



## ACMG STATEMENT

# The designated record set for clinical genetic and genomic testing: A points to consider statement of the American College of Medical Genetics and Genomics (ACMG)

**Disclaimer:** This Points to Consider document is designed primarily as an educational resource for clinical laboratory geneticists to help them provide quality clinical laboratory genetic services. Adherence to these Points to Consider is voluntary and does not necessarily assure a successful medical outcome. These Points to Consider should not be considered inclusive of all proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the clinical laboratory geneticist should apply their own professional judgment to the specific clinical circumstances presented by the individual patient or specimen.

Clinical laboratory geneticists are encouraged to document in the patient's record the rationale for the use of a particular procedure or test, whether or not it is in conformance with these Points to Consider. They also are advised to take notice of the date this document was adopted, and to consider other relevant medical and scientific information that becomes available after that date. It also would be prudent to consider whether intellectual property interests may restrict the performance of certain tests and other procedures. Where individual authors are listed, the views expressed may not reflect those of authors' employers or affiliated institutions.

This document is not intended to serve as legal advice, nor is it a legal opinion that the approaches discussed here will ensure compliance with applicable regulations. Decisions about legal and regulatory compliance are fact-specific and depend on many factors, including a laboratory's business organization, its mode of operation, and the states in which it operates. The goal of this document is to identify points that laboratories may wish to consider when developing their own compliance strategies in consultation with their own legal and regulatory advisors.

Requests for permissions must be directed to the American College of Medical Genetics and Genomics, as rights holder.

### ARTICLE INFO

#### Article history:

Received 14 November 2022

Accepted 15 November 2022

Available online xxxx

#### Keywords

Designated record set

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Individual access right

Privacy Rule

Protected health information (PHI)

### Background

Individuals have a right to access certain information in their medical records as established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).<sup>1</sup> The specific information to which individuals have access is called a designated record set (DRS), a legal term of art defined in the HIPAA Standards for Privacy of Individually Identifiable Health Information (Privacy Rule).<sup>2</sup> The Privacy Rule is a federal medical privacy law that applies to most clinical laboratories operating in the United States. Therefore, international laboratories are generally not subject to this law unless they provide and bill for testing services within the US health care system. Although an individual's right to access information held in a DRS is

Marwan K. Tayeh and Margaret Chen contributed equally.

The Board of Directors of the American College of Medical Genetics and Genomics approved this statement on October 24, 2022.

\*Correspondence: ACMG. E-mail address: [documents@acmg.net](mailto:documents@acmg.net)

A full list of authors and affiliations appears at the end of the paper.

doi: <https://doi.org/10.1016/j.gim.2022.11.010>

1098-3600/© 2022 American College of Medical Genetics and Genomics. Published by Elsevier Inc. All rights reserved.

clearly established and legally enforceable, laboratories engaged in genetic and genomic testing have faced lingering uncertainty about what is included in the DRS and how to implement HIPAA's access right. HIPAA-regulated laboratories that receive such requests are obligated to provide direct access and "may not impose unreasonable measures on an individual requesting access that serve as a barrier to or unreasonably delay the individual from obtaining access."<sup>3</sup> Laboratory personnel have at times struggled to square this legal directive with their prior customs and ethical duties to avoid unnecessary and foreseeable harm.

This statement (1) highlights key provisions of the HIPAA Privacy Rule that create the individual right of access to data in the DRS, (2) summarizes the guidance the US Department of Health and Human Services (HHS) has offered about what the DRS means and how it applies at clinical laboratories engaged in genetic and genomic testing, (3) explores ethical and practical concerns that continue to surround this legally enforceable access right, and (4) identifies specific points genetic and genomic laboratories should consider when crafting their own compliance strategies and procedures for implementing HIPAA's individual access right.

The workgroup tasked with developing this points to consider statement was composed of individuals with expertise in laboratory genetics, clinical genetics, genetic counseling, bioethics, and health law. This statement was informed by targeted review of literature discussing or referencing HIPAA's access right, located through searches on its Code of Federal Regulations citation "45 C.F.R. § 164.524," as well as a diligent review of relevant statutes, regulations, regulatory guidance documents, and case law. Resources consulted included PubMed, relevant American College of Medical Genetics and Genomics (ACMG) guidelines, Federal and Administrative law materials accessible on the Thomson Reuters Westlaw legal database, and regulatory agency web sites. The workgroup members also used consensus expert opinion and empirical data to inform their recommendations. Conflicts of interest for workgroup members were reviewed per ACMG policy and are listed at the end of the paper. The ACMG Laboratory Quality Assurance Committee and the ACMG Social, Ethical and Legal Issues Committee reviewed the document, providing further input on the content, and a final draft was presented to the ACMG Board of Directors for review and approval to post on the ACMG website for member comment. Upon posting to the ACMG website, an email and a link were sent to all ACMG members inviting participation in the 30-day open comment process. All members' comments and additional evidence received were assessed by the authors, and these recommendations were incorporated into the document as deemed appropriate. Member comments and author responses were reviewed by representatives of the ACMG Laboratory Quality Assurance Committee, the ACMG Social, Ethical and Legal Issues Committee, and the ACMG Board of Directors. The final document was approved for publication by the ACMG Board of Directors.

## Discussion

### General principles

#### HIPAA's right of access to genetic and genomic information

The HIPAA<sup>1</sup> Privacy Rule<sup>2</sup> establishes a set of national standards for the protection of certain health information.<sup>4</sup> HHS finalized the Privacy Rule,<sup>5</sup> which became effective on a phased schedule in 2003-2004. The Privacy Rule addresses the use and disclosure of individuals' protected health information (PHI), the term for identifiable health information that HIPAA protects.<sup>6</sup> The Privacy Rule also creates federally protected civil rights for individuals to understand and control how their health information is used. One of those rights is a legally enforceable right for individuals, upon request, to inspect and receive a copy of their own health information: the so-called HIPAA access right.<sup>3</sup> Within HHS, the Office for Civil Rights (OCR) has the responsibility for implementing and enforcing the Privacy Rule, including its mandatory access right.

Not all laboratories that conduct genetic and genomic testing are HIPAA-covered entities that are subject to the Privacy Rule and, thus, to its access right. HIPAA-covered entities include, but are not limited to, laboratories that conduct specific types of electronic transactions such as billing for health care services or verifying insurance benefits. Therefore, virtually all clinical laboratories that bill for testing services are HIPAA-covered entities.<sup>7</sup> Business associates of a HIPAA-covered laboratory also become HIPAA-covered and must comply with the Privacy Rule.<sup>6</sup> Thus, a software service provider that receives PHI from a HIPAA-covered laboratory to provide data-analysis services for that laboratory also falls under the Privacy Rule and must comply with its requirements. Note, however, that a non-HIPAA-covered investigator who receives data from a covered entity for use in research (for example, pursuant to an institutional review board (IRB)-approved HIPAA waiver)<sup>8</sup> would not usually become a business associate to the entity that supplied the data. However, research laboratories can become HIPAA-covered entities if they electronically conduct even a single billing-related transaction or if they function as part of a larger covered entity, such as a hospital or academic medical center that is HIPAA-covered.<sup>7,9</sup> Once a laboratory becomes a HIPAA-covered entity, the Privacy Rule protects all of the PHI it stores, whether in paper or electronic formats.<sup>6</sup>

The original Privacy Rule that took effect in 2003-2004 had provisions exempting laboratories from the HIPAA access right if the laboratories were in states that limited individuals' direct access to laboratory information. That changed on February 6, 2014, when the Clinical Laboratory Improvement Amendments of 1988 (CLIA)<sup>10</sup> regulations<sup>11</sup> and the HIPAA Privacy Rule were both amended to expand individuals' right of access to information held at HIPAA-covered laboratories.<sup>12</sup> Those 2014 amendments preempted (nullified) state laws when they interfere with HIPAA's

access right,<sup>12</sup> such as state laws requiring laboratories to report information to clinicians rather than to individuals. These changes took effect on October 6, 2014, granting individuals the right to inspect and receive copies of identifiable information in their DRS maintained by HIPAA-covered laboratories. HIPAA's access right is designed to enhance privacy by empowering individuals to know what types of information are being stored about them.

### State and federal data storage requirements

Individuals have the right to access data in their DRS as long as a HIPAA-covered laboratory keeps the data in an identifiable form. Genetic and genomic laboratories generate a massive amount of data that requires expansive data storage infrastructure. The Privacy Rule does not itself set any data storage requirements. Instead, HIPAA-covered laboratories should be guided by genetic and genomic data storage requirements mandated by state and federal governments, CLIA regulations, and College of American Pathologists (CAP) guidelines. Per CAP guidelines, next-generation sequencing (NGS) data/variant calling files as well as chromosomal microarray data that support primary results and reanalysis must be saved for a minimum period of 2 years (Molecular Pathology Checklist, CAP, version 9.22.2021). Images of G-banded karyograms and fluorescence in situ hybridization (whether digital or hardcopy) must be retained for 10 to 20 years, depending on whether testing is being performed for neoplastic vs constitutional disorders, respectively (Cytogenetics Checklist, CAP, version 9.22.2021). Likewise, CAP requires laboratories to retain reports for 10 to 20 years, for neoplastic vs constitutional disorders, respectively. Laboratories which are certified by and fall under the jurisdiction of the New York State Department of Health must retain laboratory reports for a minimum of 7 years, with cytogenetics reports being an exception, requiring an extended storage period of 25 years.<sup>13</sup> Biochemical genetic test reports that indicate disease genotype information in the report should be retained for at least 21 years after the date of reporting, and must comply with applicable state laws and other requirements that mandate longer retention.<sup>14</sup>

### The DRS

A DRS is the set of information to which an individual has a right of access through a HIPAA-covered facility, if the individual requests the information. The Privacy Rule's definition of DRS notes that it includes information "about individuals" that is "maintained by or for a covered entity."<sup>15</sup> Thus, an individual's DRS only includes information about that individual and does not include information about other people that might be present in an individual's medical files, and it only includes information that is currently stored by the covered entity at the time an access request is made. The information contained in an individual's DRS can differ from one HIPAA-covered facility to the next, because each facility (a hospital, a laboratory, a primary care provider, etc) maintains different information about that individual.

#### Box 1. DRS components of relevance to genetic and genomic laboratories

- Laboratory reports
- Identifiable laboratory data
  - All available electronic raw data files (eg, fastq, bam, vcf, ab1, cel, bpm, get, wiff). However, laboratories are not required to provide any additional in silico files or software to help assess the validity of the data.
  - Paper raw data (eg, printouts, pictures, graphs, plots).
- Billing information
- Health record information

The crucial question is what types of information are encompassed by the DRS. The Privacy Rule states that the DRS includes medical records and billing records of health care providers (including clinical laboratories) and various information held by health plans.<sup>15</sup> The Privacy Rule also requires a covered entity to include a record in the DRS if it is "used, in whole or in part, by or for the covered entity to make decisions about individuals."<sup>15</sup> This last provision means, eg, an individual's entire binary alignment map (bam) or variant call format (vcf) file would be in the DRS, if the covered entity uses any part of those files to make decisions (Box 1).

In 2000, the HHS offered guidance on the DRS and interpreted it rather broadly to include "records that are used to make decisions about any individuals, whether or not the records have been used to make a decision about the particular individual requesting access."<sup>16</sup> Thus, a variant that was not included in the original targeted testing for an individual who is requesting access is nevertheless included in that individual's DRS, if the laboratory ever uses that variant in any decision-making for any individual. In 2016, the HHS provided further guidance stating that the DRS encompasses the laboratory test reports, the underlying information generated as part of each test, as well as other information concerning tests a laboratory runs on an individual.<sup>17</sup>

Specifically, for HIPAA-covered clinical laboratories that conduct NGS of DNA, HHS/OCR has stated that the DRS includes a copy of the completed test report, the full gene variant information generated by the test, as well as any other information concerning the test.<sup>3</sup> This would include all available raw and curated data files (eg, fastq, bam, vcf, ab1, cel, bpm, get, wiff, to name a few). However, the DRS would not include any additional in silico files or software to help assess the analytical validity of the data.

It is important to note that an individual has a right of access to information within a file that is identifiable to that specific individual, but not to data in that file relating to other individuals, including other family members' data generated to assess zygosity and/or inheritance. Hence, if a laboratory has deidentified information in accordance with HIPAA's standards—ie, using HIPAA's safe-harbor or expert determination methods<sup>18</sup>—the data are no longer

considered part of a person's DRS. At present, HHS does not expect laboratories to reidentify "deidentified" data to fulfill individual access requests. This is true even though data that has been deidentified under HIPAA's standards may not, in fact, be fully anonymized, and might in theory be linkable to the individual. Furthermore, individuals have no right of access to information that has been destroyed or discarded under a laboratory's data-retention practices. Such information is no longer "maintained" by the laboratory. The Privacy Rule has no requirement that laboratories must retain information solely to enable individual's access (although laboratories may, of course, be subject to data-retention requirements under the CLIA<sup>10,11</sup> regulations, CAP guidelines, or relevant state medical records laws).<sup>19</sup> Finally, it is important to note that the location of stored information, such as at an off-site facility or cloud storage provider, does not alter whether it is part of an individual's DRS. The laboratory is obliged to retrieve the information and to grant access upon request.

In summary, HIPAA-covered laboratories should be aware that the DRS includes not only laboratory test reports, but also identifiable underlying information generated as part of each test and stored in electronic or paper formats (Box 1). Of note, the DRS is the amount of information an individual theoretically has access to. The laboratory is only required to provide access if the individual actually requests it. When an individual makes an access request, the individual may choose not to receive all the information in their DRS. For example, they may request a copy of the laboratory report and not the full gene variant file. In such instances, HIPAA-covered laboratories are only obligated to provide what the individual has requested and do not have to provide the entire DRS.

### Interacting with individuals who are considering making an access request

A natural question is whether laboratories can help guide the choices individuals make about what to request, to avoid unnecessary requests for the entire DRS when a more narrowly tailored portion of the DRS would have met the individual's needs. The Privacy Rule strictly limits how far covered entities can go in trying to steer or discourage access requests.<sup>3</sup>

By law, HIPAA-covered laboratories are required to document the DRS(s) they hold that are subject to access by individuals.<sup>20</sup> This list must be available in paper or electronic form.<sup>21</sup> Laboratories also must explain whom an individual should contact to gain access to those data.<sup>20</sup> Documenting the information in the DRS offers an opportunity for genetic and genomic laboratories to explain, in layperson's terms, the nature of the files (eg, fastq, bam, vcf) in the DRS and the types of information they contain. Such information can help individuals make informed choices about which files are most responsive to their needs and whether files contain duplicative information.

Beyond that, HHS cautions against trying to influence individuals' access requests—unless, of course, the individual asks for help. HHS/OCR states that a covered entity "may not require an individual to provide a reason for requesting access," and if individuals voluntarily share their rationale for requesting access, this "is not a permitted reason to deny access."<sup>3</sup> Individuals can request any part, or all, of their DRS, and it would violate the Privacy Rule to erect barriers that deter people from requesting their data.<sup>3</sup> There is no HHS/OCR guidance on what counts as facts about the contents of the DRS (eg, a data quality disclosure) vs what counts as a barrier to access (eg, warnings that try to dissuade people from exercising their access right by emphasizing possible harms of accessing the data). At the point when individuals are weighing whether to make an access request, the safest course is to offer facts explaining what is in the DRS, while minimizing value judgments about whether the individual is right to request access and whether access might harm the individual.

Of note, the Privacy Rule is a "what's-on-file-is-what-you-get" right and does not require laboratories to conduct any further reinterpretation or to provide interpretive or explanatory assistance to help individuals understand the clinical meaning of information stored in their DRS.<sup>3</sup> The Privacy Rule allows a laboratory, in its sole discretion, to provide an explanation of the DRS but only if both sides can agree on fees for providing the explanation and the individual agrees in advance to cover them.<sup>22</sup> Otherwise, laboratories have no obligation under HIPAA to provide counseling or explanatory services along with the data.

### Exceptions to the individual right to access

Once an individual makes an access request, HIPAA-covered entities are required to provide requested portions of the DRS to individuals within 30 days (with up to one 30-day extension).<sup>23</sup> The HHS is currently considering amending that time line to 15 days (with one 15-day extension).<sup>24</sup>

The Privacy Rule has a few exceptions to the HIPAA access right.<sup>25</sup> The exceptions are narrow, and HHS intends for covered entities to invoke these access exceptions "rarely, if at all."<sup>26</sup> If a covered laboratory has grounds to deny access to some data elements in an individual's DRS, it still must provide access to all remaining information in the DRS that the individual has requested.<sup>27</sup>

Most of the HIPAA access exceptions rarely have any relevance to genetic and genomic laboratories: eg, individuals cannot access psychotherapy notes, data developed for use in court proceedings, and prison health care data.<sup>28</sup> Occasionally, other exceptions might be relevant in specific circumstances: eg, there are exceptions for government-held data that is subject to individual access restrictions under the Privacy Act of 1974 and data that would divulge confidential information about third parties.<sup>29</sup> There are, however, 2 exceptions of which every genetic and genomic testing laboratory needs to be aware.



**Box 2.** Potential implications of denying an individual's HIPAA access right

- The compliance date for HIPAA-covered laboratories to provide access to laboratory-held data in patients' DRS was October 6, 2014. In 2018, Lye et al documented ongoing problems patients face when exercising their HIPAA access rights in various health care settings.<sup>33</sup>
- Patients wrongly denied access to their data cannot sue HIPAA-covered entities directly. They must file a complaint with the HHS Office for Civil Rights, which contacts the covered entity to enforce access. In 2016, the American Civil Liberties Union filed a complaint on behalf of 4 breast cancer patients and family members who were denied access to variant data after testing by Myriad Genetics. On the eve of filing the complaint, Myriad provided the patients with their data.<sup>34</sup>
- When a covered entity repeatedly denies access or fails to cooperate with an HHS complaint investigation, the Secretary of Health and Human Services has the power to sue the covered entity on behalf of patients who were denied access. One such suit, *Sebelius v Uplift Med., P.C.*, enforced civil fines of \$4.3 million for denial of timely HIPAA access by 41 patients or approximately \$100,000 per denied patient.<sup>35</sup>
- The late Steven Keating, diagnosed with brain cancer while pursuing PhD studies several years ago, donated tumor tissue to a research study, assuming he would have access to the genome sequencing results. The laboratory withheld access based on a disputed legal theory about how HIPAA's access right works.<sup>36</sup> "I wanted to see my sequence and share it with the world to benefit science. Instead, the reward for donating valuable tumor tissue was a legal barrier preventing me from seeing my future." He ultimately was granted access after a difficult struggle and shared his data as a legacy for future research.<sup>37</sup>

The first is that there are reviewable grounds for denying a request for access if a "licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person."<sup>30</sup> To invoke this exception, the covered entity must promptly explain its denial to the individual in writing, grant the individual a timely review of the denial by a second licensed health care professional, and abide by that reviewer's decision.<sup>31</sup> Laboratories need to be aware that HHS takes a narrow view of what counts as a danger to life or safety (eg, suicide-risk qualifies, but mere emotional distress or psychosocial harm or the possibility that a layperson might misunderstand the information do not qualify).<sup>3,12,32</sup> In addition, the regulations envision that a "licensed health care professional" would make this determination—presumably a health care provider who is in a treatment relationship with the individual and knows their overall situation well, as opposed to an ethicist, ethics committee, or laboratorian who has not interacted closely with the individual. HIPAA-covered entities should know that the statute and regulations provide potential penalties for unjustified denial of the HIPAA access right (Box 2).

The second important exception addresses individual access to identifiable information generated during clinical research. Somewhat controversially, the Privacy Rule allows access to research data. There is only a narrow exception allowing access to be temporarily suspended if it would "unblind" a clinical trial that is in progress. This exception applies, however, only if the individual consented to the suspension of access when consenting to participation in a research study, and if the access will be reinstated upon completion of the research.<sup>38</sup> If those steps have been followed, access can be suspended temporarily, and the suspension is not subject to further review. This is

the only exception the Privacy Rule provides for information from research, which is otherwise subject to HIPAA's access right when held by a HIPAA-covered laboratory.

### The role of IRBs

Laboratories with joint research and clinical testing portfolios often assume that the local IRB should help adjudicate DRS requests, which is not correct. The Privacy Rule does not provide for IRBs to be involved at the point when individuals are contemplating making an access request, eg, to make sure individuals are informed about potential risks of seeking access. Such involvement could be seen as interfering with individuals' right to request access.<sup>3</sup> Nor does the Privacy Rule call for IRBs to adjudicate whether one of HIPAA's limited access exceptions applies. Instead, access is treated as a federally protected civil right to be administered and enforced by HHS/OCR.<sup>39</sup> The Privacy Rule sets a floor (or minimal required level) of privacy protection, and states or institutions are free to implement "more stringent" privacy protections. With respect to the HIPAA access right, the Privacy Rule makes clear that a "more stringent" privacy protection is one that involves giving people "greater rights of access" than the Privacy Rule requires.<sup>40</sup> Allowing an IRB to interfere with or reduce individuals' HIPAA access rights would amount to a less stringent privacy protection, which would violate the HIPAA Privacy Rule.

In summary, covered entities "must provide the access requested by individuals."<sup>41</sup> If the data are not in their possession, they "must inform the individual where to direct the request for access."<sup>42</sup> Thus, if a patient requests complete variant data from a clinician who only has the final test report, the clinician is obligated to refer the patient to the laboratory. Once the request is directed to the laboratory, the

laboratory “must provide the access” if the laboratory has the information on file. There is no provision in the Privacy Rule allowing an IRB to block access based on any ethical concerns that the IRB identifies.

The IRB can, however, recommend ethical measures to be taken at the point of data delivery (PODD)—ie, at the time data are delivered to the requesting individual, which may be as long as 30 to 60 days after the request was made (or 15-30 days if proposed changes take effect). These measures could include, eg, clear disclosures about data quality issues or warnings against improper data uses. Such measures do not interfere with individual access, but rather aim to make access as safe and useful as it can be. PODD disclosures, made when data are transferred to requesting individuals, should not be confused with informed consent. Informed consent is relevant before a person makes a decision. In this case, an individual already has decided to request data—because HIPAA grants them a right to do so—and PODD disclosures aim to promote safe, appropriate use of the data after receipt.

### Logistics of delivering data in response to HIPAA access requests

When responding to access requests, HIPAA-covered laboratories are required to provide data “in the form and format requested by the individual” if the information “is readily producible” in that format.<sup>43</sup> If a laboratory stores files electronically, individuals are entitled to receive data in their preferred electronic format if it is readily producible or, if not, in an alternative “readable electronic format” on which both sides agree.<sup>44</sup> HHS clarifies that a covered laboratory “is not required to purchase new software or equipment to accommodate every possible individual request,” but it must be capable of providing some form of electronic copy of data that it maintains electronically. If an individual declines all of the readily producible electronic formats the laboratory offers, the final default would be to a readable hard copy,<sup>3</sup> although it is not clear this guidance appreciates the vast size of some genomic data files.

HHS regards mail and email to be readily producible delivery methods, but recognizes that email cannot always accommodate the file size for certain data types and can pose security risks in transit.<sup>3</sup> Encrypted transmittal methods should be the default, although it is acceptable to use unencrypted methods if an individual insists on unencrypted transmittal after being informed of the risks.<sup>3</sup> “A covered entity is not expected to tolerate unacceptable risks to the security of its systems;” therefore, a laboratory could decline a request to download data onto a suspect storage device provided by the individual. Alternatives would be for the laboratory to supply a new storage device “at cost” if the individual is willing to cover the cost. If the individual refuses, the final options may be mailing a hard copy, emailing, or making the data available for the individual to download through a secure, internet-based portal.

The Privacy Rule strictly limits the fees HIPAA-covered laboratories can charge for providing access. They can charge a “reasonable, cost-based fee” based on (i) labor for copying the requested PHI in paper or electronic form, (ii) supplies for creating the paper copy or electronic media (eg, CD or USB drive) if the individual requests the data on portable media, and (iii) postage for mailing records the individual asks to be mailed.<sup>45</sup> Although laboratories are not required to prepare a summary or explanation, they can charge a preagreed fee for doing so if the individual has requested those services and agreed in advanced to pay for them.<sup>45</sup>

Laboratories should be aware that the allowed labor costs do not include all of the costs they may actually incur while responding to access requests. HHS states that the “fee may not include costs associated with verification; documentation; searching for and retrieving” the requested data or the cost of “maintaining systems, recouping capital for data access, storage, or infrastructure” even if such costs are authorized by state law.<sup>3</sup> This incentivizes laboratories to maintain orderly information systems that allow expeditious file location and retrieval. Laboratories can recover labor costs for making and delivering copies “once the PHI that is responsive to the request has been identified, retrieved, and collected, compiled and/or collated, and is ready to be copied”—in other words, after the data have already been located and prepared.<sup>3</sup> Moreover, laboratories cannot recover the costs of “labor associated with ensuring compliance with HIPAA (and other applicable law) in fulfilling the access request (eg, verification, ensuring that only information about the correct individual is included).”<sup>3</sup> Scholars sometimes refer to HIPAA’s access right as an “unfunded mandate,”<sup>46,47</sup> but it is better thought of as a cost of doing business in a world where most modern privacy laws (including the European Union’s General Data Protection Regulation and many US state privacy and medical records laws) protect individuals’ right of access.

### Points to consider

- Individuals have the right, which is protected by federal privacy law, to inspect and receive copies of data in their DRS from HIPAA-covered entities as long as the data are stored and are identifiable to the requesting individual.
- HIPAA requires laboratories to provide access to requested portions of the DRS within 30 calendar days of receiving an individual’s request. A single 30-day extension is allowable if written justification is provided to the individual. Of note, rulemaking is in progress that could change this to 15 days with one 15-day extension.
- HIPAA requires laboratories to document the types of data and files included in the DRS and identify whom individuals should contact to request access.
- The DRS includes the laboratory test reports and any identifiable underlying information generated as part of the test and stored in electronic or paper formats.

- HIPAA-covered laboratories are only required to provide those elements of the DRS (data or files) that the individual requests. They do not have to provide the entire DRS unless an individual asks for the complete DRS.
- At the point when individuals are weighing whether to request HIPAA access, it is inappropriate for HIPAA-covered laboratories to try to influence, discourage, or limit the amount of information people request. Laboratories can, however, provide factual descriptions of the types of data that are accessible in the DRS, and laboratories can respond to questions individuals raise as they decide which elements of the DRS are most responsive to their needs.
- Once an individual submits an access request and a laboratory is providing data in response to it, HIPAA-covered laboratories, if they wish to do so, can attach PODD disclosures to help the recipient understand limits and appropriate uses of the data.
- HIPAA-covered laboratories are not required to provide interpretive assistance or reinterpretation at the time patients request HIPAA access to information in their DRS, but HIPAA allows laboratories to do so, at their discretion, if the patient requests it and agrees to cover costs associated with the additional analysis.
- Data must be provided in the form and format requested by the individual, as long as the requested form and format are “readily producible” by the laboratory. This standard does not require laboratories to purchase new equipment or software, or to share their software with individuals, to accommodate individuals’ format requests, but data stored in electronic formats should be provided in some “readable electronic format” if individuals request it.
- The DRS may include information for which the individual has not previously been consented, eg, when the individual first consented to exome sequencing or if the individual declined to receive secondary findings that are part of the entire data set included in the DRS. The Privacy Rule does not require a further consent process as a precondition of responding to individual access requests nor does it allow laboratories to require processes that “serve as barriers to or unreasonably delay the individual from obtaining access.”<sup>3</sup>
- HIPAA does not itself set data storage or retention requirements, therefore clinical laboratories should comply with the data storage requirements established by the state law, federal CLIA regulations, and accreditation standards such as CAP guidelines.
- HIPAA-covered laboratories can deny an individual’s right of access only in certain specified situations. Some of these grounds grant the individual a right to have such denials reviewed by a licensed health care professional and others require preparatory steps such as having patients agree in advance to have their access rights temporarily suspended, eg, during clinical research.

- The HIPAA privacy rule does not call for IRBs to play a role in adjudicating access requests, and it is not proper to inquire why individuals want their data or otherwise erect barriers that delay or interfere with individuals’ right to request access. IRBs can, however, help define ethically appropriate PODD disclosures and warnings to be delivered at the time when laboratories provide data to requesting individuals.

### Considerations for genetic and genomic data

Although genetic and genomic data are included in HIPAA’s individual access right, these data may be considered qualitatively different than other kinds of health information. For example, genetic and genomic data in a DRS could predict later-onset medical conditions, inform reproductive risks, and/or could hold implications for other family members.<sup>48</sup> When delivering genetic and genomic data in response to an access request, it may be ethically appropriate to accompany the data with PODD disclosures to help the data recipients understand appropriate precautions and uses of the data they are receiving. This section highlights several topics that a laboratory might choose to address in its PODD disclosures.

### Potential risks and limitations of using or sharing genetic and genomic data in a DRS

The interpretation of genetic and genomic data is a dynamic process that evolves over time as new scientific evidence becomes available. Therefore, genetic and genomic data accessed via a HIPAA access request may not always reflect the most up-to-date interpretation, and in certain cases, updated testing (achieved via independent analysis of a new DNA sample) may be more appropriate than relying on older data available through HIPAA access rights. HIPAA-covered laboratories are not required to provide new or updated interpretation of genetic and genomic data in response to an access request. This creates a concern that data recipients could erroneously conclude that the data they are receiving are current as of the date of their data request as opposed to the earlier date when testing was performed. Laboratories may wish to consider including a clear, prominent statement that data provided through a HIPAA access request were current only as of the date the test was performed, have not been updated or reinterpreted, and may not match the results that could be obtained if retesting was performed using current testing methodologies.

In addition, laboratories may wish to make clear that genetic and genomic data released as part of a HIPAA access request are not intended for use in clinical decision-making without appropriate clinical guidance. Raw genetic and genomic data may include information of uncertain analytical validity, such as variants in regions of poor coverage, sequence homology, or mapping errors. In addition, the initial analysis may have been limited (eg, exome

was performed but secondary findings were originally declined) or targeted to specific regions (eg, targeted disease panels) of the genome. Secondary analysis using third-party interpretation services of potentially low-quality data may result in false-negative or false-positive results.<sup>49-51</sup>

More generally, laboratories should also be aware that providing data (whether to an individual or to a clinician) can trigger unwanted US Food and Drug Administration or CLIA scrutiny if the regulator concludes the laboratory intended the data for clinical use. Laboratories responding to a HIPAA access request may wish to consider stating, clearly and in writing, that they are providing the data strictly to comply with the Privacy Rule's access right. They may wish to point out that data released as part of a HIPAA access request sometimes goes beyond what was included in the patient's original test report. A laboratory may wish to state that only the original test report was intended for clinical use and that any other data being received as part of an access request *are not* intended for use in the diagnosis of disease of other conditions; in the cure, mitigation, treatment, or prevention of disease; or for the assessment of health and *should not* be used for those purposes.<sup>52,53</sup>

Ideally, reanalysis of genetic and genomic data should be performed at the clinical laboratory that initially performed the testing. In instances when this is not feasible, performing this service at another CLIA-compliant clinical laboratory, as opposed to a non-CLIA laboratory or online interpretation service, is recommended, although reinterpreting data from one CLIA-compliant laboratory at a different CLIA-compliant laboratory may not constitute a clinical quality result unless the entire testing process has been validated. It is important to keep in mind that there can be variations in the quality of non-CLIA third-party interpretation services and therefore these results are not considered to be equivalent to a clinical test result.<sup>49</sup> A potential harm of access to the DRS is that individuals may attempt to make medical decisions based on incorrect data or misinterpretation of the significance of the results (Table 1). Adverse outcomes from misinterpretation of data by individuals can include failure to recognize a pathogenic variant in a given gene or if an initial test was not comprehensive, resulting in a delay of care. Conversely, misinterpretation of results could lead to medical decision-making resulting in patient harm, such as proceeding with a bilateral mastectomy in the case of a nondiagnostic variant of uncertain significance in a hereditary cancer gene.<sup>54-56</sup> Results obtained through third-party interpretation services or research studies must therefore be confirmed in a CLIA-compliant clinical laboratory before making any medical decisions (Table 1).<sup>49</sup>

Although the ability to obtain and share one's genetic and genomic data helps limit duplicate data collection, individuals need to be aware of the potential risk of privacy breaches if they upload or share data on an unprotected site or with a third-party. The risks of sharing data for research use include that once such data are publicly released, they may be virtually impossible to retrieve or make private

again. There are some options to mitigate these risks, including data anonymization and data access controls for data security.<sup>51</sup> Laboratories may wish to caution patients and their families about the need for responsible data sharing if they wish to facilitate future research endeavors by sharing their data to help create larger data sets. Sharing in this manner could yield clinically useful evidence and has the potential to improve our understanding of a condition and inform precision medicine specific treatments, but awareness of privacy risks is warranted.

### Potential implications for family members

The genetic and genomic data in a DRS may reveal sensitive information about disease risk status that is shared with other family members. These family members may not want to receive information about potential shared disease risks. Laboratories responding to access requests may wish to urge recipients to be discreet and encourage them to speak with at-risk adult family members about whether they would want to know any medically relevant findings if identified. Similar to consenting before genetics testing, it may be wise to inform data recipients that further analysis of the genetic and genomic data can reveal unexpected findings, including evidence of consanguinity and/or misattributed parentage.<sup>57</sup>

Genetic and genomic data in a minor's DRS may have the potential to provide information on disease risks of relevance to biological parents and other adult family members. Furthermore, analysis of genetic and genomic data from a minor's DRS could reveal information about risk for adult-onset conditions. This could undermine the minor's future autonomy and has the potential to negatively affect the parent-child relationship.<sup>58</sup> Therefore, laboratories may consider reminding adult data recipients that a child's views about a DRS request should be elicited before communicating any information. Finally, it may be appropriate to caution caregivers that they have an ethical obligation to inform the child of the HIPAA access request when that child is capable of making their own decisions and transfer access and decision-making responsibility to the child when age-appropriate.<sup>59</sup>

Similarly, genetic and genomic data received through a HIPAA access request could potentially become a valuable postmortem resource for subsequent generations, and laboratories may wish to advise data recipients on appropriate preservation and future sharing of the data they receive. For example, consider the case of an individual who succumbed to sudden cardiac death at a young age and had genetic testing performed before death. The genomic data generated from the prior clinical testing that is part of the decedent's DRS is the most informative sample for consideration of reanalysis for hereditary arrhythmias (eg, long QT syndrome) or structural cardiac disease (eg, hypertrophic cardiomyopathy). Reanalysis of such genetic and genomic data in a DRS might encourage family members to seek clinical care.<sup>60</sup>



**Table 1** Different plausible scenarios for requesting data in a DRS

Individual Request	Laboratory Response
<p>Individual A contacts a clinical laboratory to request a copy of their original test report.</p>	<ul style="list-style-type: none"> <li>• Laboratory verifies the identity of the requesting individual and confirms the access request is for the report only.</li> <li>• The report is shared with the individual via a secure portal (or by mail or email if the individual requested such delivery).</li> <li>• The laboratory does not have to provide any other data included in the DRS.</li> </ul>
<p>Individual B contacts a clinical laboratory to request data about a specific variant. The variant is located in an intronic region outside of the stated targeted region of the initial test.</p>	<ul style="list-style-type: none"> <li>• The clinical laboratory is not obligated to query the individual's data for a specific variant that is not currently maintained in the laboratory's files.</li> </ul>
<p>Individual C submits a HIPAA access request to obtain their vcf file in a pdf format and requests delivery via secure email. The data are stored at an off-site information facility for the laboratory.</p>	<ul style="list-style-type: none"> <li>• The individual can request the full variant data because it is contained in the raw data file as a part of their DRS.</li> <li>• The off-site location of the stored data does not affect whether it is included in the DRS.</li> <li>• Laboratory retrieves the requested vcf file and prepares a copy.</li> <li>• Laboratory must accommodate reasonable requests concerning format and mode of delivery. HHS considers a pdf file to be a "readily producible" format that covered entities should be able to provide.</li> <li>• Laboratory may contact the individual to discuss alternatives for delivery if the pdf file is too large for email delivery. Alternatives could include mailing the file on an encrypted USB storage device if the individual agrees to pay "at cost" reimbursement for the device, or making the pdf file available through a secure portal for the individual to download.</li> </ul>
<p>Individual D requests the data be emailed to a nonsecure email account. The laboratory's policy states that HIPAA-protected health information should not be sent through nonsecured, unencrypted transmission.</p>	<ul style="list-style-type: none"> <li>• Laboratory should consider providing a PODD disclosure form along with the data, detailing limitations of variant data not included in the initial test report and providing other information and warnings to promote appropriate future uses of the data.</li> <li>• Laboratory should inform the individual of preferred method of data sharing through a secure ftp server.</li> <li>• However, HHS has made it clear that if the individual nevertheless prefers to receive the data via a less-secure method of transmission, the laboratory should honor the individual's preference.</li> <li>• The laboratory may wish to document that it informed the individual about the privacy risks and that the individual nevertheless insisted on nonsecure transmission.</li> </ul>
<p>Individual E cannot access the ftp server and requests that the data be copied onto a personal USB device. Laboratory policy does not allow the use of external/personal USB drives for security reasons. The laboratory prefers to provide copies of the data on an approved USB device that the laboratory supplies.</p>	<ul style="list-style-type: none"> <li>• Promptly within the 30-day period for delivery of the data, laboratory contacts the individual to offer alternatives for electronic delivery of the requested data.</li> <li>• Laboratory offers to ship the data on an approved, encrypted USB device "at cost" and the individual agrees to reimburse the cost of the device.</li> <li>• The USB is shipped to the patient through a certified means that requires confirmation of receipt.</li> <li>• In total, the laboratory charges the individual a reasonable cost-based fee for the cost of (i) labor for copying the data onto the USB device and shipping it but excluding labor costs to locate and retrieve the requested data and remove extraneous data elements that cannot be shared (eg, joint calling files with information about other individuals), (ii) the "at cost" price of the approved USB device that the individual agreed to reimburse, (iii) delivery costs including the cost of packaging and certified shipping. If the laboratory and individual mutually agreed that the laboratory would provide an optional explanation or summary, laboratory may also charge the preagreed fee for providing that service.</li> </ul>

(continued)

**Table 1** Continued

Individual Request	Laboratory Response
Individual F requests laboratory data about how frequently a variant of interest has been identified.	<ul style="list-style-type: none"> <li>• This information is not “about” the individual and is not part of the DRS. Laboratory is not required to comply with this request.</li> <li>• Laboratory, at its discretion, can come to an agreement with the individual to provide this additional analytical support for a fee that both agree to.</li> </ul>
Individual G contacts laboratory interested in learning more about how to interpret the variant data obtained through an earlier access request. Individual G is also interested in learning about health risks to be proactive and seeks advice about third-party interpretation services to provide variant interpretation and health data.	<ul style="list-style-type: none"> <li>• Laboratory must comply with requests for variant data included in an individual’s DRS but is not required to provide analytical support or interpretive services.</li> <li>• Laboratory is not obligated to help the individual understand variant data received under an access request.</li> <li>• If the laboratory routinely provides patient-directed testing and interpretation services, it could at its sole discretion agree to provide the requested analytical support, if individual G and the laboratory agree in advance to a fee for such services.</li> <li>• If the laboratory does not offer patient-directed testing services and therefore states they cannot provide additional analytical support, it could refer the patient to the original ordering clinician and/or a clinical genetics service for consultation.</li> <li>• Laboratory is concerned the patient may not understand the potential for low-quality variant calls that could result in false-positive/negative data. Ideally, laboratory should have addressed this concern in PODD disclosures made when data from the earlier access request were delivered to individual G. If that was not done or if individual G disregarded the earlier PODD disclosures, laboratory may provide such warnings at the time individual G seeks interpretive support.</li> <li>• Laboratory is not required to, and may wish to avoid, recommending third-party interpretation services. Laboratory should emphasize the importance of working with CLIA-compliant laboratories if data are to be used to inform health planning.</li> </ul>
Individual H contacts the laboratory requesting access to their full DRS. Their test was completed 10 years prior.	<ul style="list-style-type: none"> <li>• Laboratory determines the individual’s data are still in storage and must comply with the request.</li> <li>• When delivering data to individual H, laboratory provides their standard PODD disclosure form and emphasizes the significant risks and limitations of using older variant data.</li> </ul>
Individual I stresses that they need the data to investigate new symptoms as soon as possible. They request a “STAT” record within 5 days.	<ul style="list-style-type: none"> <li>• Laboratory is not obligated to rush the release of information. They currently must comply to requests within 30 days, with the potential for one 30-day extension. The laboratory, at its discretion, can try to accommodate the timing request but is not required to do so.</li> <li>• Laboratory accompanies the data with a PODD disclosure form emphasizing the risks and limitations of genetic and genomic data in the DRS and displaying the Laboratory’s standard watermark stating that the data were provided strictly to comply with the HIPAA Privacy Rule and are not intended for clinical decision-making.</li> </ul>

### Points to consider

- It is not appropriate to interfere with individual decisions to request HIPAA access, but once an individual has requested data, it may be ethically appropriate to provide PODD disclosures, which are warnings and advisory statements made at the point when individuals receive the data they have requested.
- The appropriate PODD disclosures can vary depending on the specific types of data a laboratory stores, the

state(s) where the laboratory operates, and its institutional policies. Therefore, laboratories should consult with their IRBs, regulatory compliance officers, and general counsel’s offices when developing appropriate PODD disclosures to include when providing data in response to HIPAA access requests.

- Laboratories should consider including a clear statement that the data are being provided to comply with the Privacy Rule’s access right and the data (other

- than those that were included in the original test report) are not intended for clinical use and should not be so used.
- Laboratories should also consider explaining that HIPAA does not require laboratories to provide new or updated interpretation of genetics and genomics data in response to HIPAA access requests. The PODD disclosure form could prominently indicate the date on which testing was originally performed and make clear that the information provided was only current as of that date and may not reflect advances in testing technology and genomic interpretation.
  - Laboratories should consider noting that data provided in response to HIPAA access requests may include information that the individual has not originally been consented for, eg, if the individual, at the time of exome sequencing, declined receiving secondary findings that are part of the entire data set included in the DRS.
  - Laboratories should consider advising data recipients about potential benefits, limitations, and risks of the secondary use of the data without appropriate clinical consultation.
  - When providing data in electronic form, laboratories should consider inserting an indelible electronic “watermark” to warn clinicians with whom the patient shares the data that the information is not intended for use in clinical decision-making. Similar difficult-to-remove watermarks could be placed on information provided in paper form.
  - Reanalysis of genetic and genomic data should be performed at the original laboratory where the entire testing process has been validated. When this is not feasible, it is best to have another CLIA-compliant clinical laboratory perform the reanalysis, even if it may not be considered a fully validated clinical test if the entire process has not been previously validated. Laboratories should consider warning about the risks of misinterpretation because of secondary use of the data using third-party interpretation services, and they might encourage patients to consult with their clinician about whether reanalysis or retesting is a more appropriate way to address outstanding questions about heritable disease risk.
  - Laboratories may consider advising data recipients about the potential implications of genetic and genomic data for other family members.
  - Laboratories may also consider including a statement for adults requesting data on behalf of minors about the importance of eliciting and including the minor’s views when appropriate to respect their emerging autonomy and that parents should disclose the information in the DRS to their child, when appropriate, and transfer access and decision-making responsibility for such information when the child reaches an age of majority.

- Laboratories should consider including a statement about responsible data sharing for research and the potential privacy risks associated with sharing.

## Role for clinicians

### Role of clinical genetic and genomic professionals

Requesting and receiving genetic and genomic data from the DRS is, at its core, a transaction between individuals and laboratories. Laboratories cannot delay or deny DRS access based on the laboratory’s perception that genetic counseling should be provided. In this narrow view, clinical geneticists and/or genetic counselors are not integral to this exchange and have no explicit role as gatekeepers to limit access to information in the DRS. However, individuals sometimes, of their own accord, seek assistance when contemplating a HIPAA access request and clinical geneticists and/or genetic counselors are encouraged to educate and guide individuals in ways that will leverage the benefits and minimize the potential harms of a request. The genetic and genomic information being requested typically exists at the laboratory because of a prior clinical evaluation resulting in genetic testing, and individuals would often have received pretest and post-test counseling and results disclosure. Given these previously established relationships, clinical geneticists and/or genetic counselors may consequently serve as a resource for information-seeking individuals considering a HIPAA access request and can help guide downstream uses and explore alternatives. For instance, some clinical questions might be more appropriately addressed by new genetic and genomic testing, which is often more expansive and/or updated to be more inclusive than the previous testing.

As scientific knowledge grows and bioinformatic software improves, the ability to use data effectively expands. Having access to genetic and genomic data in a DRS enables reanalysis of the data, which in certain cases could help limit duplicative, labor-intensive, and/or expensive retesting. Clinical geneticists and genetic counselors may recommend reanalysis of genetic and genomic data rather than a HIPAA access request if appropriate. Periodic reanalysis of the data, typically every 1 to 2 years, may enhance the diagnostic yield.<sup>61-63</sup> In addition, clinical geneticists and genetic counselors may sometimes recommend a limited HIPAA access request seeking only the information of highest relevance or interest to the clinical scenario. For example, if an individual is seeking an answer to a specific clinical question, a request could be crafted to target the relevant information only, rather than requesting the entire DRS. This targeted approach can help maximize utility and address an immediate clinical question while minimizing potential harms.

It is also important to note that individuals may also seek out a clinical geneticist or genetic counselor after receiving data from a HIPAA access request. Therefore, clinical geneticists and genetic counselors should understand the

potential benefits and limitations of these data to potentially counsel individuals as well.

In addition, clinical genetic and genomic professionals should be aware that other health care professionals may also be approached with questions about data that individuals receive through HIPAA access requests. Clinical genetic and genomic professionals should, wherever possible, serve as a resource for their colleagues and consider providing proactive guidance.

### Points to consider

- When individuals seek advice about whether to make a HIPAA access request, it is permissible for clinical geneticists and genetic counselors to serve as a resource to help explain the potential benefits and limitations of genetic and genomic data in a DRS.
- HHS emphasizes that covered entities “may not require an individual to provide a reason for requesting access. Further, the individual’s rationale for requesting access, if voluntarily disclosed, is not a permitted reason to deny access.”<sup>3</sup> When individuals seek help, however, providing factual information in response to their requests is consistent with this directive.
- When individuals voluntarily seek help in deciding whether to make a HIPAA access request, clinical geneticists and genetic counselors can assist in evaluating options, which may include recommending reanalysis or new testing and providing pretest and post-test counseling as appropriate.
- When individuals seek help in defining the scope of a HIPAA access request, clinical geneticists and genetic counselors can recommend specific, targeted DRS requests, to obtain only the information of highest interest to the clinical scenario.
- Other health care professionals may also be approached by individuals about HIPAA access requests or data received through such requests. Clinical geneticists and genetic counselors can be a valuable resource to these other health care professionals responding to these queries.

### Summary

The right to access one’s genetic and genomic data generated by HIPAA-covered laboratories is a civil right safeguarded by federal privacy law, but it exists in tension with concerns about possible harms from misunderstanding or misuse of data. Further research is needed to determine best practices for presenting data in response to patients’ HIPAA access requests. Owing to the complex nature of genetic and genomic data, great care is needed to limit the potential for misunderstanding or misuse of the information laboratories are required to provide in response to HIPAA access requests. Interfering with access is not permissible but much can be done to make access safer by ensuring good

communication at the PODD when patients receive the data they requested under HIPAA’s access right. HIPAA-covered laboratories should consider developing PODD disclosures that would routinely be supplied at the time they respond to an access request. Furthermore, genetic and genomic professionals should lead future research efforts to study options that maximize the benefits and minimize potential harms of HIPAA access requests to help create future best practice guidelines.

### Acknowledgments

The authors would like to thank Sandor Roberts for his administrative support. In addition, the authors would like to thank Elizabeth Lorbeer, Library Director and Medical Library Department Chair at Western Michigan University Homer Stryker M.D. School of Medicine, for her assistance with obtaining several references used in the preparation of this manuscript.

M.K.T. was an associate professor in the Division of Pediatric Genetics, Department of Pediatrics, Metabolism & Genomic Medicine at the University of Michigan and a member of the ACMG Laboratory Quality Assurance Committee during the preparation of this document. S.J.H. was a resident in the Division of Medical Genetics at the University of Washington School of Medicine during the preparation of this document.

### Conflict of Interest

Funding and support listed in this section did not support the development of this document unless included in the acknowledgments section. M.K.T., M.C., P.R.G., and A.R.S. all serve as directors in clinical laboratories that perform a breadth of genetic and genomic analyses on a fee-for-service basis. D.R.S. is supported by the Intramural Research Program of the Division of Cancer Epidemiology and Genetics of the National Cancer Institute, Rockville, MD, and also performs contract clinical telehealth services for Genome Medical, Inc in accordance with relevant National Cancer Institute ethics policies. All other authors declare no conflicts of interest.

### Authors

Marwan K. Tayeh<sup>1</sup>, Margaret Chen<sup>2,3</sup>, Stephanie M. Fullerton<sup>4,5</sup>, Patrick R. Gonzales<sup>6</sup>, Samuel J. Huang<sup>7</sup>, Lauren J. Massingham<sup>8,9</sup>, Julianne M. O’Daniel<sup>10</sup>, Douglas R. Stewart<sup>11</sup>, Ashlee R. Stiles<sup>12</sup>, Barbara J. Evans<sup>13,14</sup>; on behalf of the ACMG Laboratory Quality Assurance Committee and the ACMG Social, Ethical and Legal Issues Committee<sup>15,\*</sup>



## Affiliations

<sup>1</sup>Indiana University School of Medicine, Indianapolis, IN; <sup>2</sup>Western Michigan University Homer Stryker M.D. School of Medicine, Kalamazoo, MI; <sup>3</sup>GeneDx, Gaithersburg, MD; <sup>4</sup>Division of Medical Genetics, Department of Medicine, University of Washington School of Medicine, Seattle, WA; <sup>5</sup>Department of Bioethics & Humanities, University of Washington School of Medicine, Seattle, WA; <sup>6</sup>Department of Pathology and Laboratory Medicine, University of Kansas Medical Center, Lenexa, KS; <sup>7</sup>Division of Medical Genetics, Marshfield Clinic, Marshfield, WI; <sup>8</sup>Division of Medical Genetics, Department of Pediatrics, Hasbro Children's Hospital, Providence, RI; <sup>9</sup>The Warren Alpert School of Medicine at Brown University, Providence, RI; <sup>10</sup>Department of Genetics, University of North Carolina at Chapel Hill, Chapel Hill, NC; <sup>11</sup>Clinical Genetics Branch, Division of Cancer Epidemiology and Genetics, National Cancer Institute, Rockville, MD; <sup>12</sup>Division of Medical Genetics, Department of Pediatrics, Duke University Medical Center, Durham, NC; <sup>13</sup>Levin College of Law, University of Florida, Gainesville, FL; <sup>14</sup>Herbert Wertheim College of Engineering, University of Florida, Gainesville, FL; <sup>15</sup>American College of Medical Genetics and Genomics, Bethesda, MD

## References

- Health Insurance Portability and Accountability Act of 1996. HR 3103, 104th Cong (1996). Pub L No. 104-191. Accessed June 3, 2022. <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>
- 45 CFR pts. 160, 164 (Privacy Rule), id. at § 164.501 (Definitions).
- United States Department of Health & Human Services. Individuals' right under HIPAA to access their health information 45 CFR § 164.524. Update January 31, 2020. Accessed June 3, 2022. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>
- United States Department of Health & Human Services. The HIPAA Privacy Rule. United States Department of Health & Human Services. Updated March 31, 2022. Accessed May 18, 2022. <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>
- Health Insurance Portability and Accountability Act of 1996 § 264(a)-(c), 110 Stat. 1936, 2033. HR 3103, 104th Cong (1996). Pub L No. 104-191. Accessed March 1, 2022. <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>
- 45 CFR § 160.103. Definitions.
- Evans BJ, Dorschner MO, Burke W, Jarvik GP. Regulatory changes raise troubling questions for genomic testing. *Genet Med*. 2014;16(11):799-803. <http://doi.org/10.1038/gim.2014.127>
- 45 CFR § 164.512(i). Uses and disclosures for which an authorization or opportunity to agree or object is not required.
- Centers for Medicare & Medicaid Services. Are you a covered entity? Centers for Medicare & Medicaid Services. Update May 11, 2022. Accessed June 3, 2022. <https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity>
- Clinical laboratory improvement amendments of 1988. HR 5471, 100th Cong (1988). Pub L No. 100-578. Accessed June 3, 2022. <https://www.govinfo.gov/content/pkg/STATUTE-102/pdf/STATUTE-102-Pg2903.pdf>
- 42 CFR 493. Laboratory requirements.
- Centers for Medicare & Medicaid Services. Centers for Disease Control and Prevention, Office for Civil Rights, United States Department of Health and Human Services. CLIA program and HIPAA privacy rule; patients' access to test reports. *Fed Regist*. 2014;79(25):7290-7316.
- New York State Department of Health. Cytogenetics. Accessed May 18, 2022. <https://www.wadsworth.org/sites/default/files/WebDoc/Cytogenetics%20-%20Effective%20August%202020.pdf>
- Centers for Disease Control and Prevention (CDC). Good laboratory practices for biochemical genetic testing and newborn screening for inherited metabolic disorders. *MMWR Recomm Rep*. 2012;61(RR-2):1-44.
- 45 CFR § 164.501. Definitions.
- United States Department of Health and Human Services. Standards for privacy of individually identifiable health information. Office of the Assistant Secretary for Planning and Evaluation, DHHS. Final rule. *Fed Regist*. 2000;65(250):82461-82829.
- United States Department of Health & Human Services. FAQ Guidance No. 2049, Does an individual have a right under HIPAA to access more than just test results from a clinical laboratory? Updated June 24, 2016. Accessed March 1, 2022. <https://www.hhs.gov/hipaa/for-professionals/faq/2049/does-an-individual-have-a-right-under/index.html>
- 45 CFR § 164.514(b)(1),(2).
- Evans BJ. The Genetic Information Nondiscrimination Act at age 10: GINA's controversial assertion that data transparency protects privacy and civil rights. *William Mary Law Rev*. 2019;60(6):2017-2109.
- 45 CFR 164.524(e)(1). Implementation specification: Documentation.
- 45 CFR 164.530(j).
- 45 CFR § 164.524(c)(iii). Access of individuals to protected health information. Implementation specifications: Provision of access.
- 45 CFR § 164.524(b)(2). Access of individuals to protected health information. Implementation specifications: Requests for access and timely action. Timely action by the covered entity.
- United States Department of Health and Human Services. Proposed modifications to the HIPAA privacy rule to support, and remove barriers to, coordinated care and individual engagement. *Fed Regist*. 2021;86(12):6446-6538.
- 45 CFR § 164.524(a)(1)-(3). Access of individuals to protected health information.
- United States Department of Health and Human Services. Standards for privacy of individually identifiable health information. Office of the Assistant Secretary for Planning and Evaluation, DHHS. Proposed rule. *Fed Regist*. 1999;64(212):59918-60065.
- 45 CFR § 164.524(d)(1). Access of individuals to protected health information. Implementation specifications: Denial of access. Making other information accessible.
- 45 CFR § 164.524(a)(1)(i),(ii), (a)(2)(ii). Access of individuals to protected health information. Right of access.
- 45 CFR § 164.524(a)(2)(iv),(v). Access of individuals to protected health information. Unreviewable grounds for denial.
- 45 CFR § 164.524(a)(3)(i). Access of individuals to protected health information. Reviewable grounds for denial.
- 45 CFR § 164.524(a)(4),(d)(4). Access of individuals to protected health information. Review of a denial of access.
- McGraw D. Return of genetic results in the All of Us research program. March 7, 2017. Accessed March 1, 2022. <https://videocast.nih.gov/summary.asp?Live=21887&bhcp=1>
- Lye CT, Forman HP, Gao R, et al. Assessment of US hospital compliance with regulations for patients' requests for medical records. *JAMA Netw Open*. 2018;1(6):e183014. <http://doi.org/10.1001/jama-networkopen.2018.3014>
- ACLU. Our genes, our data: patients' right to access their own genetic information. ACLU. Published May 18, 2016. Accessed March 1, 2022. <https://www.aclu.org/cases/our-genes-our-data-patients-right-access-their-own-genetic-information>
- Sebelius v Uplift Medical, P.C. et al. RWT 11cv2168 Author-Anonymous, (2012). Accessed June 3, 2022. [https://www.govinfo.gov/content/pkg/USCOURTS-mdd-8\\_11-cv-02168/pdf/USCOURTS-mdd-8\\_11-cv-02168-0.pdf](https://www.govinfo.gov/content/pkg/USCOURTS-mdd-8_11-cv-02168/pdf/USCOURTS-mdd-8_11-cv-02168-0.pdf)
- McGowan K. The man who dissected his own brain. *WIRED*. Published February 11, 2016. Accessed March 1, 2022. <https://www.wired.com/2016/02/the-man-who-dissected-his-own-brain/>

37. Lohr S. The healing power of your own medical records. *The New York Times*. Published March 31, 2015. Accessed March 1, 2022. <https://www.nytimes.com/2015/04/01/technology/the-healing-power-of-your-own-medical-data.html>
38. 45 CFR § 164.524(a)(3)(iii). Access of individuals to protected health information. Standard: Access to protected health information. Reviewable grounds for denial.
39. 45 CFR § 164.512(i). Uses and disclosures for which an authorization or opportunity to agree or object is not required.
40. 45 CFR § 160.202. Definitions.
41. 45 CFR § 164.524(c)(1). Access of individuals to protected health information. Implementation specifications: Provision of access. Providing the access requested.
42. 45 CFR § 164.524(d)(4). Access of individuals to protected health information. Implementation specifications: Denial of access. Review of denial requested.
43. 45 CFR § 164.524(c)(2)(i).
44. 45 CFR § 164.524(c)(2)(ii).
45. 45 CFR § 164.524(c)(4). Fees.
46. Evans BJ. HIPAA's individual right of access to genomic data: reconciling safety and civil rights. *Am J Hum Genet*. 2018;102(1):5-10. <http://doi.org/10.1016/j.ajhg.2017.12.004>
47. National Academies of Sciences, Engineering, and Medicine. *Returning Individual Research Results to Participants: Guidance for a New Research Paradigm*. The National Academies Press; 2018.
48. Grebe TA, Khushf G, Chen M, et al. The interface of genomic information with the electronic health record: a points to consider statement of the American College of Medical Genetics and Genomics (ACMG). *Genet Med*. 2020;22(9):1431-1436. <http://doi.org/10.1038/s41436-020-0841-2>
49. Tandy-Connor S, Guiltinan J, Krempely K, et al. False-positive results released by direct-to-consumer genetic tests highlight the importance of clinical confirmation testing for appropriate patient care. *Genet Med*. 2018;20(12):1515-1521. <http://doi.org/10.1038/gim.2018.38>
50. Rehder C, Bean LJH, Bick D, et al. Next-generation sequencing for constitutional variants in the clinical laboratory, 2021 revision: a technical standard of the American College of Medical Genetics and Genomics (ACMG). *Genet Med*. 2021;23(8):1399-1415. <http://doi.org/10.1038/s41436-021-01139-4>
51. Aziz N, Zhao Q, Bry L, et al. College of American Pathologists' laboratory standards for next-generation sequencing clinical tests. *Arch Pathol Lab Med*. 2015;139(4):481-493. <http://doi.org/10.5858/arpa.2014-0250-CP>
52. 21 U.S.C. Sec. 321(h)(1)(B). Definitions; generally.
53. 42 U.S.C. Sec. 263a(a). Certification of laboratories. "Laboratory" or "clinical laboratory" defined.
54. Bennett C. Ambiguous genetic test results can be unsettling. Worse, they can lead to needless surgeries. *The Washington Post*. Published February 7, 2021. Accessed March 1, 2022. [https://www.washingtonpost.com/health/genetic-tests-uncertain-results/2021/02/05/80a06d9a-65a2-11eb-8468-21bc48f07fe5\\_story.html](https://www.washingtonpost.com/health/genetic-tests-uncertain-results/2021/02/05/80a06d9a-65a2-11eb-8468-21bc48f07fe5_story.html)
55. Welsh JL, Hoskin TL, Day CN, et al. Clinical decision-making in patients with variant of uncertain significance in BRCA1 or BRCA2 genes. *Ann Surg Oncol*. 2017;24(10):3067-3072. <http://doi.org/10.1245/s10434-017-5959-3>
56. Claustres M, Kozich V, Dequeker E, et al. Recommendations for reporting results of diagnostic genetic testing (biochemical, cytogenetic and molecular genetic). *Eur J Hum Genet*. 2014;22(2):160-170. <http://doi.org/10.1038/ejhg.2013.125>
57. Eno C, Bayrak-Toydemir P, Bean L, et al. Misattributed parentage as an unanticipated finding during exome/genome sequencing: current clinical laboratory practices and an opportunity for standardization. *Genet Med*. 2019;21(4):861-866. <http://doi.org/10.1038/s41436-018-0265-4>
58. Botkin JR, Belmont JW, Berg JS, et al. Points to consider: ethical, legal, and psychosocial implications of genetic testing in children and adolescents. *Am J Hum Genet*. 2015;97(1):6-21. <http://doi.org/10.1016/j.ajhg.2015.05.022>
59. Chad L, Szego MJ. Please give me a copy of my child's raw genomic data. *NPJ Genom Med*. 2021;6(1):15. <http://doi.org/10.1038/s41525-021-00175-y>
60. Elger B, Michaud K, Mangin P. When information can save lives: the duty to warn relatives about sudden cardiac death and environmental risks. *Hastings Cent Rep*. 2010;40(3):39-45. <http://doi.org/10.1353/hcr.0.0254>
61. Liu P, Meng L, Normand EA, et al. Reanalysis of clinical exome sequencing data. *N Engl J Med*. 2019;380(25):2478-2480. <http://doi.org/10.1056/NEJMc1812033>
62. Sun Y, Xiang J, Liu Y, et al. Increased diagnostic yield by reanalysis of data from a hearing loss gene panel. *BMC Med Genomics*. 2019;12(1):76. <http://doi.org/10.1186/s12920-019-0531-6>
63. Costain G, Jobling R, Walker S, et al. Periodic reanalysis of whole-genome sequencing data enhances the diagnostic advantage over standard clinical genetic testing. *Eur J Hum Genet*. 2018;26(5):740-744. <http://doi.org/10.1038/s41431-018-0114-6>