DEAN M. HARRIS

Associate Professor, Department of Health Policy and Management, Gillings School of Global Public Health, University of North Carolina at Chapel Hill, United States of America; Bachelor of Arts degree from Cornell University in 1973; Juris Doctor degree from UNC School of Law in 1981; Member of the American Health Law Association; Member of the European Association of Health Law
dean_harris@unc.edu

THE LAW OF MEDICAL PRIVACY IN THE USA: NOT GOOD ENOUGH FOR COVID-19

This article addresses the privacy of medical and health data in the US. It analyzes the scope and requirements of federal and state laws in the US, and it discusses the weaknesses in the US protection of medical privacy. Then, this article explains how the weak US system of privacy protection was unable to handle many important privacy issues in the COVID-19 pandemic. Finally, the article concludes with some recommendations for action.

Key words: privacy; medical privacy; HIPAA privacy rule; COVID-19; US law.

Compared to many other countries, the United States (US) provides less protection for the privacy of medical information. The comparative weakness of US privacy protection is not limited to medical information, but rather applies to many types of data about individuals. For example, on July 16, 2020, the European Court of Justice (ECJ) concluded that the «Privacy Shield» agreement for transfer of data from the European Union (EU) to the US was invalid, because US law does not provide a level of privacy protection that meets EU standards [1]. In that case, the ECJ determined that «the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States ... are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law ...» [2].

The privacy laws of each country reflect the culture and values of that society. In adopting and amending their privacy laws, people in each country are making decisions on how to balance the interests of individuals against the needs of society. In addition, they are making decisions on how to limit

the activities of the public and private sectors in their society. How much should the government restrict and regulate how private companies collect and use personal information about individuals? How much access should the government have to personal information about individuals? How should government balance the goal of individual privacy and other important goals of society such as public health.

At the World Economic Forum in Davos on January 23, 2019, German Chancellor Angela Merkel explained the different approaches to data privacy in the US, China, and Europe. «On the one hand, we have the United States. There, data is largely in the hands of private stakeholders.... On the other hand, we have China. There the state has extensive access to all data – even personal data. Neither of these two very different approaches is in line with my own ideas or those which influenced Germany with its social market economy, ideas that include the protection of privacy» [3]. Thus, the US approach to privacy is very different from the approach in China, and it is very different from the approach in Europe as set forth in the EU's General Data Protection Regulation.

This article addresses the privacy of medical and health data in the US. It analyzes the scope and requirements of federal and state laws in the US, and it discusses the weaknesses in the US protection of medical privacy. Then, this article explains how the weak US system of privacy protection was unable to handle many important privacy issues in the COVID-19 pandemic. Finally, the article concludes with some recommendations for action.

Scope and requirements of federal and state laws in the US

For many years, state governments in the US have regulated the privacy of health data. Each of the 50 US states has different privacy laws. Even within one state, there might be separate laws that apply to data in the possession of doctors, hospitals, pharmacies, insurance companies, and other organizations. Some state laws only relate to information about a specific disease, such as laws that protect data about HIV/AIDS.

State laws in the US try to balance the two goals of preserving individual privacy, on one hand, and promoting disclosure to protect the public, on the other hand. To promote the goal of privacy, laws of state governments prohibit the unauthorized disclosure of private medical information. State laws might allow patients to sue their health care providers for improper disclosure of information.

In contrast, other state laws promote the goal of disclosure to protect public health, by requiring doctors to notify public health authorities about communicable diseases, even if the patient does not consent to that disclosure [4, p. 98–100]. Some state laws also promote the goal of disclosure for public safety, by imposing legal liability on health care professionals for failing to disclose when their patient threatens to harm another person. Therefore, under state law a doctor could be sued for improperly disclosing or failing to disclose.

In *Tarasoff v. Regents of the University of California* [5], a student named Prosenjit Poddar told his psychologist at the University of California at Berkeley that he planned to kill Tatiana Tarasoff, who rejected him. The psychologist called the campus police about Poddar, but the campus police released him. The psychologist did not warn Tatiana about the threat. Two months later, Poddar killed Tatiana, for which he was charged with murder.

In a related civil lawsuit, Tatiana's parents sued the psychologist and the university. Among other claims, Tatiana's parents argued that the psychologist had a duty to protect Tatiana. However, Tatiana was not the psychologist's patient. Moreover, warning Tatiana about Poddar's intentions would have resulted in a breach of Poddar's medical privacy. The California Supreme Court held that therapists have a duty to potential victims, as well as a duty to their patients. According to the Court, «[w]hen a therapist determines, or pursuant to the standards of his profession should determine, that his patient presents a serious danger of violence to another, he incurs an obligation to use reasonable care to protect the intended victim against such danger» [5, p. 340]. Since that 1976 California decision, legal rules to require disclosure or permit disclosure have been adopted in most—but not all—US states [6].

In contrast to the long history of state medical privacy laws, the US federal government had a relatively small role in medical privacy before 1996. Historically, the federal government has regulated the privacy of records in federal agencies and federal health care facilities, such as hospitals for military personnel or veterans. Federal law has also regulated the privacy of records about treatment for substance abuse and alcoholism, and federal regulations have required confidentiality of data in federally-funded research with human subjects. Aside from that limited role, the federal government left the protection of health privacy to the 50 state governments.

In 1996, the federal government started to take a more active role in medical privacy, when Congress enacted a federal statute called the Health Insurance Portability and Accountability Act (HIPAA) [7]. That federal statute required the Executive branch of government, specifically the US Department of Health and Human Services (HHS), to adopt a rule on the privacy of health data. The first HIPAA privacy rule became effective in 2001, and the rule has been amended since that date.

The HIPAA privacy rule applies to «covered entities» and their «business associates». Covered entities that are subject to the privacy rule are health plans (such as insurance companies), health care clearinghouses (such as billing services), and health care providers who transfer health information in electronic form (such as doctors and hospitals). In 2009, Congress passed a separate federal statute called the «HITECH Act». The HITECH Act required the Executive branch to amend the HIPAA privacy rule so that it would also apply to «business associates» of a covered entity [8]. Business associates are outside contractors of a covered entity, such as outside lawyers or accountants for a hospital, who could have access to private medical information in the course of their work for the hospital.

Like state privacy laws, the federal HIPAA privacy rule tries to balance the competing public interests of preserving individual privacy and promoting disclosure when it is necessary to protect the public. The HIPAA privacy rule generally prohibits use or disclosure of «protected health information». However, the rule permits disclosure of protected health information with consent of the patient (or someone who has authority to act for the patient). In addition, the rule permits disclosure without consent of the patient in some circumstances, as set forth in the very complicated rule. For example, disclosure is permitted without prior written consent for purposes of health care treatment or payment, as well as for public health activities.

The HHS Office for Civil Rights has authority to enforce the federal HIPAA privacy rule. Health care providers may be required to pay large fines for violation of the rule. HIPAA does not give individual patients the right to sue health care providers for improper disclosure of private information. However, patients might be able to sue health care providers for improper disclosure under state medical privacy laws [4, p. 113; 9, p. 838].

The federal HIPAA privacy rule does not completely replace or «preempt» state medical privacy laws. Congress has the power to determine the relationship between the federal HIPAA privacy rule and state medical privacy laws. One alternative was to make the federal HIPAA privacy rule the only medical privacy law in the US, and prohibit different medical privacy laws in each state. Another alternative was to allow state governments to adopt separate privacy laws in each state, which would apply in addition to the federal HIPAA privacy rule.

Congress decided to give some flexibility to the states, rather than uniformity in the whole country. Therefore, the federal HIPAA privacy rule allows state governments to provide more legal protection for medical privacy within their states. The HIPAA privacy rule does not «preempt» (supersede or replace) state laws which give more protection for medical privacy. As a practical matter, a state law which gives less privacy protection than the HIPAA privacy rule would be irrelevant. If a state law gives more privacy protection than the HIPAA privacy rule, organisations that have medical information in that state must comply with both the federal HIPAA privacy rule and the applicable state law.

Weaknesses in the US protection of medical privacy

There are several basic weaknesses in current US laws on the privacy of medical information. First, the US does not have one comprehensive law to protect the privacy of data about individuals, but rather has separate laws for data in different sectors of the economy and society. For example, the US has different laws that apply to medical data, financial information, and educational records of students. Second, in regard to medical privacy, the federal HIPAA privacy rule does not regulate personal health data as a type of property, but only regulates some «holders» of some types of health data [9, p. 837–38]. Third, the HIPAA privacy rule regulates the use and transfer of

data, but does not regulate the collection of data [9, p. 837–38]. Finally, some health-related data is not regulated, because it is in what Professor Nicolas Terry calls «HIPAA-free space» [9, p. 837–38].

Under these circumstances, «big data» companies use unprotected health-related data, instead of HIPAA-protected data. Big data uses «predictive analytics» (algorithms) on large volumes of data to predict and influence individual behavior [10, p. 77–80]. For example, big data companies can use unprotected «medically inflected data» about individuals from sources other than the health system, such as individuals' purchases, online searches, and social media [10, p. 84–87]. In addition, patients can create unprotected health data when they download their medical records from health care providers to their personal devices [10, p. 82–84].

Imagine what big data companies, advertisers, and sellers could know—or strongly assume—about an individual's health, without seeing that individual's medical records. What could they know or predict about that individual's health conditions or health concerns from the types of food which that individual buys at supermarkets, such as food that is salt-free, sugar-free, fat-free, or gluten-free? What could they know or predict from the non-prescription («over-the-counter») medicines and health-related products which that individual buys online or in stores other than pharmacies? What do that individual's internet searches and social media activity indicate about his or her likely health status or health concerns?

As discussed above, the federal HIPAA privacy rule only applies to «covered entities» and their «business associates». Therefore, the rule does not apply to personal information that is collected by many types of stores, online retailers, or internet sites. Many state medical privacy laws have similar limitations. Under these circumstances, US laws on medical privacy are not sufficient to address many types of privacy issues, including many privacy issues that arise during a pandemic.

HIPPA does not effectively protect privacy during COVID-19

During a pandemic, some people think that the balance between individual privacy and the needs of society should shift to provide less protection for the privacy of medical data and more disclosure of private data for the benefit of public health. How far should we go in allowing disclosure of private medical data—even during a pandemic? Will we be able to get back to the pre-pandemic level of privacy protection? As Casey Ross asked, «Will we go back to normal, or will the erosion of privacy become part of the fabric of American health care, accepted as the price of continued vigilance against new viruses, in the same way Americans tolerated the loss of privacy and personal freedoms after the 9/11 terrorist attacks?» [11].

In fact, the HIPAA privacy rule already provided flexibility for the health care industry to deal with issues of communicable disease, even before the COVID-19 pandemic. For example, the HIPAA privacy rule allows health care

professionals and health care facilities to disclose protected health information to a public health department about an individual, without consent of that individual, for purposes of public health activities [12]. It was not necessary, therefore, to amend or repeal the HIPAA privacy rule during the pandemic. However, the federal government did issue some guidance about applying the HIPAA privacy rule during COVID-19. The government also used its enforcement discretion to reassure the health care industry that it would not be penalized for certain technical violations of the rule [13].

For example, the HHS Office for Civil Rights (OCR) explained that the HIPAA privacy rule allows disclosure of private medical data, without consent, to police and first responders when necessary to provide treatment or to protect responders or other people [14]. OCR also announced that, during the pandemic, it would use its enforcement discretion to refrain from imposing penalties when business associates of covered entities disclose protected health information in good faith for purposes of health oversight and public health [15]. Similarly, OCR announced that, during the pandemic, it would use its enforcement discretion to refrain from imposing penalties on health care professionals and facilities that provide services to patients in good faith by means of telehealth, even if the technology or its use do not strictly comply with the HIPAA privacy rule [16].

In each of these statements, the federal government was assuring health care providers (and their business associates) that, during the pandemic, the HIPAA privacy rule will not prevent them from disclosing appropriate information to protect public health or using telehealth in good faith to provide health care services. The guidance from OCR and its use of enforcement discretion were relatively small actions in the overall scheme of privacy protection. The government did not significantly reduce the overall level of protection for individual privacy in the US, such as it is, but neither did the government increase the level of protection for medical privacy. Nevertheless, those small actions by the government were probably useful in the context of an American society which is very litigious and a health care industry which is very risk-averse.

Most importantly, those statements from the government—and the HIPAA privacy rule itself—do not reduce many risks to medical privacy which arise from use of technology during a pandemic. In the modern world, and especially during the COVID-19 pandemic, people are increasingly likely to seek medical information from online sources that are not regulated by the HIPAA privacy rule. Like many state-level medical privacy laws, HIPAA regulates the relationship between individuals and the health care industry. This includes health care professionals, health care facilities, insurance companies, and health care clearinghouses, as well as their outside contractors called business associates.

However, HIPAA does not regulate the online sources outside the health care industry from which many people now obtain medical information, such as information about symptoms of COVID-19 or where to obtain testing for

possible infection. By seeking that type of information online from unregulated sources, individuals put their medical privacy at risk from a practice called «web tracking» [17]. Recent research has demonstrated that the vast majority of websites related to COVID-19 contain tools, such as third-party data requests or «cookies,» that transmit data to advertisers or other companies. This practice is not limited to COVID-19 websites created by for-profit corporations [17]. «Third-party tracking was pervasive even among government and academic COVID-19–related web pages, on which visitors might reasonably expect greater privacy protections. Decision-makers at these institutions may be unaware of third-party tracking on their websites because they do not realize that tools used to monitor website traffic transmit data to third parties» [17, p. 1464]. In a separate article, three of the researchers who performed that study explained that the practical consequences of this loss of individual privacy could include receiving advertisements for fake COVID treatments, being «profiled» as a possible COVID patient, and being subjected to discrimination by potential employers [18].

Another threat to medical privacy, which is beyond the reach of HIPAA, is the possible collection of personal information from online communication platforms by means of «data vacuuming technologies» [19]. One effect of COVID-19 is that many more people are using online communication platforms to work from home or attend classes from home. Generally, those online communication platforms are not covered entities or business associates, as defined in the HIPAA privacy rule. Therefore, the rule does not apply. Concerns have been raised about individual privacy when adults or children use those platforms, such as the possibility that some of those sites might collect information about users [19]. Even if the information collected by some of those platforms does not include medical data, third-parties could use non-medical information to assume or predict an individual's health status or health concerns, as discussed above.

In addition, the HIPAA privacy rule generally fails to protect individual privacy in the use of «apps» for COVID-19 contract tracing. Contact tracing apps can notify users if they were close to a person who tested positive for COVID-19. Several countries have been using digital tools in an effort to control the pandemic, including technology to trace individuals who have been--or might have been--exposed to COVID-19 [20]. In the US, however, only a small percentage of the population has used apps for contact tracing, most of which are established by state governments [21]. Reasons for the low utilization of contract tracing apps in the US include lack of coordination by government, insufficient spending on advertising, and concerns about privacy [21].

In most situations, the HIPAA privacy rule does not apply to the apps which are used for COVID-19 contract tracing. The operators of those apps are generally not covered entities or business associates, as defined in the privacy rule. The federal government has explained that an individual may tell his

or her health care provider to transfer private medical information to an app, which is unrelated to the health care provider. After the medical information is transferred from the health care provider to an unrelated app, the HIPAA privacy rule no longer applies [22]. «Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules» [22].

Finally, the HIPAA privacy rule does not protect individuals from potential harms caused by publication of non-individual, aggregated data. Even if data published during a pandemic could not be used to identify a specific individual, some individuals could be harmed by publication of data about a group to which those individuals belong. The HIPAA privacy rule only applies to «protected health information» (PHI), which generally means information that is individually identifiable or could be used to identify an individual [23]. What if the data indicate that a particular city or neighborhood has a very high rate of COVID-19 infections, hospitalizations, or deaths? Making that data available to the public online or in news media could subject individuals who live there to discrimination or perhaps even violence.

Some people have argued that the public has a «right to know» so that people could protect themselves from COVID-19 [24]. Also, it is arguable that publishing information could help citizens to understand the seriousness of the situation, and help them to make informed choices about supporting or opposing government policies to deal with the pandemic. On the other hand, some people have expressed concerns about the possibility of stigmatizing the residents of a particular community or encouraging harassment of its residents [25].

In the US, this issue is complicated by the need to increase awareness about the serious health disparities that exist on the basis of race and ethnicity. African-American (Black) people in the US have a shorter life expectancy than Whites, and the rate of infant mortality for Blacks in the US is much worse than it is for Whites. As compared to White Americans, Black and Latino people in the US have higher rates of COVID-19 infection and higher death rates from COVID-19 [26]. Therefore, it is important to carefully consider how to publicize non-individual data about COVID-19, without causing stigma or harassment. The HIPAA privacy rule does not help in resolving this complex issue, because that rule only applies to information that identifies or could be used to identify a specific individual.

Recommendations for action

Potential solutions to address these problems of medical privacy could be taken at the federal level, including legislative action by Congress or regulatory changes by the Executive branch of government, or both. Aside from action at the federal level, state governments could increase their own protection of privacy by means of state legislation or regulation. Even without any action by government, technology companies and industry organisations could take steps

that would help to protect medical privacy to some extent. Finally, individual consumers could increase their own level of protection by learning more about the risks to privacy that arise from use of technology, and by using technology in ways that provide a higher level of protection.

The most effective method to increase medical privacy in the US would be for Congress to enact a statute to protect the privacy of all data about individuals, or at least to provide more effective protection for the privacy of medical data. However, that is not likely as a practical matter. In fact, the inability of Congress to enact a statute about medical privacy is the reason that the US currently relies on the HIPAA privacy rule, which was adopted by the Executive branch of government.

When Congress enacted the HIPAA statute in 1996, Congress gave itself three more years to enact additional legislation that would establish standards for privacy of medical data [27]. Congress appeared to recognize that it might be unable to enact that additional legislation. Therefore, Congress provided explicitly for that possibility. In the event that Congress did not enact additional legislation for medical privacy within three years, the HIPAA statute required the Executive branch (HHS) to adopt standards for medical privacy by means of a regulation [27]. Congress failed to meet the three-year deadline, and HHS adopted the HIPAA privacy rule, which still exists today after several amendments. In light of this history, and in light of the highly partisan state of US politics, it is unlikely that Congress would be able to enact comprehensive legislation for protection of medical privacy.

Nevertheless, it is possible that Congress could enact more limited legislation that would address only one issue of medical privacy or a small number of related issues. This type of small-scale federal legislation might relate to privacy risks that arise from use of technology during a pandemic. One alternative is that Congress could prohibit practices that pose the most risk to privacy during a pandemic, such as «web tracking» [17], «data vacuuming» [19], or some uses of contact tracing apps [21]. Another alternative is to require more disclosure to consumers, and require that consumers have more choice about the use or transfer of their medical information. Rather than prohibiting specific technologies or uses of technology, it might be more politically feasible for Congress to require web sites, technology companies, and apps to clearly disclose to consumers how their private information would be collected and used, and give consumers a realistic opportunity to easily «opt out».

Without legislative action by Congress, could the Executive branch of government (HHS) amend the HIPAA privacy rule to protect against risks to privacy that arise from use of technology during a pandemic? HHS might be able to make some useful amendments to its HIPAA privacy rule, but the actions of HHS would be limited by the terms of the HIPAA statute. In adopting or amending rules or regulations, an administrative agency may only act within the scope of authority that was delegated to the agency by the legislative branch in a statute.

In this case, the relevant part of the HIPAA statute relates to the health care system including health care providers, health insurance plans, and the administrative process for payment of health insurance claims [27, § 261–264]. In the 2009 HITECH Act, Congress extended the scope of the HIPAA privacy rule to include «business associates» of covered entities [8]. However, neither the HIPAA statute nor the HITECH Act extends the scope of privacy protection to include all internet sites, technology providers, big data companies, or operators of apps. It is unlikely that HHS could extend the scope of its HIPAA privacy rule beyond the health care industry and its business associates, and any attempt to do so would be met by serious legal challenges in the federal courts.

Regardless of any action or inaction by the federal government, state governments have the power to enact or amend their own laws about medical privacy. As discussed above, the federal HIPAA privacy rule allows state governments to provide more legal protection for medical privacy within their states. Thus, state medical privacy laws would not be limited to covered entities and their business associates.

State laws and federal laws have advantages and disadvantages in trying to meet the goals of health policy and public health. The US federal government can create laws which apply uniformly throughout the entire nation. In addition, the federal government has more money than state governments to implement and enforce its laws. However, state governments might be more responsive to local conditions and local needs. In addition, state governments can experiment with new laws to determine what works best. A state law might be more feasible as a practical matter, because it does not require a nationwide consensus or agreement by a majority in the national legislature.

Some people have expressed concern that adoption of state privacy laws could force websites and apps to use different privacy policies for each of the 50 states [28]. However, the State of California enacted its own privacy law in 2018 before COVID. At least one large technology company said that it would apply the requirements of California law throughout the US, rather than create different policies for different states [29].

Technology companies and operators of apps could take action on their own to increase protection of medical privacy, even without any requirement or prohibition from federal or state government. The motivation for companies and apps would be to increase acceptance and utilization of their systems by consumers, and possibly gain an advantage in a competitive market. Trade associations or other industry organisations could create voluntary codes of conduct, in regard to protection of medical privacy. Although compliance would be voluntary, companies and apps that choose to comply could receive a certification, which would provide a signal to consumers about the level of privacy protection.

Matthew McCoy and colleagues recommended that agencies, institutions, and organisations which operate websites about COVID-19 should conduct privacy audits of their websites to prevent «web tracking» [18]. McCoy et al

also recommend that for-profit companies which operate health websites should change their advertising policies to increase privacy protection. «Commercial websites that provide health information may rely on advertising revenue, but they can do so in ways that are more protective of user privacy. They should consider moving to non-targeted ads which are proving profitable in Europe, where health-based ad targeting is illegal» [18, p. 6].

Meanwhile, the Brennan Center for Justice made several recommendations about privacy for state governments which operate apps for contact-tracing or other purposes [30]. «It is incumbent on state health departments to set forth clear privacy policies in order to foster public trust. While Covid-19 apps will necessarily involve some tradeoff between public health and user confidentiality, it is important that states work to minimize privacy harms to encourage the utilization of their apps and protect their residents. Recognizing this, states must be vigilant in auditing their apps and prioritizing transparency and public accountability» [30, p. 9].

Finally, individual consumers could do more to protect their own privacy, by learning more about the risks to privacy, and by using technology in ways that provide more protection. In the US, most people think that a website which has a «privacy policy» will not share personal data without their consent, but that is not correct [31]. Rather, privacy policies «explain how companies will use your information—because they are using it» [31].

1. Satariano, A, E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact, *New York Times*, (July 16, 2020). URL: <https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html>

2. Schrems and Facebook Ireland v Data Protection Commissioner, (2020) CJEU Case C-311/18, Paragraph 185. URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=9791227>

3. Speech by Federal Chancellor Angela Merkel at the 49th World Economic Forum Annual Meeting in Davos on 23 January 2019. URL: <https://www.bundesregierung.de/breg-en/news/speech-by-federal-chancellor-angela-merkel-at-the-49th-world-economic-forum-annual-meeting-in-davos-on-23-january-2019-1574188>

4. Harris, D, Contemporary Issues in Healthcare Law & Ethics (4th edition), (Chicago, Health Administration Press, 2014).

5. 551 P.2d 334 (Cal. 1976).

6. National Conference of State Legislatures, Mental Health Professionals' Duty to Warn (October 12, 2018). URL: <http://www.ncsl.org/research/health/mental-health-professionals-duty-to-warn.aspx>

7. Public Law No. 104–191 (1996).

8. Public Law No. 111–5, §§ 13401, 13404 (2009).

9. Terry, N, Health Privacy Is Difficult but Not Impossible in a Post-HIPAA Data-Driven World, *CHEST*, (2014), 146(3): 835–840.

10. Terry, N, Big Data Proxies and Health Privacy Exceptionalism, *Health Matrix*, (2014), 24(1): 65–108.

11. Ross, C, After 9/11, we gave up privacy for security. Will we make the same trade-off after Covid-19? *STAT*, (April 8, 2020). URL: <https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/>

12. 45 CFR §164.512(b)(1)(i).
13. HIPAA and COVID-19. URL: <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html>
14. COVID-19 and HIPAA: Disclosure to law enforcement, paramedics, other first responders and public health authorities. URL: <https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf>
15. 85 Federal Register 19392-93 (April 7, 2020).
16. 85 Federal Register 22024-05 (April 21, 2020).
17. McCoy, M *et al*, Prevalence of Third-Party Tracking on COVID-19 – Related Web Pages, *JAMA*, (October 13, 2020), 324(14):1462–1464.
18. McCoy, M, T Libert, & A Friedman, Online privacy loss: another Covid-19 aftershock, *STAT*, (September 30, 2020). URL: <https://www.statnews.com/2020/09/30/online-privacy-loss-another-covid-19-aftershock/>
19. New York Times Editorial Board, Privacy Cannot Be a Casualty of the Coronavirus, *New York Times*, (April 7, 2020), <https://www.nytimes.com/2020/04/07/opinion/digital-privacy-coronavirus.html>
20. Singer, N, and SH Choe, As Coronavirus Surveillance Escalates, Personal Privacy Plummets, *New York Times*, (April 17, 2020). URL: <https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>
21. De la Garza, A, Contact Tracing Apps Were Big Tech’s Best Idea for Fighting COVID-19. Why Haven’t They Helped? *TIME* (November 10, 2020). URL: <https://time.com/5905772/covid-19-contact-tracing-apps/>
22. Does a HIPAA covered entity that fulfills an individual’s request to transmit electronic protected health information (ePHI) to an application or other software (collectively “app”) bear liability under the HIPAA Privacy, Security, or Breach Notification Rules (HIPAA Rules) for the app’s use or disclosure of the health information it received? URL: <https://www.hhs.gov/hipaa/for-professionals/faq/3009/does-a-hipaa-covered-entity-bear-liability.html>
23. 45 CFR §160.103.
24. Fuller, T, How Much Should the Public Know About Who Has the Coronavirus? *New York Times*, (March 30, 2020). URL: <https://www.nytimes.com/2020/03/28/us/coronavirus-data-privacy.html>
25. Tahir, D, and M Ravindranath, How the coronavirus is upending medical privacy, *POLITICO*, (April 28, 2020). URL: <https://www.politico.com/news/2020/04/28/coronavirus-medical-privacy-217671>
26. Oppel, R, *et al*, The Fullest Look Yet at the Racial Inequity of Coronavirus, *New York Times*, (July 5, 2020). URL: <https://www.nytimes.com/interactive/2020/07/05/us/coronavirus-latinos-african-americans-cdc-data.html>
27. Public Law No. 104-191, Title II, Subtitle F, § 264 (c)(1) (1996).
28. Litman-Navarro, K, We Read 150 Privacy Policies. They Were an Incomprehensible Disaster, *New York Times*, (June 12, 2019). URL: <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>
29. Singer, N, What Does California’s New Data Privacy Law Mean? Nobody Agrees, *New York Times*, (December 29, 2019). URL: <https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html>
30. Hecht-Felella, L, and K Mueller-Hsia, Rating the Privacy Protections of State Covid-19 Tracking Apps, *BRENNAN CENTER FOR JUSTICE*, (November 5, 2020). URL: <https://www.brennancenter.org/our-work/research-reports/rating-privacy-protections-state-covid-19-tracking-apps>

31. Turow, J, Let's Retire the Phrase 'Privacy Policy' *New York Times*, (August 20, 2018). URL: <https://www.nytimes.com/2018/08/20/opinion/20Turow.html>

Дін М. Гарріс

*Доцент, кафедра охорони здоров'я та політики,
Школа глобального громадського здоров'я Гіллінга, Університет
Північної Кароліни в Чапел-Хілл, Сполучені Штати Америки;
бакалавр мистецтв Корнельського університету (1973);
доктор права юридичного факультету Університету Північної
Кароліни (1981); член Американської асоціації з охорони здоров'я;
член Європейської асоціації медичного права
dean_harris@unc.edu*

Законодавство США щодо конфіденційності у сфері охорони здоров'я: недостатньо ефективно за умов COVID-19

Висвітлено особливості правової охорони конфіденційності медичних даних і даних, пов'язаних з охороною здоров'я у США. Проаналізовано сферу застосування та приписи федеральних законів і законів штатів США, виокремлено проблемні аспекти захисту медичної таємниці. Порівняльна слабкість захисту конфіденційності США не обмежується медичною інформацією, а стосується багатьох видів персональних даних. Порівняно з багатьма іншими країнами США забезпечують нижчий рівень захисту конфіденційності медичної інформації, що набуває важливого значення в реаліях сьогодення, а саме за умов пандемії. Проаналізовано закони штатів США щодо збалансування приватних і публічних інтересів, а саме збереження недоторканності приватного життя особи, з одного боку, та сприяння розкриттю інформації для захисту громадськості – з іншого. Виокремлено слабкі сторони системи захисту конфіденційності США та проблеми у вирішенні важливих питань конфіденційності за умов пандемії COVID-19. Сформульовано практичні рекомендації щодо вирішення проблемних питань аналізованої сфери.

Ключові слова: конфіденційність; конфіденційність у сфері охорони здоров'я; закон щодо конфіденційності (HIPAA); COVID-19; законодавство США.

Стаття надійшла до редакції 11.11.2020

Прийнята до друку 01.12.2020