommend against reliance upon NIST resources alone, as many private sector stakeholders have additional expertise, including expertise in non-governmental environments, that would provide a

---

4 See generally John R. Christiansen, An Integrated Standard of Care for Healthcare Information Security: Risk Management, HIPAA and Beyond (2005), and authorities cited therein.

5 The specific strategies required for security program management will necessarily vary depending on the architecture implemented for the PMI. A centralized architecture would call for direct oversight on behalf of the PMI governing body, while a distributed architecture in which different organizations hosted PMI systems would call for delegated security responsibilities under centrally developed policy requirements, for example.
valuable supplement and help ensure that security policies are developed which are not inconsistent with the needs and administration of private sector participating organizations.

A model of committee of this type might be the Privacy and Security Tiger Team from the Health Information Technology Policy Workgroups.\(^6\) It consisted of industry and Federal government officials with solicited input at monthly meetings from the public, and generated some valuable reports and commentary on a range of privacy and security issues.

3. **Clarification of Healthcare Provider Participation**

It would be helpful to clarify possible terms of participation by healthcare providers (academic medical centers and other hospitals and health systems, physician practices, etc.) as users of PMI Data for clinical care purposes, as opposed to from their participation as researchers or research sponsors.

The Proposed Principles do not exclude this type of participation. However, the only roles the Proposed Principles reference for healthcare providers are as (a) a source of data (e.g., medical records) contributed by the Participant, or (b) a user of PMI Data as a researcher (or perhaps by implication research sponsor or site). It is therefore not clear whether “authorized users” of PMI Data would include healthcare providers using the data in order to provide care to Participants.\(^7\)

The goal of precision medicine is to identify and implement individualized disease prevention and treatment strategies. A healthcare provider therefore might appropriately receive and use PMI Data to help diagnose and provide treatment to a Participant. While it is not clear, the use of PMI Data to support healthcare decisions seems necessary to support research on differing outcomes for healthcare enabled by PMI Data and comparison to control groups whose care was not so enabled.

If healthcare uses of PMI Data were permitted as authorized uses, it must be noted that a healthcare provider which used PMI Data for clinical care purposes (for example, genomic information used to help select appropriate cancer treatment) would be legally required to include such information in the Participant’s medical records. The healthcare provider might also have legal or ethical obligations to re-disclose such information as part of its clinical records, to other healthcare providers of the Participant or to oversight agencies, and so on. Data access policies and data use agreements appropriate for research purposes may not accommodate such obligations.

We therefore recommend clarification whether PMI Data will be authorized for use to support healthcare decisions. If so, policies and data use agreements appropriate for healthcare provider access and use of PMI Data for healthcare purposes should therefore be

---


\(^7\) It is also not clear whether healthcare providers would have access to Participant Data in order to provide Participant healthcare. This seems less likely to be desirable, as healthcare providers should generally have access to medical records and related types of Participant Data through customary channels and processes.
developed. In order to appropriately represent this interest, appropriate representation of this clinical care interest should be included in PMI governance decision-making.

4. Specific Additional Recommendations for Governance

a. The following recommendations apply to the first Governance sub-principle, calling for a partnership model of governance which is dynamic and transparent:

- To facilitate flexibility and a highly dynamic nature, consider temporary special committees and working groups that develop and propose policies and best practices, and produce guidance on current scientific, technological and ethics-related developments.\(^8\)
- Specifically include universities conducting research, as their experience is different from industrial/corporate research.
- Delegate development responsibilities as needed to private sector while maintaining public comment and transparency, taking advantage of developed expertise.
- Consider the potential use of a Steering Group Committee subject to the Federal Advisory Committee Act (“FACA”), to support transparency and flexible governance with multi-sector input.\(^9\)

b. The following recommendation applies to the third Governance sub-principle, with respect to legal compliance:

- Use existing baseline laws for collection, transfer and authorization of research data as already provided through HIPAA and Nationwide Health Information Network. Note that the HIPAA Security Rule is scalable and flexible per entity. Ideally, governance will involve extending the baseline to include model or best practices for PMI Cohort data.

c. The following recommendations apply to the fourth Governance sub-principle, calling for mechanisms to ensure accountability, and responsible data management and protect against unauthorized or inappropriate access, use, disclosure or re-identification of PMI Cohort data:

---

\(^8\) See PATIENT-CENTERED OUTCOMES RESEARCH INSTITUTE, STANDARDS IN THE USE OF COLLABORATIVE OR DISTRIBUTED DATA NETWORKS IN PATIENT CENTERED OUTCOMES RESEARCH (2012) at 188, Table 8b (Summary of Guidelines/Practices Followed by Selected Networks: Governance Guidelines) row 4e, for examples of Committees and Workgroups used by various Research Networks in managing data and governance in research.

\(^9\) FACA requires committee memberships to be “fairly balanced in points of view represented and functions to be performed.” Proportional representation from privacy and security advocacy groups, industry, Federal Government and non-profit research initiatives would be sample (as well as other stakeholders); meetings open to the public with public notice given at least 15 days prior to the meeting. See FACA Final Rule 2001, available at http://www.gsa.gov/portal/content/104034. The FACA was applied to the Privacy and Security Tiger Team.
Consider establishing a dedicated committee or set of committees for ensuring data privacy and researcher/data-user education with participation from Participants, researchers, Healthcare Providers and other stakeholders.

To further this goal, actively recruit individual members or industries with specialization in data management and access (technical and legal) as well as researchers and data-users currently in the research field.

Consider appropriate remedies for unauthorized use or disclosure of data. This could include suspension or exclusion from PMI access. Whether or not financial penalties in addition to any penalties available under applicable federal or state law would make sense should be considered, in light of existing penalties which would apply. Any penalties should be proportionate to the violator’s intent and potential harm caused by the violation.

C. Transparency

1. Informed Consent/Authorization

The first Transparency sub-principle identifies certain information that should be provided to Participants, but does not expressly require that the PMI obtain the Participants’ informed consent or authorization to use and share the Participant’s data. We recommend that an informed consent or authorization strategy be considered for adoption in the final Principles.

This is consistent with existing Organization for Economic Cooperation and Development (“OECD”) guidelines, which recommend that genetic research databases obtain “prior, free and informed consent” from each participant.\(^\text{10}\) The PMI Cohort will include genomic data and other data that enjoys a higher level of protection under federal and state laws. Therefore, while it appears such a requirement may be implied in the Proposed Principles, we recommend that consideration be given to explicitly requiring informed consent consistent with OECD guidelines, both initially and periodically thereafter in order to ensure the validity of each Participant’s informed consent. Consideration should be given to whether an informed consent form appropriate for initial enrollment and periodic confirmation is adequate for purposes of specific projects or data uses, and the extent to which project- or use-specific informed consent documentation should be required.

We also recommend that careful consideration be given to whether and to what extent Participants will include minors and adults not legally capable of giving consent. Obtaining consent to use and share information about such individuals for research is partially a matter

of state law, as state laws determine the age of majority and legal capacity, and when and under what circumstances such individuals may consent to their own medical treatment. Because HIPAA defers to state law, whether such an individual or his or her parent (if a minor), legal guardian or other personal representative has the right to consent to the individual’s participation in the cohort will vary depending on the state and whether the individual or his or her legal representative consented to the treatment that is the subject of the information. Development of a consent process and documentation which satisfies state law requirements would be a necessary step if the PMI Cohort is to include minors.

Finally, we recommend considering that the informed consent process include notification to Participants consistent with OECD guidelines, including in particular: (1) a disclosure that the information may be used for commercial purposes and the policy for commercialization; (2) PMI policies for sharing data for non-research purposes, e.g., insurers, employers, law enforcement and for public health emergencies; (3) PMI policies for providing feedback of research results and incidental findings to Participants; (4) PMI policies for communications and contact with the Participant; and (5) the PMI Cohort and other data retention periods.11

2. Breach Notification

The third Transparency principle addresses breaches of Participants’ personal information. We recommend that policies and procedures be adopted for security incident and breach response which are consistent with and at least as protective of individual rights and interests as the HIPAA Breach Notification Rule.12

The PMI is not subject to the HIPAA rules because it is neither a Covered Entity nor Business Associate under HIPAA. Nevertheless, Participants are likely to interact with the PMI in a healthcare-related setting, perhaps in many cases exclusively in consultation with their healthcare provider. Likewise, Participant Data will largely consist of information that is equivalent to “Protected Health Information”, as defined in the HIPAA rules. Participants are therefore likely to expect breach notification consistent with Breach Notification Rule.

Further, we note that breaches may be experienced not only with respect to data in systems under direct PMI governance, but also in participating organizations’ systems subject to delegated security obligations.13 Many of these organizations will be HIPAA Covered Entities or Business Associates, which will be required to respond to breaches of Participant Data in their systems as required by the Breach Notification Rule.


12 See 45 CFR Part 164, subpart D.

13 Specific details will depend on the specific architecture adopted by the PMI. See footnote 5.
We therefore recommend that breach notification standards for Participant Data be harmonized with the Breach Notification rule.14

3. Publication and Posting of Research Findings

The fourth Transparency principle sets forth an expectation for data users to publish or post publicly summaries of research findings. We agree with this expectation, but we also think it raises practical questions about the timeliness of the publication or posting, and whether data users should be permitted to delay publication or posting to protect their own proprietary interests or to protect Participants. The PMI governing body should adopt policies in this area to provide clear guidance.

Additionally, OECD guidelines recommend that genetic research databases provide participants with information about commercial products that may arise from the research conducted using the information provided by participants.15 Again, as the PMI Cohort will include genomic data and other data that enjoy a higher level of protection under federal and state laws, and because data users will include for-profit entities, we recommend that the PMI adopt policies which require data users to disclose information about commercial products that may arise from the research.

D. Respecting Participant Preferences

1. Third Sub-Principle: Withdrawal from PMI.

The third Participant Preference sub-principle is a basic restatement of the rights of research subjects to withdraw from research at any time and dates to the 1947 Nuremberg Code. However, the articulation of that right in the context of the PMI is somewhat more complicated. In particular, the statement in this sub-principle might be interpreted to mean that Participants may not only stop providing additional information to the PMI, but might also be able to withdraw information from an ongoing research project. We recommend development of policies, procedures and notifications to Participants which would clarify when and how the right could be exercised, distinguish between identifiable and non-identifiable personal information, and articulate the limits on the withdrawal of information already in use.

Such documentation might usefully clarify that (1) consent for the use and disclosure of information that is not personally identifiable cannot be withdrawn (almost by definition, since it might not be possible to locate the information); (2) personally identifiable information, including genomic data and tissue, that is currently being use in a research

________________________________________

14 We note also that almost all states have breach notification statutes which apply to a limited data set of personally identifiable information. Most of these statutory requirements are consistent with the HIPAA Breach Notification Rule, but there are variations in notification standards in particular which would have to be taken into account. Any PMI breach notification policy should acknowledge and allow for notification according to applicable states’ requirements.

15 OECD Guidelines at 9.
project could not be withdrawn, subject to appropriate time- or project purpose-based limitations; and (3) notices of withdrawal of consent for use and/or disclosure of personally identifiable data, including genomic data and tissue, must be submitted in writing using a readily available form. In order to minimize potential Participant confusion and ensure the Participant understands the implications of withdrawal, consideration should be given to an “exit interview” discussion.

There is also a slight disconnect between the reference to withdrawal of consent and the subsequent reference to withdrawal of data. Both may need to be addressed, unless in every case the withdrawal of an individual’s consent would necessarily entail the deletion (or possibly the physical return) of such individual’s personal data/sample. This might usefully be addressed by a clarifying policy.

E. Reciprocity

The first Reciprocity sub-principle indicates that the PMI should facilitate Participants’ access to the medical information that they contribute to PMI. This raises a number of issues that need clarification, especially since such a relationship between researchers and subjects is novel.

Traditionally, participants in in human-based studies have not been provided with research findings from their specimens, medical records, or other data sets contributed to the project. For example, if a genetic mutation is discovered in the participants DNA that may predispose them to some pathologic malady, this information might not be communicated to the participant. While this practice is not universal, where applied it precludes medical interventions that might mitigate development of a malady that is potentially life threatening. This harmful potential is worth avoiding, but adoption of an alternative, open-access practice raises issues which need to be recognized and addressed.

The first issue is whether the availability of information to Participants could create an expectation of medical intervention and/or treatment, and if so by whom. The question is whether a researcher might have a duty of care to a Participant if research findings indicate a condition for which medical intervention might be possible and beneficial. Such an implication might not be apparent to the Participant, and a duty to explain data implications and/or notify the Participant’s healthcare providers might be implied. This issue should at least be analyzed, and policies and/or Participant acknowledgements of the limitations of PMI researcher (and perhaps administrator) responsibility for healthcare decisions be implemented. Participant education in such limitations should also be considered.

The second issue is that a Participant’s healthcare providers might not be able to usefully apply PMI Data. Precision medicine is a relatively new concept in the healthcare field and the number of healthcare professionals with expertise in applying such information is limited. An inability to provide appropriate healthcare may be perceived as falling below
the standard of care under these circumstances and create a liability issue for the Participant’s healthcare providers. We recommend in particular that the PMI consider development of training for healthcare professionals in this area.

A third issue is that there should be appropriate standards for Participant access to information to ensure the information has been validated through proper scientific procedures and principles. Unvalidated findings should never be communicated to participants because they may be confusing and obfuscate any meaningful application to improving healthcare. Policies and procedures for approving information for release to Participants and for validating the scientific basis for findings should be implemented.

A fourth issue is that use of Participant Data and PMI Data for treatment of the Participant may require communication of some of the information to the Participant’s health insurance carrier or self-insuring employer. The potential for use of such information in a discriminatory fashion should be considered, and if possible protections against it identified or developed. Consideration should be given to limitations on the type and content of information which should be disclosed for such purposes, and any such communications should be through the health care provider’s usual procedures rather than any direct access to PMI information.

F. Data Sharing, Access and Use

1. We support the principle that there should be multiple tiers of data access available. Such tiers should be based upon clearly articulated and objective criteria, which are publicly available to data users and contributors. Access tiers should be developed which are consistent with the terms of the Participants’ informed consent, as well as the research protocol. Indeed, PMI must ensure that the database and any access comply with applicable laws, particularly including the Common Rule, as regulations dictate that future access to, and use of, an individual’s identifiable information, be properly disclosed to the participant.

16 Though the Code of Federal Regulations exempts research involving the collection or study of existing data from human subject regulations if such information is publicly available or if the information is recorded in a manner that individuals cannot be identified, the PMI data is not public, and the database may allow for information regarding an individual to be linked to the identity of such individual. 45 C.F.R. § 101(b). It is worth noting, however, that changes to the Common Rule, including this exemption, are currently being considered. The requirements that (1) all data must exist as of the time that the study commences and (2) the researcher cannot record and retain information that identifies individuals, would be eliminated. If a researcher obtains and records identifiable information, an individual’s consent would be required; however, such consent could be obtained at the time the materials are collected by using a general, open-ended consent to future research. The ANPRM is available here.

17 Appendix D to Secretary’s Advisory Committee on Human Research Protections, available at http://www.hhs.gov/ohrp/sachrp/appendixd.html; See Note 1.
2. Access should be permitted only where there are assurances that the recipient of the data has adequate protections in place to ensure the privacy of participants and confidentiality of their information, based upon the level of data received.18

3. Access to data should be subject to a data access or comparable agreement. The terms of any agreement between the PMI and the user should be dictated by the types of data to be accessed and/or downloaded. For example, even access to de-identified data should require terms that consider the type of data to be provided, the purpose of the access, the credentials of the recipient, assurances that the recipient will comply with applicable laws as well as the consent of all participants, terms governing the PMI’s right to obtain a copy of the recipient’s research results, the rights of users and contributors to the data and research results using a contributor’s data, and requirements to ensure publication of the research results.19

4. The data access agreement should provide assurances of appropriate security for the protection of information and that data access, use, and sharing is consistent with the participants’ consent. It should also include the prohibition of the use of data for any unauthorized purpose, including the sale of the information.20 Further, since downloading of data to local systems can increase security risks significantly, if it is permitted then baseline requirements for such systems should be established, including requirements related to updated security patches.

5. The PMI should consider whether to require that data recipients agree to pay costs associated with security breach notification to affected Participants, and perhaps for penalties and fines for such unauthorized or unlawful access, use or disclosure. However, the use of penalty clauses must be flexible, and take into consideration that some institutions may be prohibited by state law from indemnifying third parties or paying the penalties.21 Any penalty clause should be proportional to the harm caused by unauthorized activity, in order to

---


19 For example, see OECD Guidelines on Human Biobanks and Genetic Research Databases, Annotation 66. With regard to publication and intellectual property terms, it will be of vital importance to researchers and institutions that institutions generating the data to be provided on PMI retain ownership to such data, and that all data provided to PMI and created using PMI data be required to be published. For many institutions, their participation in PMI will require that such data not be subject to confidentiality provisions, absent ensuring the privacy of individually identifiable information. See, e.g., University of California, Regulation No. 4; Stanford University, Policy 1.4 (Openness in Research); University of Michigan Openness in Research Policy (Standard Practice Guide 303.01); University of Minnesota, Openness in Research Policy.

20 Note that for simplicity in drafting such an agreement, many of the details of such obligations might be incorporated in PMI policies which the agreement binds the party to comply with.

ensure that institutions and researchers are not dissuaded from participating, nor precluded from participating due to state laws or institutional policies.  

6. We agree that data analyses should be conducted with coded data to the extent feasible. However, there should be available exceptions for legitimate instances in which research warrants access to non-coded data. Thus, in order to foster research that could benefit from the disclosure of non-coded data, we encourage the PMI to develop objective, transparent criteria that would enable a user to obtain access to non-coded data.

7. We agree that re-identification and re-contacting of Participants should generally be prohibited, and the terms of any data access agreement (or policies incorporated in such an agreement) should set forth both the prohibition on, as well as the consequences for, attempting to contact Participants. However, we do note that there may be instances in which identification or contact with Participants may be desirable and promote patient-powered research. For example, from accessing the data, a user may develop a study that could benefit Participants; in such a situation, both the advancement of science and the medical condition of Participants, could potentially benefit from the creation of a mechanism that enables the identification of participants. Thus, we recommend that the PMI develop a policy that sets forth the situations in which a participant may be identified and/or contacted.

8. We agree that the PMI should maintain a link to Participant identities. This linkage would enable the potential identification of Participants for future studies that may benefit both the advancement of science as well as that Participant’s individual welfare. In addition to maintaining this link, we recommend that the use of each Participant’s data should be tracked and maintained. This would enable the Participant to remain informed about the types of research that may be utilizing his or her data, and to withdraw consent for such use, if so requested by the Participant.

---

22 See above. Other public institutions are precluded pursuant to institutional policy from agreeing to terms that would impose liability for acts or omissions not directly caused by the institution or its employees and agents. See, e.g., Univ. of California, Standing Order 100.4(dd)(9).

23 However, it is worth noting that the code should not be translated in a manner that identifies the individual, and that the mechanism for re-identification should not be disclosed by the provider of such data. OHRP Guidance on Research Involving Coded Private Information or Biological Specimens, October 16, 2008.

24 OECD, for example, notes that research involving rare diseases may benefit from non-coded data. OECD Guidelines, Annotation 62.

25 OECD Guidelines provide that human biobanks and genetic research databases could set forth that access to participants will only be allowed with the written approval from the participant and from a research ethics committee. OECD Guidelines, Annotation 64.

26 Under federal regulations, research participants must be informed that their participation in research is voluntary, and that the participant may discontinue participation at any time without penalty or loss of benefits to which the participant was otherwise entitled. 45 C.F.R.§ 46.116(a)(8).
9. We concur that protection against use of Participant information from disclosure in proceedings is important; many in the research enterprise have little trust in the Certificate of Confidentiality process under the Public Health Service Act. We recommend the PMI consider more robust protections, to the extent legally possible.

G. Security

As discussed in the comments on Governance, Section II(B)(2), effective security requires governance-level commitment and involvement, with mechanisms to assure well-informed adaptation to existing and emerging threats, vulnerabilities and technical changes.

In a typical enterprise, the governance level sets (1) organizational security policies, which provide the overall mandates for limitations on use and disclosure, and protection of information which apply to all authorized users or administrators, and (2) information system security program policies, which specify the terms under which organizational policies are to be implemented in information system design, implementation and administration. Policies and procedures at this level are often referred to as “controls,” as distinguished from “safeguards.” Administrative, physical and technical safeguards for information and systems, in turn, are then implemented under the terms of these policy controls, and revised and adapted in response to changes in the environment, operating conditions, and changes in threats and technologies. For federal agencies, there is a formal process of policy-based security development and implementation including acceptance by an authorized official.

In this context, while we agree that the PMI should implement a robust Data Security Framework, to the extent that this Framework is defined as the set of administrative, physical and technical safeguards adopted for purposes of the PMI, we recommend that the Framework be considered a continuous work-in-progress under the oversight of Governance-level security program controls.

Specific program-level controls will vary depending on the architecture adopted by the PMI. Systems and data under direct PMI administration may be subject to direct program controls, while program controls in a federated or distributed architecture would have to be implemented by agreement with the parties responsible for the federated systems. Likewise, significantly different security processes would be needed for a system that permits direct participation of all individuals, rather than limiting participation to a few carefully cleared researchers. Security needs will also vary depending on whether data is mostly de-identified, and depending on how easily it can be re-identified.

Given the nature of science, technology and the security threat environment, it is likely that the factors affecting the use of various security safeguards will change over time. Therefore, a Data Security Framework should be derived from generally accepted security

---

27 See, e.g., Christiansen, supra note 4.

principles incorporated in technology-neutral program controls (policies). Specific safeguards should then be adopted and required upon recommendations of an appropriate security committee or working group, and revised and adapted as needed.

We recommend considering the following in connection with security:

- Privacy and security for the PMI are a critical component; however, at this stage, security should be approached from the perspective of establishing principles that can withstand the test of time. These principles should establish the basic expectations for security, rather than the specifics of how security should be attained.

- Security for the PMI should be structured as a framework, not a technology mandate. A good example is the NIST Cybersecurity Framework, which provides context and structure regarding the approach to cybersecurity, but remains technology-neutral and scalable. Establishing a technology-neutral, scalable framework will facilitate compliance by those entities and individuals that are already subject to other competing information security mandates, while avoiding the risk of preventing others from participating in the PMI due to cost or incompatibility with the current technology environment at the organization. Further, it will support free market choice and innovation in the development of new security approaches, as well as an agile, risk-based response to ever-evolving security threats.

- The PMI Framework should be based on the generally-accepted information privacy and security principles that have already been broadly recognized, both in the United States and abroad. Health and science are global pursuits, and it is important both for the advancement of science, and for the maintenance of the United States' position in the scientific and medical realm, for scientists and healthcare professionals to be able to share data with their international peers without undue limitations or security burdens.

- Interoperability will be an important component of data security. Incompletely interoperable software can introduce vulnerabilities that increase the attack surface or otherwise permit breaches to occur. Improved interoperability, particularly through the use of standardized processes, will help minimize the vulnerability of data as it is passed between systems.

III. Conclusion

The Section appreciates the opportunity to provide these comments. If you have any questions or would like any additional information or explanation, please contact Simeon Carson, Director, ABA Health Law Section, at simeon.carson@americanbar.org.
August 4, 2015
Page 17

Very truly yours,

[Signature]

William W. Horton
Chair
ABA Health Law Section