COMMENT | Genetics inMedicine

Open

Genomic databases, subpoenas, and Certificates of Confidentiality

Leslie E. Wolf, JD, MPH[1] and Laura M. Beskow, PhD, MPH[2]

Genetics in Medicine (2019) 21:2681–2682; https://doi.org/10.1038/s41436-019-0592-0

The arrest of the Golden State Killer focused attention on law enforcement use of nonforensic DNA databases, a technique that has since been used to apprehend suspects in other unsolved cases.[1,2] Although none of these cases involved a research database, it is not difficult to imagine the utility of such resources for law enforcement purposes. While few can dispute the public benefit of identifying perpetrators of violent crimes, this prospect raises questions regarding the adequacy of protections afforded DNA collected for research purposes. These concerns have particular relevance to large-scale endeavors, such as the National Institutes of Health's (NIH) All of Us Research Program or the Million Veterans Program, both of which seek to recruit 1 million participants who will share their DNA and a substantial depth and breadth of other information to aid scientific discovery.

In the wake of the Golden State Killer's arrest, NIH provided reassurance about the confidentiality of All of Us data, noting that "the information is off limits to subpoenas and search warrants via 'certificates of confidentiality'."[2,3] Based on our research on Certificates and our evaluation of the 21st Century Cures Act amendments to them, the situation is not quite so clear.[4,5]

Certificates are federal legal tools that allows researchers who hold them to resist compelled disclosure of identifiable research data "in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings."[4] They were originally authorized in 1970 as part of the war on drugs, but have been expanded over time to apply to a broader range of research, including genomic research. Prior to the passage of the 21st Century Cures Act, researchers had to apply for a Certificate; now, NIH automatically issues a Certificate for any study it funds involving identifiable data.

Our research on Certificates indicated that, although they generally seem to work as intended, there is a paucity of legal cases establishing their effectiveness. Even when a Certificate has been obtained, attorneys and courts often rely on other justifications for protecting research data or are able to resolve the demand through disclosure of de-identified data. However, other cases have been resolved—whether by party agreement or court order—through the production of information that should have been protected, accompanied by restrictions on access and use.[6]

The 21st Century Cures Act implements some significant positive changes to Certificates' protections.[4] Voluntary disclosures are no longer permitted. The protections extend to any data that are identifiable, a term that is now explicitly defined and includes "a very small risk" of re-identification. These protections apply to any copies of the data, as well as biospecimens, that may be shared with other researchers. If protected data are disclosed, they cannot be admitted in a legal proceeding. For example, if information about a research participant's illegal drug use were inadvertently disclosed, that information could not be used in a criminal case against him.

Nevertheless, the changes to Certificates are not uniformly positive. Under the 21st Century Cures Act, disclosure "as required by Federal, State, or local laws," except for those pertaining to use in legal proceedings, is now explicitly permitted. NIH restricts its discussion of this provision to complying with mandatory public health reporting. However, the language of this provision is not so limited and, given the wide universe of laws encompassed by the provision and substantial variation in state laws, it is difficult to predict the extent of required disclosures that might fall under it. Once research information is disclosed, it seems likely that the Certificate's protections would no longer apply. That is, the disclosed data would be integrated it into the recipient's records and confidentiality maintained according to applicable laws. For example, public health authorities who receive infectious disease information from researchers will treat it the same as information received from other sources. Thus, there will be confidentiality protections, but also, commonly, exceptions to those obligations that often include law enforcement.[7] The impact of restriction on admissibility in court may be limited in practice. As critical as the genealogy databases were to solving the Golden State Killer and other such cases, they only identify a potential suspect. To make the

[1]Center for Law, Health & Society, Georgia State University College of Law, Atlanta, GA, USA; [2]Center for Biomedical Ethics and Society, Vanderbilt University Medical Center, Nashville, TN, USA. Correspondence: Leslie E. Wolf (lwolf@gsu.edu)

Submitted 8 April 2019; accepted: 13 June 2019
Published online: 26 June 2019

case, law enforcement must collect the suspect's DNA (typically surreptitiously) to compare it with crime scene DNA, and it is these results that will be introduced in court.

The provision permitting disclosure as required by law is not the only potential threat to a Certificate's protections. NIH's automatic issuance of Certificates will extend protections to a larger number of studies. But given our earlier research demonstrating important knowledge gaps about Certificates,[5] without significant educational efforts, institutions and researchers may not even know the protections exist and therefore not assert them if data are subpoenaed. The risks may be exacerbated for multisite studies, as sites may vary in their understanding of and experience with Certificates. It is incumbent on study leadership to make participating sites aware of the Certificate's protections and the obligations it imposes to refuse attempts to compel disclosure. Moreover, there are many DNA research repositories that do not have a Certificate; for example, repositories that are not federally funded and have not applied for one. Nonresearch databases, like the genealogy databases used in the Golden State Killer case, are not eligible for a Certificate, which protects only research data.

In sum, the revised Certificate provides important protections for research participants who share their genomic and other sensitive information in federally funded research. But it is also important to recognize the limits to those protections, as well as some uncertainties introduced by the new provisions, so as not to overly reassure participants as to the confidentiality of their data.

ACKNOWLEDGEMENTS

This work was supported in part by a grant from the National Human Genome Research Institute (NHGRI) (R01-HG-007733, principal investigator: L.M.B.). The content is solely the responsibility of the authors and does not necessarily represent the official views of NHGRI or NIH.

DISCLOSURE

The authors declare no conflicts of interest.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

1. Fuller T. How a Genealogy Site Led to the Front Door of the Goldent State Killer Suspect. 26 April 2018. The New York Times. https://www.nytimes.com/2018/04/26/us/golden-state-killer.html. Accessed 24 June 2019.
2. Ram N, Guerrini CJ, McGuire AL. Genealogy databases and the future of criminal investigation. Science. 2018;360:1078–1079.
3. Bernstein L. NIH seeks health data of 1 million people, with genetic privacy suddenly an issue. 1 May 2018. The Washington Post. https://www.washingtonpost.com/national/health-science/nih-seeks-health-data-of-1-million-people-with-genetic-privacy-suddenly-an-issue/2018/05/01/cb38a588-4d4b-11e8-b725-92c89fe3ca4c_story.html. Accessed 24 June 2019.
4. Wolf LE, Beskow LM. New and improved?: 21st Century Cures Act revisions to Certificates of Confidentiality. Am J Law Med. 2018;44:343–358.
5. Wolf LE, et al. Certificates of Confidentiality: protecting human subject research data in law and practice. J Law Med Ethics. 2015;43:594–609.
6. Beskow LM, Dame L, Costello E. Research ethics. Certificates of Confidentiality and compelled disclosure of data. Science. 2008;322:1054–1055.
7. Gostin LO, Hodge JG Jr., Burghardt MS. Balancing communal goods and personal privacy under a National Health Informational Privacy Rule. St. Louis Univ Law J. 2002;46:5–35.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, and provide a link to the Creative Commons license. You do not have permission under this license to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2019