Published in final edited form as:

Am J Law Med. 2018 May ; 44(2-3): 343–358. doi:10.1177/0098858818789431.

New and Improved? 21st Century Cures Act Revisions to Certificates of Confidentiality

Leslie E. Wolf, JD, MPH and

Georgia State University College of Law and School of Public Health, lwolf@gsu.edu

Laura M. Beskow, MPH, PhD

Vanderbilt Center for Biomedical Ethics & Society, Department of Health Policy, Vanderbilt University, laura.m.beskow@vanderbilt.edu

Certificates of Confidentiality are a federal legal tool designed to protect sensitive, identifiable research data from compelled disclosure. Congress first authorized their use in 1970 to facilitate research on illegal drug use. The scope of their use was later expanded to cover mental health research and then again to apply broadly to identifiable, sensitive research data, regardless of topic. Certificates can be critical to enabling conduct of essential research on sensitive topics, such as effective interventions to curb the opioid epidemic or reduce HIV transmission among minority youth. Nevertheless, there have been criticisms about Certificates and their use on several grounds. For example, researchers and institutional review boards (IRBs) may lack sufficient knowledge about them and, therefore, may not consider using them in studies for which they would be appropriate. In contrast to other protections, such as Department of Justice Privacy Certificates, Certificate protections were not automatically extended, but required an application. In addition, the concept of identifiable data had not kept up with technological changes that may allow for reidentification of data previously considered unidentifiable. Although a researcher who obtained a Certificate could use it to resist a legal demand for identifiable data, little was known about the actual effectiveness of the protection provided.

The 21st Century Cures Act substantially revises the Certificate authorizing statute, and many of the changes are directly responsive to the criticisms that have been raised. Significantly, the Secretary of the Department of Health and Human Services (HHS) must issue Certificate protection to federally funded research involving identifiable, sensitive research data, and the National Institutes of Health (NIH) will automatically include such protections to research it funds. Non-federally funded researchers can continue to apply for Certificate protection. The definition of identifiable has been expanded to include data “for which there is at least a very small risk” of identification. Certificates will now not only protect against compelled disclosure, but also render protected data inadmissible in legal proceedings without participant consent. In addition, voluntary disclosure is no longer authorized, but there is now a broad exception for disclosure as required by federal, state, and local laws. In this paper, based on our previous research on Certificates, we critically evaluate the 21st Century Cures Act’s Certificate revisions and their positive and negative

impact on the dual goals of facilitating important, sensitive research while maximally protecting individual research participants.

Background

Congress originally authorized what has become known as the Certificate of Confidentiality in 1970 for research involving drug use.¹ Part of a larger effort to reform federal laws regarding drug use and control, the Certificate authorization represents congressional recognition of the importance of research toward finding effective treatments and the challenges of conducting such research given its focus on an illegal activity.² Individuals rightly may be reluctant to participate in research if doing so placed them at legal jeopardy. Accordingly, some additional protections were viewed as necessary to facilitating the conduct of such research.³ The statute allowed the Secretary of the Department of Health, Education and Welfare (now HHS):

“[to] authorize persons engaged in research on the use and effect of drugs to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals.”⁴

The original authorizing statute had been amended several times before the 21st Century Cures Act Amendments.⁵ These prior changes expanded the scope of research eligible for the protections. The first amendment added research on mental and alcohol use to the drug use of the original statute.⁶ The next amendment considerably broadened the range of eligible research to “biomedical, behavioral, clinical, or other research.”⁷ Although there were some minor changes to the wording, the protections remained essentially the same as in the original authorizing statute.⁸

Unlike the previous amendments in the Certificates 46-year history—which mainly focused on the scope of the research eligible for the protections—the 21st Century Cures Act

¹Comprehensive Drug Abuse Prevention and Control Act of 1970, Pub. L. No. 91-513, sec. 3(a), § 303(a), 84 Stat. 1236, 1241 (codified at 42 U.S.C. § 242a(a) (1970)) (current version at 42 U.S.C. § 241(d) (2016)).

²For a discussion of the history of the Comprehensive Drug Abuse Prevention and Control Act, see Leslie E. Wolf et al., *Certificates of Confidentiality: Protecting Human Subject Research Data in Law and Practice*, 14 MINN. J.L. SCI. & TECH. 11, 20-25 (2013).

³Id.

⁴Comprehensive Drug Abuse Prevention and Control Act, sec. 3(a).

⁵For a discussion of the history of the Comprehensive Drug Abuse Prevention and Control Act, see Wolf et al., *supra* note 2, at 24-25.

⁶Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act Amendments of 1974, Pub. L. No. 93-282, sec. 122(b), § 303(a), 88 Stat. 125, 132-33 (codified at 42 U.S.C. § 242a(a) (1974)) (current version at 42 U.S.C. § 241(d) (2016)).

⁷Health Omnibus Programs Extension of 1988, Pub. L. No. 100-607, sec. 163, § 303(a), 102 Stat. 3048, 3062 (codified at 42 U.S.C. § 241(d) (1988)). This Act redesignated section 303(a) of the Public Health Service Act to section 301(d), moving the Certificate authority from 42 U.S.C. § 242a(a) to 42 U.S.C. § 241(d); see Wolf, *supra* note 2, at 24.

⁸The language, which was in effect from 1988 to 2015, read “[t]he Secretary [of Health and Human Services] may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, including research on the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals.” 42 U.S.C. §§ 201(c), 241(d) (2015).

implements several significant substantive and procedural changes.⁹ These changes, which are described in more detail in our analysis of them, are as follows:

- The Secretary's authority to issue Certificates is now mandatory for qualified research that is funded wholly or in part by the Federal government. It remains discretionary for non-federally funded research.¹⁰
 - Relatedly, and consistent with the statute's mandate to "minimize the burden to researchers, streamline the process, and reduce the time it takes to comply with the requirements of this subsection,"¹¹ NIH will now consider a Certificate automatically issued for all research it funds that involves identifiable information.¹²
- The disclosure prohibition applies to "any information, document, or biospecimen" that contains identifiable, sensitive information that "was created or compiled for purposes of the research."¹³
- "Identifiable, sensitive information" is now explicitly defined and includes information
- "(A) through which an individual is identified; or (B) for which there is at least a very small risk, as determined by current scientific practice or statistical methods, that some combination of the information, a request for information, and other available data sources could be used to deduce the identity of an individual."¹⁴
- Notice that the definition focuses solely on identifiability, rather than sensitivity.¹⁵
- The disclosure prohibition now has new exceptions for disclosures or uses "required by Federal, State, or local laws" but, importantly, this does not include laws permitting compelled disclosure in legal proceedings, medical treatment

⁹21st Century Cures Act, Pub. L. 114-255, sec. 2012, § 301, 130 Stat. 1033, 1049-50 (2016) (codified at 42 U.S.C. § 241(d) (2016)).

¹⁰*Id.* § 241(d)(1)(A).

¹¹*Id.* § 241(d)(1)(G).

¹²NATIONAL INSTITUTES OF HEALTH, NOT-OD-17-109, NOTICE OF CHANGES TO NIH POLICY FOR ISSUING CERTIFICATES OF CONFIDENTIALITY (2017), <https://grants.nih.gov/grants/guide/notice-files/NOT-OD-17-109.html> [<https://perma.cc/GHX4-BFXC>] (effective October 1, 2017) (explaining NIH will provide Certificates automatically to any NIH-funded research in which identifiable information is collected).

¹³42 U.S.C. § 241(d)(1)(B).

¹⁴*Id.* § 241(d)(4). The previous statute referred only to withholding "names or other identifying characteristics," without defining "identifying characteristics." *Id.* § 241(a). The regulations defined "identifying characteristics" as "the name, address, any identifying number, fingerprints, voiceprints, photographs or any other item or combination of data about a research subject which could reasonably lead directly or indirectly by reference to other information to identification of that research subject." 42 C.F.R. § 2a.2(g) (2011). However, the regulation did not include the "very small" risk of reidentification now included in the statute. Moreover, NIH indicates these regulations now only apply to non-federally-funded research and "only to the extent that the regulations do not conflict with the amended statute." *Frequently Asked Questions (FAQ), Certificates of Confidentiality (CoC) Kiosk*, NAT'L INSTS. HEALTH, <https://humansubjects.nih.gov/coc/faqs> [<https://perma.cc/RG7H-QG9N>] [hereinafter *FAQs*].

¹⁵The NIH emphasizes this point, noting that "[t]he new statute that governs Certificates of Confidentiality broadened the meaning of sensitive, identifiable information and focuses more directly on identifiability. Identifiable, sensitive information is considered to be information about an individual, gathered or used during the course of biomedical, behavioral, clinical or other research, through which the individual is identified, or there is at least a very small risk that some combination of the information, a request for the information, and other available data sources could be used to determine the identity of the individual. The CoC defines this as 'covered information.' Identifiable, sensitive information includes but is not limited to name, address, social security or other identifying number, and fingerprints, voiceprints, photographs, genetic information, tissue samples, or data fields that when used in combination with other information may lead to identification of an individual." *FAQs*, *supra* note 14.

with individual consent, and “for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.”¹⁶ Participants’ consent to disclose for any purpose remains a permissible exception.

- Identifiable information protected by a Certificate is now “immune from the legal process, and shall not, without the consent of the individual to whom the information pertains, be admissible as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceeding.”¹⁷
- The protections afforded to the information now explicitly apply to all copies of identifiable, sensitive information collected for the purposes of research in perpetuity.¹⁸

Summary Key Changes to Certificates¹⁹

Issue	Previous Statute	Revised Statute
How to get one	Issued upon approval of application	Federally-funded – mandatory issue upon application NIH-funded – <i>automatically issued upon award</i> Non-NIH-funded – upon approval of application
Disclosure	PI/Institution could voluntarily disclose	Disclosure is prohibited unless within a statutory exception including with participant consent
Admissibility	Information protected by a Certificate could be used in a legal proceeding if disclosed	Protected information cannot be used in a legal proceeding even if it is disclosed elsewhere
Copies	Unclear; typically advised to amend or extend	All information, including copies is protected

These changes build on what has been the core protection afforded by Certificates since their inception – imposing an obligation to protect the confidentiality of identifiable information and authorizing researchers to avoid compelled disclosure in virtually every type of legal proceeding.²⁰ In the next section, we critically examine each of the changes and their implications for Certificates’ use and protections.

Analysis

Substantive and Procedural Changes to the Certificate Provisions

Mandatory issuance for federally-funded research and automatic issuance for NIH-funded research.—Under the previous statute, the Secretary of Health and Human Services “*may*” grant the protections to qualified researchers,²¹ whereas under the 21st Century Cures Act, the Secretary “*shall*” issue a certificate of confidentiality ... if the research is funded wholly or in part by the Federal Government” (emphasis added).²² The

¹⁶42 U.S.C. § 241(d)(1)(C).

¹⁷*Id.* § 241(d)(1)(E).

¹⁸*Id.* § 241(d)(1)(F). Although NIH guidance stated that the Certificates protections continued without end, this was not previously included in the statutory authority.

¹⁹Elonna Ekweani et al., NIH, Address at the Public Responsibility in Medicine and Research, 2017 Advancing Ethical Research Conference: Certificates of Confidentiality (CoC): When, Why and So What? (Nov. 8, 2017) (on file with the author).

²⁰*See* 42 U.S.C. § 241(d)(1)(D). This protection is further supported by the addition of language specifying that “Identifiable, sensitive information protected [by a Certificate], and all copies thereof, shall be immune from legal process.” *Id.* § 241(d)(1)(E).

²¹*Id.* § 241(d).

²²*Id.* § 241(d)(1)(A)(i).

authority remains permissive, upon application, for research that is not federally funded.²³ This mandatory language for federally-funded research may expand the type of research to which the protections attach. Historically, NIH has not issued Certificates for research that does not “fall within the NIH mission,”²⁴ an option that no longer seems permissible for federally-funded research.²⁵

This change also appears to address criticisms that have been leveled against the previous Certificate authority because it relied on investigators to elect to or IRBs to require or recommend that investigators apply for the protection.²⁶ This approach may have resulted in inconsistent protections among studies that posed similar risks because investigators and IRBs were unaware of Certificates or their appropriateness for particular studies. In this way, Certificate have been unfavorably compared to the more encompassing protections afforded by other agencies, such as the Department of Justice, as well as some state laws.²⁷

The previous approach was also criticized for the burdens of the application process and the potential for delays in protection.²⁸ The NIH’s new approach to Certificates for research it funds addresses both of these criticisms. Research involving identifiable data will automatically receive Certificate protections upon award. For other federally-funded research, the protection is guaranteed, in that the Secretary “shall issue” a Certificate for research involving identifiable data. Moreover, the application process for non-NIH funded research should be streamlined because the issuance is mandatory.

The benefits of this change may not be fully realized. For example, if federal funding for a particular project lapses, but recruitment is continuing, then the researcher must apply for a Certificate to avoid a gap in coverage.²⁹ For now, those who are funded by Federal Agencies other than NIH will need to apply for a Certificate.³⁰ Applicants must still find the right institute to which to apply,³¹ which could add to burden and delay.³² Whether NIH will be

²³See *id.* § 241(d)(1)(A)(ii) (stating that the Secretary may issue a certificate of confidentiality if the research is not funded by the Federal Government).

²⁴*FAQs*, *supra* note 14.

²⁵The list of type of research which is eligible for Certificate protection supports this interpretation. Although it mostly refers to the type of research that HHS supports (i.e., “biomedical, behavioral, [and] clinical” research), it includes the unqualified “other research,” rather than limiting it to similar types of research (e.g., by stating “other *such* research”). See 42 U.S.C. § 241(d)(1)(A).

²⁶See Sec’y’s Advisory Comm. on Human Research Protections, *Final Recommendations: Certificates of Confidentiality (COCs)*, HHS (Mar. 13, 2014), <https://www.hhs.gov/ohrp/sachrp-committee/recommendations/2014-july-3-letter-attachment-b/index.html> [<https://perma.cc/PPU2-A6PW>] [hereinafter *Final Recommendations*]; Leslie E. Wolf et al., *Certificates of Confidentiality: Protecting Human Subject Research Data in Law and Practice*, 43 J. L. MED. & ETHICS 594, 600-01 (2015); Wolf et al., *supra* note 2, at 55-65.

²⁷*Final Recommendations*, *supra* note 26; Wolf et al., *supra* note 26, at 600-01; Wolf et al., *supra* note 2, at 55-65.

²⁸*Final Recommendations*, *supra* note 26; see Leslie E. Wolf et al., *The Certificate of Confidentiality Application: A View from the NIH Institutes*, 26 IRB: ETHICS & HUM. RES. 14, 15-16 (2004); Leslie E. Wolf & Jolanta Zandecki, *Sleeping Better at Night: Investigators’ Experiences with Certificates of Confidentiality*, 28 IRB: ETHICS & HUM. RES. 1, 4 (2006).

²⁹As stated by Petrice Brown-Longenecker, NIH Extramural Human Research Prot. Officer, Presentation at the Public Responsibility in Medicine & Research Advancing Ethical Research Conference, San Antonio, Tex., (Nov. 8, 2017).

³⁰Non-NIH HHS agencies issue Certificates, including CDC, FDA, HRSA, and SAMHSA. NIH refers researcher funded by those agencies contact Certificate coordinators at those agencies to determine how to obtain a Certificate. Researchers funded by other non-NIH HHS and other federal agencies may apply to NIH for a Certificate. *Certificates of Confidentiality for Other HHS Funded Research (non-NIH)*, NAT’L INSTS. HEALTH, <https://humansubjects.nih.gov/coc/HHS-funded> [<https://perma.cc/GTQ9-JJ2Y>]; *Certificates of Confidentiality for Research Funded by Non-HHS Federal Agencies*, NAT’L INSTS. HEALTH, <https://humansubjects.nih.gov/coc/another-FedDep>, [<https://perma.cc/LB25-DFZ4>]. Because the revisions provide that the Secretary “shall coordinate with the heads of other applicable Federal agencies to ensure that such departments have policies in place with respect to the issues of a certificate confidentiality,” the processes for non-NIH funded research may eventually become automatic as well. 42 U.S.C. § 241(d)(1)(G)(2).

³¹*Certificates of Confidentiality for Research Funded by Non-HHS Federal Agencies*, *supra* note 30.

³²*Final Recommendations*, *supra* note 26.

willing to provide expanded protections to non-federally funded research remains to be seen. However, if NIH continues to require the research to fall within its mission, then some research may not get the benefit of the expansion.³³

Despite the potential benefits of the expanded scope of Certificates, the automatic issuance may create significant problems for NIH-funded research given stakeholders' lack of knowledge about the protections afforded. Our previous research, for example, revealed some lack of knowledge on the part of IRB chairs and institutional legal counsel about Certificates and their protections.³⁴ However, under the old system, there was a conscious choice to obtain a Certificate's protection – either researchers elected to or their IRBs recommended they apply.³⁵ With the automatic issuance under NIH policy, many more research projects will be covered, and researchers and their institutions may not understand their obligations not to disclose even upon legal demand. This problem may be exacerbated when research data are shared, as permitted under the new statute. NIH notes researchers' obligations to ensure that other researchers with whom they share data, as explicitly permitted by the statute, are aware of the statute's requirements.³⁶ However, if researchers do not fully understand those obligations, they are unlikely to convey them effectively to other researchers. We previously identified a need for stakeholder education on Certificates.³⁷ In light of the changes, such education is even more critical. In addition, IRB measures to address these obligations – such as monitoring such disclosures through the studies they oversee – may undermine the improvements on burden.

Expansion of the disclosure prohibition to “any information, document, or biospecimen that contains identifiable, sensitive information.”—The Certificate's disclosure prohibition no longer refers only to the names or other identifying information, but explicitly expands to the data, including biospecimens, themselves. This provides a more comprehensive protection to the data, and, thus, may be more in keeping with IRBs', investigators', and participants' expectations of the Certificate's protections.³⁸ Accordingly, this expansion may make it easier for people to understand and comply with the provisions.

³³For some examples of studies that were not eligible for a Certificate as falling outside the NIH mission, see *id.*; Wolf et al., *supra* note 26, at 17. Anecdotally, we have heard complaints from researchers and IRB members about other cases in which NIH determined a Certificate could not issue because the research fell outside of its mission.

³⁴Laura M. Beskow et al., *Institutional Review Boards' Use and Understanding of Certificates*, 7 PLOS ONE e44050 (2012); Leslie E. Wolf et al., *Certificate of Confidentiality: Legal Counsels' Experiences with and Perspectives on Legal Demands for Research Data*, 7 J. EMPIRICAL RES. ON HUM. RES. ETHICS 1, 1 (2012).

³⁵Beskow et al., *supra* note 34; Wolf & Zandecki, *supra* note 28, at 4.

³⁶FAQs, *supra* note 14, at A.11 (“The NIH Policy on Certificates of Confidentiality expects that the recipient of a Certificate shall ensure that an investigator or institution who receives a copy of information protected by a Certificate understands that they are also subject to the requirements of subsection 301(d) of the Public Health Service Act.”); see also Michael Lauer, *NIH's Certificates of Confidentiality Policy Enhances Confidentiality of Participants Enrolled in Clinical Research Studies*, NAT'L INST. HEALTH OFF. OF EXTRAMURAL RES. (Sept. 7, 2017), <https://nexus.od.nih.gov/all/2017/09/07/nih-new-certificates-of-confidentiality-policy/> [<https://perma.cc/B8Y3-C3JE>] (noting “A point that is important to understand is that if your research is covered by a CoC, you are required to ensure that any investigator or institution with whom you share a copy of the identifiable sensitive information that is protected by the policy understands that they are they are [sic] also subject to the disclosure restrictions, even if they are not funded by NIH.”).

³⁷Beskow et al., *supra* note 34.

³⁸Beskow et al., *supra* note 34; Wolf et al., *supra* note 34 (reporting on the legal demands for data protected by a Certificate, identified by legal counsel).

Changes to disclosure prohibition exceptions and removal of voluntary disclosures.—The previous statutory language has been interpreted in regulations and NIH guidance as permitting voluntary disclosures of the information protected by the Certificate, as well as with individual consent.³⁹ The statute now delineates four circumstances under which the disclosure prohibition does not apply: disclosures or uses that are:

“(i) required by Federal, State, or local laws, excluding instances [of compelled disclosures in legal proceedings]; (ii) necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual; (iii) made with the consent of the individual to whom the information, document, or biospecimen pertains; or (iv) made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.”⁴⁰

This list coupled with the change in statutory language regarding compelled disclosure from “may not” to “shall not” is being interpreted as shutting the door on other voluntary disclosures.⁴¹ This change regarding voluntary disclosure removes a significant gap in the previous authority. Although researchers who sought a Certificate’s protection under the previous authority might have used this option sparingly,⁴² NIH relied on this language as a mechanism for disclosure of communicable diseases, child abuse, and other reportable conditions.⁴³ Accordingly, this constituted a large gap, that also created a strange legal fiction of “voluntarily” complying with mandatory state reporting requirements.⁴⁴

For the most part, the exceptions to the disclosure prohibition are not problematic. Disclosure with individual consent (whether in general or for the purpose of treatment) is consistent with the previous legislation.⁴⁵ Because the Certificate’s protections apply to any copies of the data in perpetuity,⁴⁶ permitting disclosure for other scientific researchers maintains the protections, provided, as discussed above, that all researchers who receive the data understand their obligations.

³⁹Under the regulations for the previous statute, “The Confidentiality Certificate does not govern the voluntary disclosure of identifying characteristics of research subjects.” 42 C.F.R. § 2a.4(j)(4) (consent disclosure requirements); see *Certificates of Confidentiality (COC) FAQs*, CTR. FOR DISEASE CONTROL AND PREVENTION OFF. OF THE ASSOCIATE DIRECTOR FOR SCI., https://www.cdc.gov/od/science/integrity/confidentiality/faq_confidentiality.htm [<https://perma.cc/UXV2-99BP>] (“Identifying information or characteristics protected by a Certificate may be disclosed under the following circumstances:... Voluntary disclosure of information by the research of information on such thing as child abuse, reportable communicable diseases, possible threat to self or others, or other voluntary disclosures provided that such disclosures are spelled out in the informed consent form; Voluntary compliance by the researcher with reporting requirements of state laws, such as knowledge of communicable disease, provided such disclosures are spelled out in the informed consent form.”); see also 42 C.F.R. § 2a.7 (regarding the effect of the Certificate).

⁴⁰42 U.S.C. § 241(d)(1)(C) (2016).

⁴¹*Id.* § 241(d)(1)(D).

⁴²See generally Wolf & Zandacki, *supra* note 28 (reporting on researchers’ experiences with the Certificate of Confidentiality and their opinions about the usefulness of obtaining this form of protection).

⁴³*FAQs*, *supra* note 14 (“Identifying information or characteristics protected by a Certificate may be disclosed under the following circumstances:... Voluntary disclosure of information by the research of information on such thing as child abuse, reportable communicable diseases, possible threat to self or others, or other voluntary disclosures provided that such disclosures are spelled out in the informed consent form; Voluntary compliance by the researcher with reporting requirements of state laws, such as knowledge of communicable disease, provided such disclosures are spelled out in the informed consent form.”). NIH policy required that researchers report communicable diseases. *Reporting of Communicable Diseases Policy*, NAT’L INST. OF HEALTH CERTIFICATES OF CONFIDENTIALITY KIOSK (Aug. 9, 1991), http://grants.nih.gov/grants/policy/coc/cd_policy.htm [<https://perma.cc/ZQ7X-AQ9L>].

⁴⁴Wolf et al., *supra* note 34, at 5.

⁴⁵It is not clear why provisions (ii) and (iii) were listed separately, as disclosure for treatment requires consent.

⁴⁶42 U.S.C. § 241(d)(1)(E); see *FAQs*, *supra* note 14.

On the other hand, the first provision, permitting disclosure as “required by Federal, State, or local laws,”⁴⁷ could create significant gaps in protections. In its guidance, including its suggested consent language, NIH appears to be interpreting this exception as incorporating mandatory reporting requirements for communicable diseases, abuse, and harm to self or others.⁴⁸ However, we do not believe that this exception is so limited. The language is unrestricted – it applies to any requirements under federal, state, or local laws – and, thus, it is difficult to predict the myriad of requirements that may fall within it.⁴⁹

The indeterminate nature of this gap creates other problems. First, there is a problem for consent. How do you describe what this exception may include, if you do not know which laws may be implicated? Second, there is a question of what happens to information that is disclosed as required by federal, state, or local laws. It is possible that once the information is disclosed into another sphere, it is no longer protected by the Certificate. It is possible that the statutory provisions protecting all copies of the data in perpetuity⁵⁰ could extend to the information that is disclosed. But it seems more likely that information disclosed in accordance with other laws would be treated no differently than other information in that realm. It would be extremely difficult to keep track, for example, of the different protections afforded to different pieces of information that have been disclosed to public health authorities as part of mandatory reporting of communicable diseases, as well as limiting their use of such data for the purposes for which it was disclosed. The admissibility provision, described below, could play a role in limiting use of such information, but it seems impractical to expect this protection to apply when the information is held by others for non-research purposes.

Information is now inadmissible as evidence and prohibited from any other use in any legal proceeding.—The new statute provides that identifiable, sensitive information, including all copies of it, protected by the statute “shall not, without the consent of the individual to whom the information pertains, be admissible as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceeding.”⁵¹ This is an important, new additional layer of protection, which limits use of protected information as evidence, for discrediting of witnesses, or any other purpose in any legal proceedings. However, the discovery principles and their powers to issue protective orders, rather than on the unfamiliar Certificate protections.⁵² We also heard concerns that judges might be unwilling to enforce a Certificate in a case involving a criminal defendant who wants the data to support his defense. In addition, as described above, it is unclear whether this protection when data are disclosed to others outside the research context as permitted by

⁴⁷Interestingly, this exception leaves out tribal laws.

⁴⁸FAQs, *supra* note 14; *Suggested Consent Language Describing the CoC Protections*, NAT’L INSTS. HEALTH, <https://humansubjects.nih.gov/coc/suggested-consent-language> [https://perma.cc/2JSL-M5HS].

⁴⁹This also creates a consent problem. It is nearly impossible to explain to participants under what circumstances disclosures may be made. We previously documented consent challenges relating to Certificates without this complication. See Laura M. Beskow et al., *Research Participants’ Understanding of and Reactions to Certificates of Confidentiality*, 5 *AJOB EMPIRICAL BIOETHICS* 12 (2014); Devon K. Check et al., *Certificates of Confidentiality and Informed Consent: Perspectives of IRB Chairs and Institutional Legal Counsel*, 36 *IRB: ETHICS & HUM. RES.* 1 (2014).

⁵⁰42 U.S.C. § 241(d)(1)(F).

⁵¹*Id.*

⁵²Wolf et al., *supra* note 26, at 599-600; Wolf et al., *supra* note 2, at 47-52.

the regulations. Indeed, it seems unlikely as a practical matter that such protections could be enforced when the information is comingled with other data held for other purposes.

Changes in the definition of identifiability.—The changes to the definition of identifiability respond to criticisms that the previous definition failed to take into account the impact of technology on identifiability of information.⁵³ Previously, the statute permitted researchers “to protect the privacy of individuals who are the subject of [applicable] research by withholding from all persons not connected with the conduct of such research the *names or other identifying characteristics of such individuals*” (emphasis added).⁵⁴ The accompanying regulations further defined identifying characteristics along familiar lines: “the name, address, any identifying number, fingerprints, voiceprints, photographs or any other item or combination of data about a research subject which could reasonably lead directly or indirectly by reference to other information to identification of that research subject.”⁵⁵ The new definition is tighter; it retains the emphasis of explicit identifiers, without specifying what those are, but also includes information from which identification could be made.⁵⁶ The specific language is information “for which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual.”⁵⁷

This change is a significant improvement over the prior definition. The literature is replete with cases in which previously various data have been combined to identify individuals within data that were thought to be deidentified.⁵⁸ While many of these efforts have been taken by researchers and require special skills, the proliferation of databases that compile information from multiple sources continues to threaten the notion of identifiability. The new language is flexible enough to take into account new developments. Nonetheless, this new definition does raise some difficulties. In particular, given the definition of “identifiable,” it is not clear how this provision will impact sharing of deidentified data as required by the federal government, other funders, or journals, to foster resource sharing and scientific advancement as the risk of identification increases.⁵⁹

Additional issues resulting from the changes

Increased challenges for consent.—The NIH’s suggested consent language for Certificates under the previous statute has been criticized on a number of grounds, including its complexity and lack of clarity in its description of some concepts.⁶⁰ The language may also simultaneously reassure *and* concern participants.⁶¹ With additional protections – such

⁵³ *Final Recommendations*, *supra* note 26; Wolf et al., *supra* note 26, at 600; Wolf et al., *supra* note 2, at 74–82.

⁵⁴ 42 U.S.C. §241(d) (2006).

⁵⁵ 42 C.F.R. § 2a.2(g); *see FAQs*, *supra* note 14.

⁵⁶ 42 U.S.C. § 241(d)(1)(G)(4)(A).

⁵⁷ *Id.* § 241(d)(1)(G)(4)(B). Although we have heard some refer to “any risk” of identification, that interpretation is not supported by the statutory language.

⁵⁸ *See* Wolf et al., *supra* note 26, at 603; Wolf et al., *supra* note 26, at 76–78.

⁵⁹ Mark Barnes of Ropes & Gray raised this point in a meeting of the Secretary’s Advisory Committee on Human Research Protections on October 18, 2017. NIH states in its frequently asked questions that such sharing is still permitted. *FAQs*, *supra* note 14.

⁶⁰ Beskow et al., *supra* note 49; Joseph Catania et al., *Research Participants Perceptions of the Certificate of Confidentiality’s Assurances and Limitations*, 2 J. EMPIRICAL RES. ON HUM. RES. ETHICS 53 (2007); Check et al., *supra* note 49.

⁶¹ Beskow et al., *supra* note 49; Catania et al., *supra* note 60; Check et al., *supra* note 49.

as the new prohibition on information use as evidence – and exceptions to those protections, the new suggested language predictability suffers from similar complaints.⁶² It is over 350 words long, with an average of 41.0 words per sentence.⁶³ As a result, it scores poorly on two common readability scores. It has a Flesch reading⁶⁴ ease score of 19.7, much lower than the of target 70-90. It has a Flesh-Kincaid Grade Level score of 19.1, which means it requires a post-graduate level of education to understand.⁶⁵ The suggested language also limits its discussion of disclosure under federal, state, and local laws to reporting requirements for communicable diseases, abuse, and harm to self or others. These are common exceptions that often were included under the previous statute based on NIH and IRB policies. However, as described above, the potential scope of this exception is much larger. This suggested language therefore may focus attention too narrowly on these particular exceptions. The content of the NIH's suggested language matters because we found that institutions typically relied on it, even as they complained about it.⁶⁶

We are aware of efforts to draft simplified language about the new provisions. For example, the National Cancer Institute has recommended use of the following simplified language:

“Your privacy is very important to us. The study doctors will make every effort to protect it. The study doctors have a privacy permit to help protect your records if there is a court case. However, some of your medical information may be given out if required by law. If this should happen, the study doctors will do their best to

⁶²*Suggested Consent Language*, *supra* note 48. The complete text of the suggested language is as follows:

This research is covered by a Certificate of Confidentiality from the National Institutes of Health. The researchers with this Certificate may not disclose or use information, documents, or biospecimens that may identify you in any federal, state, or local civil, criminal, administrative, legislative, or other action, suit, or proceeding, or be used as evidence, for example, if there is a court subpoena, unless you have consented for this use. Information, documents, or biospecimens protected by this Certificate cannot be disclosed to anyone else who is not connected with the research except, if there is a federal, state, or local law that requires disclosure (such as to report child abuse or communicable diseases but not for federal, state, or local civil, criminal, administrative, legislative, or other proceedings, see below); if you have consented to the disclosure, including for your medical treatment; or if it is used for other scientific research, as allowed by federal regulations protecting research subjects.

[*Use the following language as applicable*] The Certificate cannot be used to refuse a request for information from personnel of the United States federal or state government agency sponsoring the project that is needed for auditing or program evaluation by [THE AGENCY] which is funding this project or for information that must be disclosed in order to meet the requirements of the federal Food and Drug Administration (FDA). You should understand that a Certificate of Confidentiality does not prevent you from voluntarily releasing information about yourself or your involvement in this research. If you want your research information released to an insurer, medical care provider, or any other person not connected with the research, you must provide consent to allow the researchers to release it.

[*language such as the following should be included if researcher intends to disclose information covered by a Certificate, such as potential child abuse, or intent to hurt self or others in response to specific federal, state, or local laws.*] The Certificate of Confidentiality will not be used to prevent disclosure as required by federal, state, or local law of [*list what will be reported, such as child abuse and neglect, or harm to self or others*].

[*language such as the following should be included if researcher intends to disclose information covered by a Certificate, with the consent of research participants.*] The Certificate of Confidentiality will not be used to prevent disclosure for any purpose you have consented to in this informed consent document [*restate what will be disclosed, such as including research data in the medical record*].

⁶³*Id.* The length is surely going to make it difficult to comply with the new Common Rule provisions designed to shorten consent documents, now slated to go into effect in July 2018. *See generally* Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7211-14 (Jan. 19, 2017); Federal Policy for the Protection of Human Subjects: Delay of the Revisions to the Federal Policy for the Protection of Human Subjects, 83 Fed. Reg. 2885 (Jan. 22, 2018).

⁶⁴A Flesch Reading rates text on a 100-point scale, with the higher the score indicating the easier the text is to understand. *Test Your Document's Readability*, MICROSOFT, https://support.office.com/en-us/article/Test-your-document-s-readability-85b4969e-e80a-4777-8dd3-f7fc3c8b3fd2#_toc342546557 [<https://perma.cc/6YN3-JFF2>].

⁶⁵We used the built-in feature in Microsoft Word to calculate these results. IRBs typically recommend that consent language be at a 6th, 8th grade level.

⁶⁶Wolf et al., *supra* note 2, at 603.

make sure that any information that goes out to others will not identify who you are.”⁶⁷

This suggested language does a much better job of meeting readability targets with an 8th grade reading level. But in simplifying the language, it creates problems with accuracy. It substitutes “privacy permit” for “Certificate of Confidentiality.” This may prevent the enterprising participant from finding out more about this protection in an internet search. Use of phrases such as “study doctors” and “medical information” rather than “researchers” and “research data” could give the impression that medical records may be protected, when the Certificate does not apply to them. Also, it omits the Certificate’s protections in non-court cases and that it cannot be used as evidence.

Another group proposed the following language:

“Most people outside the research team will not see your name on your research information. This includes people who try to get your information using a court order. One exception is if you agree that we can give out research information with your name on it. Other exceptions are information about child abuse or neglect and harm to yourself or others.”⁶⁸

Like the NCI language, this mostly succeeds in meeting readability targets, but sacrifices accuracy. It does not indicate there is a Certificate. Once again, the language focuses on court cases, leaving out other legal proceedings, and ignores the admissibility provision. Both of these efforts demonstrate the tension between conveying Certificate language in simplified form that is accessible to most Americans and accurately conveying the Certificate’s provisions. We would recommend that NIH take the lead on developing a simpler, but more accurate, version of its suggested language, as its language will likely prevail.⁶⁹

Uncertainty regarding what constitutes “consent” for purposes of disclosure and admissibility.—Consent is an important exception to both the disclosure prohibition and the admissibility restriction. However, the statute does not specify what constitutes consent. How narrowly or broadly consent is interpreted will be critically important to how effective these protections are. Suppose, for example, a participant provides written consent to allow study information to be included in her medical record. Although HIPAA and state medical privacy laws protect the confidentiality of her medical record, it is subject to subpoena. Could the consent to place the information in the medical record also be construed as consent for admissibility purposes? This kind of approach is not unprecedented. Although not involving *participant* consent, a court considered researcher disclosure of participant identities to state officials for purposes of protecting children from abuse and neglect as obviating a Certificate’s protections of all of these participants’ other study data.⁷⁰ The same logic that allowed a court to view disclosure of some information to permit

⁶⁷ *Informed Consent*, NAT’L CANCER INST. (last updated Jan. 31, 2018), https://ctep.cancer.gov/protocolDevelopment/informed_consent.htm [<https://perma.cc/4WKF-KWZP>].

⁶⁸ 425. *Certificates of Confidentiality*, U. NEVADA, RENO, <https://www.unr.edu/research-integrity/human-research/human-research-protection-policy-manual/425-certificates-of-confidentiality> [<https://perma.cc/AB8E-SWZS>].

⁶⁹ Catania et al., *supra* note 60; Check et al., *supra* note 49, at 4.

⁷⁰ See Wolf et al., *supra* note 26, at 598; Wolf et al., *supra* note 2, at 43–46.

disclosure of other information could prompt a court to view consent to disclosure as consent to admissibility or use. Because a broad reading of consent weakens the protections the Certificate affords, we recommend that HHS adopted regulations or guidance that specific consent for disclosure and admissibility are required. This specific consent should be limited to the particular use, so that consent for one disclosure or use is not expanded to other uses. This approach is consistent with how waiver of protections is used in other areas of law.⁷¹

Uncertainty regarding the effectiveness of the Certificate's protections.—Our previous research documented substantial uncertainty on the part of IRB members and institutional counsel about whether and how courts would enforce Certificates' protections under the previous authority.⁷² Through our research, we also identified the handful of reported and unreported cases involving a legal demand of data protected by a Certificate.⁷³ These cases present a mixed picture. The first and most well-known case involved a subpoena for patient photographs in the context of a murder investigation; a witness to the murder said that she saw the murder in the methadone clinic. Factually, the case is strong – the court upheld the clinic director's refusal to produce the photographs because he held a Certificate. Legally, however, the case did not really address the strength of the Certificate statute, focusing more on whether a second statute took precedence over the Certificate statute.⁷⁴ Other cases reveal how attorneys and courts often balance the Certificate's provisions with the needs of litigants – deidentified data are shared by agreement or court order, typically with protective orders that restrict additional uses and disclosures and agreements not to try to reidentify individual participants.⁷⁵ One case recognizes the limits of that approach where reidentification may be relatively easy.⁷⁶ One case shows how unfamiliar attorneys and judges may be with the Certificate's protections, discussing the protections in a case that does not have one.⁷⁷ Finally, one case shows how the general predisposition to accessing information – and other competing interests – can undermine the Certificate's protections.⁷⁸

The new statutory authority does not alleviate that uncertainty and, in some ways, may exacerbate it. Attorneys and courts are going to be as unfamiliar with this protection as they were under the previous authority, although there is some hope that the broad protection of research data (or at least federally-funded data) may ultimately raise awareness. The addition of the admissibility protection, while a good addition, may mean attorneys and courts may confront this issue more frequently. This could be troublesome if they do not understand it. Moreover, the disclosure prohibition exception for federal, state, and local laws could substantially complicate the picture. Is that information protected from subpoena and use as evidence? As described above, we think there are reasons to think it is not. But it

⁷¹ See Wolf et al., *supra* note 26, at 599-600; Wolf et al., *supra* note 2, at 48-52.

⁷² Beskow et al., *supra* note 34; Wolf et al., *supra* note 34, at 5.

⁷³ See Wolf et al., *supra* note 26, at 596-600; Wolf et al., *supra* note 2, at 18-38.

⁷⁴ See Wolf et al., *supra* note 26, at 596; Wolf et al., *supra* note 2, at 27-31 (discussing *People v. Newsman*).

⁷⁵ See Wolf et al., *supra* note 26, at 599; Wolf et al., *supra* note 2, at 22-23 (discussing *In re: Louisville Branch-National Association for the Advancement of Colored People*).

⁷⁶ See Wolf et al., *supra* note 26, at 604; Wolf et al., *supra* note 2, at 38-39.

⁷⁷ See Wolf et al., *supra* note 26, at 597; Wolf et al., *supra* note 2, at 34-36 (discussing *Murphy v. Philip Morris Inc.*).

⁷⁸ See Wolf et al., *supra* note 26, at 599-600; Wolf et al., *supra* note 2, at 48-52.

will not be easy to sort through this issue, and cases addressing these questions could add to confusion about the effectiveness of Certificates. As we saw in our previous research, some IRB members and researchers misunderstood the Certificate as protecting *all* data.⁷⁹ Thus, they would view disclosure of deidentified data as a failure of the Certificate, even if it fits within one of the exceptions. Accordingly, we see potential for more such cases, which could undermine faith in Certificates. Moreover, there will be uncertainty about whether the existing Certificate cases apply to the revised statute, given the differences between them.

Transition issues

The 21st Century Cures Act explicitly applies the revisions to holders of Certificates issued before the Act.⁸⁰ Accordingly, all existing holders of Certificates were converted to the new Certificate in June 2017. In addition, any NIH study funded on or after December 13, 2016 was “issued” a Certificate retroactively as of October 1, 2017.⁸¹ Both of these groups may have already recruited participants and, in some cases, completed recruitment. Do these researchers need to incorporate the new provisions into existing consent documents, brochures, and other research documents that are already in use? Do they need to recontact participants to inform them of the new provisions and obtain consent again? NIH has indicated that it will not require such revisions or recontact.⁸² However, individual IRBs will have to decide what to do for studies they oversee. Certainly, it could be difficult to recontact participants in certain kinds of studies that are affected by the transition. But failing to do so would leave participants uninformed about their rights. Institutional counsel told us that the majority of cases involving a legal demand are specific to the individual.⁸³ Accordingly, we can imagine cases in which a litigant could seek to use research data – gained through consent or inadvertently disclosed – against a participant. If the participant has not been informed about the Certificate’s new provisions, then she cannot assert her rights under it. While we might hope that the participant’s attorney would know about this provision and assert this protection, our previous research suggests that even institutional counsel are unfamiliar with many of the provisions of the prior Certificate authority.⁸⁴

Conclusion

We see many positives in the changes to Certificate’s protections enacted through the 21st Century Cures Act, as many of them address limitations we identified in our empirical research. These changes have extended the Certificate’s protections to many more research projects and participants. In many cases, the process is automatic, alleviating burdens on researchers and avoiding delays in protections. They have also provided additional

⁷⁹Beskow et al., *supra* note 34, at 5; Wolf et al., *supra* note 34, at 4.

⁸⁰Specifically, the Act provides that “beginning 180 days after the date of enactment of this Act, all persons engaged in research and authorized by the Secretary of Health and Human Services to protect information under section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)) prior to the date of enactment of this Act shall be subject to the requirements of such section (as amended by this Act).” § 2012(b).

⁸¹*FAQs*, *supra* note 14.

⁸²*Id.* (“Neither the NIH Policy on Certificates of Confidentiality nor subsection 301(d) expect participants consented prior to the change in authority, or prior to the issuance of a Certificate, to be notified that the protections afforded by the Certificate have changed, or that participants who were previously consented to be re-contacted to be informed of the Certificate, although IRBs may determine whether it is appropriate to inform participants.”).

⁸³Wolf et al., *supra* note 34, at 3.

⁸⁴*Id.* at 4.

protections against use, should protected data be disclosed. However, the changes are not perfect and, in some cases, may undermine the protections afforded. In particular, we are concerned that the exception to the disclosure prohibition for requirements under federal, state, and local law may have opened the door too wide and may rightly concern, rather than reassure, prospective participants. We are also concerned that members of the research community may not be adequately informed about these changes. While the NIH Certificate of Confidentiality kiosk remains a helpful resource about Certificates, we believe that significant outreach to the community is needed to ensure that all stakeholders understand their new obligations. There is also some uncertainty about some provisions. We appreciate that NIH has expended substantial effort to update its policies and website to respond to and explain the changes. We anticipate that these efforts will continue and hope that the NIH and others who issue Certificates will address some of the issues that we raise here.