

February 28, 2022

Lawrence A. Tabak, D.D.S., Ph.D.
Acting Director
National Institutes of Health
9000 Rockville Pike
Bethesda, Maryland 20892

Dear Dr. Tabak,

The HIMSS Electronic Health Record Association (EHRA) member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States. Our mission is to improve the quality and efficiency of care through innovative, interoperable health information technology adoption and use.

On behalf of the nearly 30 member companies of the EHRA, we appreciate the opportunity to provide feedback on potential updates to the National Institutes of Health (NIH) Genomic Data Sharing (GDS) Policy. We support the NIH vision of rapid data sharing to advance research while protecting patient privacy and minimizing risk through formalized informed consent expectations, and we offer our input in the areas below.

Sincerely,



Hans J. Buitendijk
Chair, EHR Association
Cerner Corporation



David J. Bucciferro
Vice Chair, EHR Association
Foothold Technology

AdvancedMD
Allscripts
Athenahealth
BestNotes
Cerner Corporation
CPSI

CureMD
eClinicalWorks
eMDs
Endosoft
Epic
Experity

Flatiron Health
Foothold Technology
Greenway Health
Harris Healthcare Group
Lumeris
MEDHOST

MEDITECH, Inc.
Medsphere
Modernizing Medicine
Netsmart
Nextech
Nextgen Healthcare

Office Practicum
Sevocity - Division of
Conceptual Mindworks, Inc.
STI Computer Services
TenEleven Group
Varian - A Siemens
Healthineers Company

HIMSS EHR Association Executive Committee



Pamela Chapman
Experity



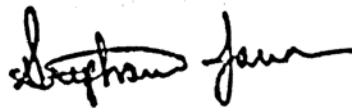
William J. Hayes, M.D., M.B.A.
CPSI



Barbara Hobbs
MEDITECH, Inc.



Cherie Holmes-Henry
NextGen Healthcare



Stephanie Jamison
Greenway Health



Alya Sulaiman, JD
Epic

About the HIMSS EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of nearly 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS.

For more information, visit www.ehra.org.

Electronic Health Record Association

Comments on the Request for Information on Proposed Updates and Long-Term Considerations for the NIH Genomic Data Sharing Policy

1. De-Identification

Permit Expert De-Identification

The EHRA supports adding the Expert Determination method as an acceptable option for de-identification under the GDS Policy. When using this method to de-identify data sets, the person responsible for determining that there is only a “very small risk” of re-identification should be made aware of the intention to submit the data set to an NIH Repository, as well as that repository’s policies for access and re-disclosure of the data set. Those details will influence the determination of the degree of risk of re-identification, though we note that *it is unlikely that many organizations would have access to large enough genomic data sources to allow them to be able to re-identify patients.*

Clarify De-Identification Expectations with OCR

There is ambiguity regarding the extent to which genomic data is considered a biometric identifier for the purposes of the 18 identifiers required for de-identification according to the HIPAA Privacy Rule. This has created challenges for entities engaging in research activities to know whether they have satisfied de-identification expectations when submitting data sets to meet obligations under the NIH’s current Genomic Data Sharing Policy.

We also note that it would be helpful if the definition of “de-identification” across various regulatory bodies was harmonized to improve the software development community’s ability to respond to these issues in a consistent way. We recommend that NIH work with the Department of Health and Human Services Office for Civil Rights (OCR) to provide greater clarity regarding the types of genomic data or scenarios in which genomic data would qualify as a biometric identifier, setting clearer expectations for entities engaging in research activities that use genomic data. We also recommend adopting a policy that considers the degree to which the genomic data could be used to identify a unique individual. If the genomic data that is part of the data set being submitted could not itself be used to identify a unique individual, it should not be considered a biometric identifier.

2. Use of Potentially Identifiable Information

Robust privacy and security measures must be implemented by NIH Repositories before it would be appropriate for potentially identifiable information to be submitted under the GDS Policy. When considering protections warranted in submitting data sets containing potentially identifiable data, the EHRA recommends employing expectations analogous to HIPAA’s privacy and security rules for the stewardship of protected health information, requiring the implementation of physical, administrative, and technical safeguards to prevent inappropriate access, use or disclosure of identifiable information.

Further, repositories should be required to hold a Certificate of Confidentiality to prevent them from being compelled to disclose identifiable information. They should also require strict adherence to data use agreements for any individual or entity accessing potentially identifiable information, with commensurate penalties for unauthorized use or inappropriate disclosure. Entities with permission to access potentially identifiable data should be prohibited from attempting to re-identify individuals in the data set.

We also request clarification to be sure that we understand what the NIH is proposing here. For entities who do want to be able to store and share identifiable information where appropriate, what exactly is being proposed? Is the NIH planning to create its own repository for public consumption? Would such a repository fall under the HIPAA framework for limited data sets, and if so, how would that work?

3. Data Linkage

A narrow reading of this could lead to a policy that indicates certain linkages are not allowed even where it is possible to craft a linked data product that includes elements of both underlying datasets that does meet the GDS Policy requirements, where, in some instances, a full linkage would not meet the same requirements. It is important not to assume risk is inherently increased as a result of linking data sets.

Recognizing the benefit of allowing combinations of existing data sets to enable more robust medical research, the EHRA supports permitting data linkage between datasets that meet GDS Policy expectations and potentially identifiable information. However, if linking two data sets compromises the de-identified nature of the resulting data set, in order to maintain patient privacy protections, we recommend that researchers combining or linking datasets be accountable for verifying that the resulting data set continues to be de-identified or take remedial action to de-identify the data set. If that is infeasible, the data set should not be re-disclosed without protections that would prohibit recipients from attempting to identify individuals who are a subject of the information and that would prevent the use or disclosure of the information for unauthorized purposes.

4. Consent for Data Linkage

At a high level, the EHRA is unsure whether there is a legitimate reason beyond public perception to treat genetic data differently than other protected health data. We believe that in practicality, it should be treated consistently with other sensitive health information, which all deserve robust and intentional protection. Making a decision to treat all sensitive data consistently would ease the work of technical resources, including the software development community, and could also do a great deal to address confusion among the provider community that currently has to remember different requirements and limitations associated with different types of data.

The EHRA does recognize the challenges inherent in prospectively informing participants about potential data linkages and appreciates the NIH objective to respect patient autonomy. Understanding that current rigorous GDS patient consent expectations include consent for the use of information in secondary research studies, we suggest that it is unnecessary to collect additional specific consent for linking data sets, particularly if due diligence is undertaken to validate that those linked data sets

continue to meet de-identification expectations. We also point out that ensuring that consent is meaningful is an issue that is much larger than just this NIH request for comment. We recommend a separate request for comment around this one topic.

Lastly, we agree that an Institutional Review Board (IRB) should weigh risks of linkage, current or future, but also be willing to revise policies as future use cases expand. The industry is still in the infancy of genomic data collection and sharing, so we caution against blanket policy approaches that may impede opportunities to maximize all patient data in the future.