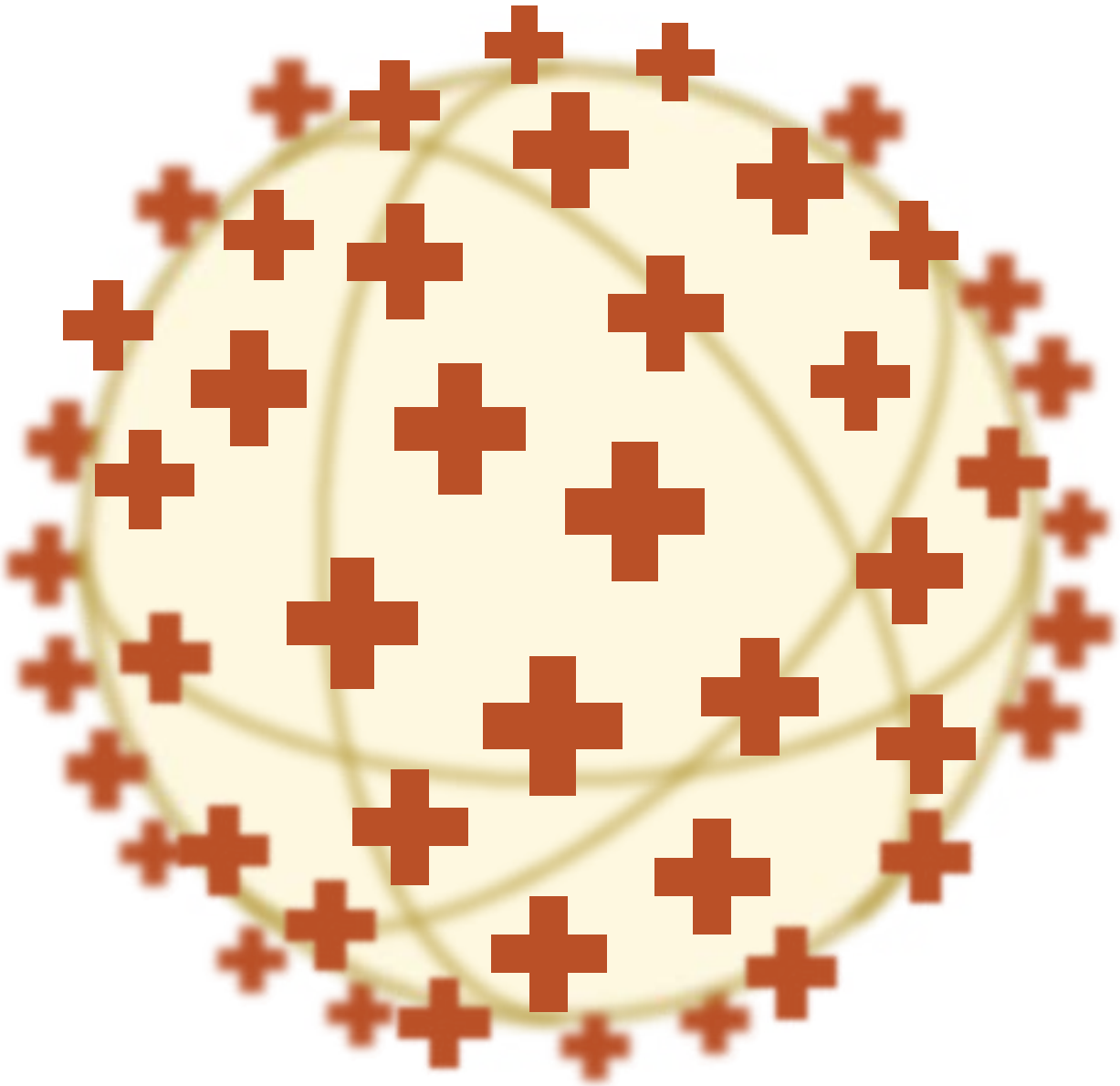
COVID-19 and HIPAA

HHS's Troubled Approach to Waiving Privacy and Security Rules for the Pandemic



By Robert Gellman and Pam Dixon

September 16, 2020

WORLD **PRIVACY** FORUM

About the Authors

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) He has written extensively on health privacy, de-identification, Fair Information Practices, and other privacy topics. Dixon and Gellman's writing collaborations include *A Patient's Guide to HIPAA*, as well as a reference book on privacy: *Online Privacy: A Reference Handbook,* as well as numerous and well-regarded privacy-focused research, articles, and policy analyses.

Pam Dixon is the founder and Executive Director of the World Privacy Forum. She is the author of eight books, hundreds of articles, and numerous privacy studies, including a landmark study on Medical Identity Theft study as well as India's Aadhaar biometric system, *A Failure to Do No Harm* (Nature Springer, 2018). She has testified before the U.S. Congress on consumer privacy issues as well as before federal agencies, as well as working internationally in OECD and developing jurisdictions.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group focused on the research and analysis of emerging and critically important privacy-related issues. The Forum was founded in 2003 and has published significant privacy research and policy studies in the area of health, online and technical, privacy, self-regulation, financial, identity, biometrics, and data brokers among other many areas. www.worldprivacyforum.org.

About this Report and Credits

Authors: Robert Gellman and Pam Dixon

Cover Illustration and Report Design: John Emerson

Publication date: September 16, 2020. Published at: www.worldprivacyforum.org

Version: 1.0

URL for report: https://www.worldprivacyforum.org/2020/09/covid-19-and-hipaa

Future version and updates can be found at worldprivacyforum.org.

The authors thank the experts and analysts who reviewed early drafts of this report, whose comments were invaluable.

Executive Summary

The COVID-19 pandemic strained the U.S. health ecosystem in numerous ways, including putting pressure on the HIPAA privacy and security rules. The Department of Health and Human Services adjusted the privacy and security rules for the pandemic through the use of statutory and administrative HIPAA waivers. While some of the adjustments are appropriate for the emergency circumstances, there are also some meaningful and potentially unwelcome privacy and security consequences. At an appropriate time, the use of HIPAA waivers as a response to health care emergencies needs a thorough review. This report sets out the facts, identifies the issues, and proposes a roadmap for change.

The Department of Health and Human Services (HHS) issued two types of HIPAA waivers during the pandemic: *statutory waivers* and *administrative waivers*. An analysis of these waivers, their consequence, and recommendations on how to proceed forward are the substance of this report. In March 2020, the Secretary of HHS initiated a set of *statutory* HIPAA waivers to respond to the national emergency that COVID-19 created. These emergency waivers utilized clear, pre-existing statutory authority. However, even though the Secretary's decision to issue these waivers was lawful and reasonable, questions remain whether the statute the Secretary relied upon needs revision.

The HHS Office of Civil Rights (OCR) took separate and later action to issue another set of *administrative* HIPAA waivers. The administrative waivers did not utilize clear statutory authority. Two of the OCR administrative waivers – one covering telehealth and one for Community-Based Testing Sites – responded to clear needs but still raise some concerns about their scope. A third administrative waiver – giving HIPAA business associates greater authority to use and disclose patient data without approval from the HIPAA covered entity that hired them – raises serious concerns about the breadth of the waiver and about the likelihood for misuse of patient data.

This report offers an analysis of existing laws and practices regarding both types of HIPAA COVID-19 waivers. The report recommends that, when the current emergency subsides, the Secretary of HHS review in a systematic way the privacy, security, and legal questions about all HIPAA waivers. The report further recommends that HHS prepare for future health emergencies with advance planning for HIPAA waiver practices. The report recommends that the National Committee on Vital and Health Statistics be tasked with the fact-finding and policy work needed to develop legislative and administrative recommendations for HIPAA waivers. Discussions about HIPAA waivers should involve all relevant stakeholders. Finally, once the Secretary completes a review of waiver authority, the report recommends that the US Congress reform the statutory HIPAA waiver rules.

I. Authority for Waiving HIPAA: Discussion of the Existing Statute

HIPAA waivers originated in 2004 when the Congress amended section 1135 of the Social Security Act to give the Secretary of Health and Human Services the express authority to waive a variety of health regulatory requirements during a national emergency.[1] Subsection (b) of that section has eight paragraphs detailing the scope of the Secretary's authority to temporarily waive or modify specified requirements of law for an "emergency area" during an "emergency period." The law addresses the HIPAA health privacy rule[2] by allowing waivers from these HIPAA requirements:

> (7) sanctions and penalties that arise from noncompliance with the following requirements (as promulgated under the authority of section 264(c) of the Health Insurance Portability and Accountability Act of 1996) –
>
> (A) section 164.510 of title 45, Code of Federal Regulations, relating to –
>
> (i) requirements to obtain a patient's agreement to speak with family members or friends; and
>
> (ii) the requirement to honor a request to opt out of the facility directory;
>
> (B) section 164.520 of such title, relating to the requirement to distribute a notice; or
>
> (C) section 164.522 of such title, relating to –
>
> (i) the patient's right to request privacy restrictions; and
>
> (ii) the patient's right to request confidential communications.[3]

---

1 Public Law 108–276, § 9, https://www.congress.gov/108/plaws/publ276/PLAW-108publ276.pdf.

2 The Health Insurance Portability and Accountability Act is a 1996 federal statute. Although many people associate HIPAA primarily with health privacy, the Act is much broader in scope. The part of the Act relevant to privacy directed the Department of Health and Human Services to write a health privacy rule. The original privacy rule took effect in April 2003. The HIPAA security rule, and other rules, came later. See 45 C.F.R. Parts 160, 162, and 164, https://www.ecfr.gov/cgi-bin/text-idx?SID=e3f580289bc5edd5f5db69cc1ce19479&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl.

3 42 U.S.C. § 1320b-5, https://www.law.cornell.edu/uscode/text/42/1320b-5. This section is section 1135 of the Social Security Act.

The relevant part of the statute provides:

> (b) Secretarial Authority To the extent necessary to accomplish the purpose specified in subsection (a), the Secretary is authorized, subject to the provisions of this section, to temporarily waive or modify the application of, with respect to health care items and services furnished by a health care provider (or classes of health care providers) in any emergency area (or portion of such an area) during any portion of an emergency period, the requirements of subchapters XVIII, XIX, or XXI, or any regulation thereunder (and the requirements of this subchapter other than this section, and regulations thereunder, insofar as they relate to such subchapters), pertaining to—
>
> ***
>
> (7) sanctions and penalties that arise from noncompliance with the following requirements (as promulgated under the authority of section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note)— [1]
>
> (A) section 164.510 of title 45, Code of Federal Regulations, relating to—
>
> (i) requirements to obtain a patient's agreement to speak with family members or friends; and
>
> (ii) the requirement to honor a request to opt out of the facility directory;

Under the statute, the statutory HIPAA waiver can last for 72 hours beginning upon implementation of a hospital disaster protocol.[4] The COVID-19 pandemic is not the first emergency for which the Secretary used this authority. The Secretary routinely invoked it over the years following hurricanes and other significant natural disasters.[5] Previous uses of the statutory waiver were typically limited in geographic scope, for example applying to a specific region, state, or county.

II. The COVID-19 HIPAA Waivers: The Basics

On March 13, 2020, the Secretary of HHS used Section 1135 to apply the statutorily authorized waivers during the COVID-19 national emergency.[6] The March 13 statutory waiver covered all five provisions identified in Section 1135(b)(7). This action conformed to the practice of previous emergency HIPAA waivers using the same Section 1135 authority.

(B) section 164.520 of such title, relating to the requirement to distribute a notice; or

(C) section 164.522 of such title, relating to—

(i) the patient's right to request privacy restrictions; and

(ii) the patient's right to request confidential communications.

The Congress amended this section of law several times during the COVID-19 emergency. Section 102 of Public Law 116-123 gave the Secretary of HHS authority to temporarily waive or modify application of certain Medicare requirements with respect to telehealth services furnished during certain emergency periods. https://www.govinfo.gov/link/plaw/116/public/123. Section 6010 of Public Law 116-127 clarified the Secretary's authority regarding Medicare telehealth services furnished during the COVID–19 emergency period. https://www.govinfo.gov/link/plaw/116/public/127. Neither amendment expanded the Secretary's waiver authority with respect to HIPAA.

4 The provision establishing the time limit and requiring a hospital disaster protocol is in Section 1135, but it appears in a paragraph with no section number that follows subsection (b)(8). The text provides:

> Insofar as the Secretary exercises authority under paragraph (6) with respect to individuals enrolled in a Medicare+Choice plan, to the extent possible given the circumstances, the Secretary shall reconcile payments made on behalf of such enrollees to ensure that the enrollees do not pay more than would be required had they received services from providers within the network of the plan and may reconcile payments to the organization offering the plan to ensure that such organization pays for services for which payment is included in the capitation payment it receives under part C of subchapter XVIII. A waiver or modification provided for under paragraph (3) or (7) shall only be in effect if such actions are taken in a manner that does not discriminate among individuals on the basis of their source of payment or of their ability to pay, and, except in the case of a waiver or modification to which the fifth sentence of this subsection applies, shall be limited to a 72-hour period beginning upon implementation of a hospital disaster protocol. A waiver or modification under such paragraph (7) shall be withdrawn after such period and the provider shall comply with the requirements under such paragraph for any patient still under the care of the provider. If a public health emergency described in subsection (g)(1)(B) involves a pandemic infectious disease (such as pandemic influenza), the duration of a waiver or modification under paragraph (3) shall be determined in accordance with subsection (e) as such subsection applies to public health emergencies.

It is difficult to parse this provision, particularly the reference in the sentence containing this language: "... except in the case of a waiver or modification to which the fifth sentence of this subsection applies, shall be limited to a 72-hour period beginning upon implementation of a hospital disaster protocol."

5 Secretary of Health and Human Services, Waiver or Modification of Requirements Under Section 1135 of the Social Security Act (March 13, 2020), https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

6 Secretary of Health and Human Services, Waiver or Modification of Requirements Under Section 1135 of the Social Security Act (March 13, 2020), https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

Following the Secretary's exercise of this authority, the Office of Civil Rights (OCR) at HHS – the office responsible for HIPAA rulemaking and enforcement – made further announcements related to the COVID-19 emergency and HIPAA. The effect was to create new waivers for additional provisions of the HIPAA rules.[7] (Again, for purposes of this report, the OCR waivers are the *administrative waivers*, in contrast to the Secretary's *statutory waivers* based on specific statutory authority.)

Telehealth waiver: On March 17, 2020, OCR announced that, effective immediately, it would exercise its enforcement discretion and would waive potential penalties for HIPAA violations against health care providers that serve patients through "everyday communications technologies" during the COVID-19 nationwide public health emergency.[8] This *Telehealth waiver* applies to "widely available communications apps, such as FaceTime or Skype, when used in good faith for any telehealth treatment or diagnostic purpose, regardless of whether the telehealth service is directly related to COVID-19."[9] OCR did not identify exactly which provisions of HIPAA the waiver covers.[10] HIPAA security rules require, among other things, a risk analysis and a risk assessment of the use of the technology[11] and consideration of the need for encryption.[12] The waiver allows use of telehealth facilities during the emergency without the need for these activities.

Business Associate waiver: On April 2, 2020, OCR announced that it would exercise its enforcement discretion and not impose penalties for violations of "certain provisions of the HIPAA Privacy Rule" against health care providers or their business associates for good faith uses and disclosures of protected health information (PHI)[13] by business associates for public health and health oversight activities during the COVID-19 nationwide public health emergency.[14] OCR said that it would not impose penalties against a business associate or covered entity under the Privacy Rule provisions 45 CFR 164.502(a)(3) [business associates may use or disclose PHI only as permitted or required by business associate contract]; 45 CFR 164.502(e)(2) [requirement for written business associate contract]; 45 CFR 164.504(e)(1) [activities required by covered entity if business associates breach contract]; and 45 CFR 164.504(e)(5) [applying contractual standards to subcontractors of business associates] if, and only if:

- The business associate makes a good faith use or disclosure of the covered entity's PHI for public

---

7 See Office of Civil Rights (HHS), *HIPAA, Civil Rights, and COVID-19*, https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html.

8 HHS Press Release, *OCR Announces Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (March 17, 2020), https://www.hhs.gov/about/news/2020/03/17/ocr-announces-notification-of-enforcement-discretion-for-telehealth-remote-communications-during-the-covid-19.html.

9 Office of Civil Rights (HHS*), Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (undated), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.

10 The announcement "encourages" providers "to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications." Id.

11 45 C.F.R. § 164.308(a).

12 Id. at § 164.312(a)(2)(iv).

13 What is PHI? HIPAA Questions, HHS (undated), https://www.hhs.gov/answers/hipaa/what-is-phi/index.html.

14 HHS Press Release, *OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency* (April 2, 2020), https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html.

health activities consistent with 45 CFR 164.512(b), or health oversight activities consistent with 45 CFR 164.512(d); and

- the business associate informs the covered entity within ten (10) calendar days after the use or disclosure occurs (or commences, with respect to uses or disclosures that will repeat over time).[15]

The announcement included the following footnote:

> Due to the public health emergency posed by COVID-19, the HHS Office for Civil Rights (OCR) is exercising its enforcement discretion under the conditions outlined herein. We believe that this guidance is a statement of agency policy not subject to the notice and comment requirements of the Administrative Procedure Act (APA). 5 U.S.C. 553(b)(A). OCR additionally finds that, even if this guidance were subject to the public participation provisions of the APA, prior notice and comment for this guidance is impracticable, and there is good cause to issue this guidance without prior public comment and without a delayed effective date. 5 U.S.C. 553(b)(B) & (d)(3).[16]

Community Based Testing Sites waiver: On April 9, 2020, OCR announced a third administrative waiver. The April 9 waiver covers "the good faith participation in the operation of COVID-19 testing sites during the COVID-19 nationwide public health emergency."[17] The focus of the waiver is on Community-Based Testing Sites (CBTS).[18] The scope of the waiver is not stated or entirely clear, but it appears to cover all provisions of all HIPAA privacy, security, and breach notification rules. OCR's explanation about the scope of the waiver states:

> OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with regulatory requirements under the HIPAA Rules against covered health care providers and their business associates in connection with the good faith participation in the operation of a CBTS during the COVID-19 nationwide public health emergency as described below.[19]

Note that OCR refers simply and broadly to "regulatory requirements under the HIPAA Rules…in connection with good faith participation in the operation of a CBTS." No stated part of the HIPAA rules appears outside the scope of this waiver.

---

15 HHS, *Notification of Enforcement Discretion under HIPAA to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities in Response to COVID-19* (April 2, 2020), https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html. See 85 Federal Register 19392 (April 7, 2020), https://www.federalregister.gov/documents/2020/04/07/2020-07268/enforcement-discretion-under-hipaa-to-allow-uses-and-disclosures-of-protected-health-information-by.

16 Id. at 85 Federal Register 19392 (April 7, 2020).

17 HHS, Press Release, *OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency*, https://www.hhs.gov/about/news/2020/04/09/ocr-announces-notification-enforcement-discretion-community-based-testing-sites-during-covid-19.html.

18 A CBTS includes mobile, drive-through, or walk-up sites that only provide COVID-19 specimen collection or testing services to the public. Id.

19 HHS, *Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS) During the COVID-19 Nationwide Public Health Emergency* (April 9, 2020), https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf. The announcement includes this admonition: "OCR encourages covered health care providers participating in the good faith operation of a CBTS to implement reasonable safeguards to protect the privacy and security of individuals' PHI.".

III. Are OCR's Administrative HIPAA Waivers Legal?

There is no question about the legality of the March 13 waiver by the Secretary of HHS. Section 1135 clearly authorizes that waiver, and the emergency created by the COVID-19 virus is undisputed.

There is, however, some question about the legal basis for the other three waivers of HIPAA enforcement discretion by OCR. These waivers include the *Telehealth waiver*, the *Business Associate waiver*, and the *Community-Based Testing Sites waiver* discussed in Section II.

The purpose here is not to undertake a complete review of the complex question of agency discretionary authority or to consider the ability of the courts to review the exercise of that type of administrative discretion. It is also not the purpose to question the nature of the COVID-19 emergency. Finally, it is not the purpose here to question the motivation of HHS's waiver choices. Rather, the goal here is to offer a straightforward outline of an argument that the OCR administrative waivers may lack a firm legal basis without attempting to reach a conclusion other than to suggest that there is an issue about the legality of any HIPAA waivers other than those specifically authorized by statute. In a later section, this paper questions whether all of the administrative waivers are as clear, limited, and narrow as possible.

The core of the problem is that section 1135 of the Social Security Act gives the Secretary specific and limited authority to waive sanctions and penalties that arise from noncompliance with five specific provisions of the HIPAA privacy rule. That statute could have given the Secretary broad or general authority to waive any or all HIPAA rules during an emergency or to waive sanctions and penalties for any or all HIPAA rules, but it did not. The statute is quite specific in the authority granted to the Secretary.

The legal maxim potentially applicable here is *Expressio Unius Est Exclusio Alterius* (the expression of one thing is the exclusion of the other).[20] By giving the Secretary express authority to waive enforcement of five specific provisions of HIPAA, the statute arguably denies the Secretary authority to waive enforcement of other provisions.

Further, by March 27, 2020, congressional action taken in response to the COVID-19 emergency did not include authority for HIPAA waivers other than those already provided in Section 1135. In the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act), the Congress included the following language in a section titled *Guidance on Protected Health Information*:

> SEC. 3224. GUIDANCE ON PROTECTED HEALTH INFORMATION. Not later than 180 days after the date of enactment of this Act, the Secretary of Health and Human Services shall issue guidance on the sharing of patients' protected health information pursuant to section 160.103 of title 45, Code of Federal Regulations (or any successor regulations) during the public health emergency declared by the Secretary of Health and Human Services under section 319 of the Public Health Service Act (42 U.S.C. 247d) with respect to COVID–19, during the emergency involving Federal primary responsibility determined to exist by the President under section 501(b) of the Robert T. Stafford Disaster Relief and Emergency 19, and during the national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.) with respect to COVID–19. Such guidance shall include information on compliance with the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note) and applicable policies, including such policies that may come into effect during such emergencies.[21]

20 Duhaime's Law Dictionary, http://www.duhaime.org/LegalDictionary/E/ExpressioUniusEstExclusioAlterius.aspx.

21 Public Law 116-136, Act of March 27, 2020, https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

This section calls on the HHS Secretary to issue new guidance on the sharing the PHI during the COVID-19 public health emergency. The last sentence emphasizes "guidance on compliance with [HIPAA regulations], including such policies that may come into effect during such emergencies." This language suggests that the Congress thought that any existing problems could be solved with additional guidance. The term *guidance* is noteworthy. *Guidance* is a term that is well defined and understood.[22]

The congressional action in the CARES Act came after the March 13 statutory HIPAA waiver by the Secretary, but before OCR issued any HIPAA administrative waivers. While the Congress did direct the Secretary to issue guidance on the sharing of PHI during the emergency, the Congress did not give the Secretary any additional HIPAA waiver authority in the CARES Act.

The Congress clearly decided to make some adjustments in confidentiality law in the emergency legislation. The CARES Act makes legislative changes affecting the law regulating the confidentiality and disclosure of records relating to substance use disorder.[23] Yet the law includes nothing that requires modification of the HIPAA privacy and security rules. In addition, the CARES Act also includes numerous waivers of other laws.[24] Arguably, the Congress did not add to the Secretary's waiver authority on the grounds that the Secretary already had all necessary waiver authority. Yet the Secretary also has unlimited authority to issue guidance, but the Congress issued directions for more – but largely unspecified – guidance about HIPAA. In the end, the CARES Act does not resolve or directly address the scope of the Secretary's waiver authority. It is always difficult to make judgments on the basis of what actions the Congress did *not* take. Still, there is nothing suggesting the need for or support for HIPAA waivers beyond those already specifically authorized by statute.

Generally, agencies have considerable authority to undertake, or to decline to undertake, enforcement of statutes within their jurisdiction. The exercise of that authority raises many questions relating to resources, unfairness, consistency, discrimination, and more. A recent report commissioned by the Administrative Conference of the United States (ACUS) on the general subject of administrative nonenforcement activities defines the nonenforcement issues thusly:

> The challenge presented by nonenforcement is easy to state but hard to solve. As a general matter, agencies have a great deal of discretion whether to enforce legal provisions. And like many types of administrative discretion, nonenforcement can be used for laudable purposes. Because resources are finite, it is impossible for agencies to investigate—much less bring enforcement actions against—every violation of statutory or regulatory law. Nor would inflexible enforcement always be desirable. Sometimes generally applicable laws are a poor fit for a particular situation: "'It is impossible for any general law to foresee and provide for all possible cases that may arise; and therefore an inflexible adherence to it, in every instance, might frequently be the cause of very great injustice.'" Yet at the same time, again as with other forms of discretion, agency discretion regarding nonenforcement can be problematic. Indeed, "a central principle of administrative law is (or at least should be) that discretion can be dangerous." Even leaving aside weighty constitutional concerns about the President's duty to faithfully execute the law

22 See Office of Management and Budget, Final Bulletin for Agency Good Guidance Practices, 72 Federal Register 3432 (Jan. 25, 2007), https://www.govinfo.gov/content/pkg/FR-2007-01-25/pdf/E7-1066.pdf. HHS is familiar with the OMB guidance bulletin, and discusses guidance subject to the bulletin on its website, https://www.hhs.gov/regulations/find-rules-by-operating-division/guidance-documents.html.

23 Id. at § 3221 (amending 42 U.S.C. 290dd–2).

24 A search of the law for the word *waiver* found 129 matches. See the complete suite of HIPAA Administrative Simplification Regulations at 45 CFR Part 160, Part 162, and Part 164, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html.

> (which are beyond the scope of this Report), nonenforcement may encourage the appearance or perhaps even reality of unfairness and irregularity, for instance when an agency decides to waive requirements for some but not all regulated parties or where the result of nonenforcement is that a potential beneficiary of the administrative scheme finds itself out of luck. **The challenge therefore is to strike the proper balance between regulatory flexibility, on one hand, and evenhanded, non-arbitrary administration of the law on the other**.[25]

The ACUS report addresses many aspects of agency nonenforcement, as well as questions surrounding the availability of judicial review of nonenforcement decisions. There can be a fine line between an agency's administratively-announced nonenforcement policy, and an actual change in a regulation that requires formal notice and comment. Emergency circumstances may factor into the analysis, and the existence of an emergency due to COVID-19 is undisputed here.

The ACUS report also summarizes court cases that emphasize a presumption of non-reviewability of agency nonenforcement actions by the courts, but the courts recognize some exceptions to the presumption.[26] Thus, despite any questions that arise about the legality of the OCR waivers, it is possible that the courts would decline to consider a challenge.

Attempts to analyze the legal questions about HIPAA waiver authority here could go on at great length with arguments on both sides. In the end, however, it is not possible to offer any firm conclusions. It is sufficient for current purposes to suggest that legitimate questions exist about the wisdom of the waiver authority, and that the uncertainty about the legality of HIPAA administrative waivers is sufficient to recommend that the Congress reconsider how much authority the Secretary should have to waive provisions of the HIPAA rules. Later in this document, there are specific suggestions about reviewing the waivers specifically identified in Section 1135 as well as other HIPAA requirements. Any debate might be influenced by questions and recommendations offered later in this report.

IV. Other Issues Raised by the COVID-19 HIPAA Waivers

A. The Secretary's Statutory Waiver

The Section 1135 HIPAA waiver provision originated in Public Law 108-276, *Project Bioshield Act of 2004*. The title of Section 9 of that Act is "Authority of the Secretary of Health and Human Services During National Emergencies."[27] The law has a limited legislative history, and nothing in it discusses Section 9.

---

25 Aaron L. Nielson, WAIVERS, EXEMPTIONS, AND PROSECUTORIAL DISCRETION: AN EXAMINATION OF AGENCY NONENFORCEMENT PRACTICES (Final Report for the Administrative Conference of the United States 2017) (emphasis added), https://www.acus.gov/report/regulatory-waivers-and-exemptions-final-report.

26 A leading case is Heckler v. Chaney, 470 U.S. 821 (1985), https://supreme.justia.com/cases/federal/us/470/821/. The Supreme Court held that an agency's decision not to take enforcement action is presumed immune from judicial review under the Administrative Procedure Act. Of some interest is the concurrence of Mr. Justice William Brennan. Brennan "identified a series of circumstances where the general principle of unreviewability of agency inaction may not block judicial review: (1) When an agency "flatly claims" that it is without authority to address particular conduct – when in fact, it has precisely that authority – the nonreviewability prohibition does not apply; and (2) If an agency engages in a "pattern of nonenforcement" or a refusal to enforce a rule that is "lawfully promulgated and still in effect" or undertakes action that is otherwise unconstitutional or illegal (for example accepting a bribe in exchange for inaction) the nonreviewability premise can be overcome." Popper, McKee, Varona, Harter, Niles, and Pasquale, Administrative Law: A Contemporary Approach, 3rd ed. 2016.

27 https://www.congress.gov/108/plaws/publ276/PLAW-108publ276.pdf.

To restate the statutory provision, during a national emergency, the Secretary of HHS can waive sanctions and penalties that might be imposed for noncompliance with these five requirements in the HIPAA privacy rule:

1. The requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 CFR 164.510(b)),
2. the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a)),
3. the requirement to distribute a notice of privacy practices (45 CFR 164.520),
4. the patient's right to request privacy restrictions (45 CFR 164.522(a)), and
5. the patient's right to request confidential communications (45 CFR 164.522(b)).[28]

The Secretary's first known use of the waiver authority occurred on September 4, 2005, in response to Hurricane Katrina.[29] In numerous subsequent hurricanes and other national emergencies, the Secretary invoked the same waiver of HIPAA rules.

During the COVID-19 crisis, the first step toward invoking the statutory HIPAA waivers came on January 31, 2020, when the Secretary announced his determination that a public health emergency existed because of the "2019 Novel Coronavirus (2019-nCoV)" and that the emergency existed nationwide since January 27, 2020. Then on March 13, 2020, as discussed, the Secretary used the authority under Section 1135 of the Social Security Act to apply the existing statutorily authorized HIPAA waiver during the COVID-19 emergency.[30] This action conformed to those taken previously when HHS invoked emergency HIPAA waivers typically in response to hurricanes, floods, fires, and natural disasters.

Specifically, paragraph (7) of the March 13, 2020 announcement provides for waiver of all five HIPAA requirements allowed under Section 1135.

The actual text of the March 13 HIPAA waiver is:

> Pursuant to Section 1135(b)(7) of the Act, I hereby waive sanctions and penalties arising from noncompliance with the following provisions of the HIPAA privacy regulations: (a) the requirements to obtain a patient's agreement to speak with family members or friends or to honor a patient's request to opt out of the facility directory (as set forth in 45 C.F.R. § 164.510); (b) the requirement to distribute a notice of privacy practices (as set forth in 45 C.F.R. § 164.520); and (c) the patient's right to request privacy restrictions or confidential communications (as set forth in 45 C.F.R. § 164.522); but in each case, only with respect to hospitals in the designated geographic area that have hospital disaster protocols in operation during the time the waiver is in effect.

---

28 See HHS FAQ 1068, *Is the HIPAA Privacy Rule suspended during a national or public health emergency?* https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html.

29 See Congressional Research Service, Hurricane Katrina: HIPAA Privacy and Electronic Health Records of Evacuees (Jan. 23, 2007), https://www.everycrsreport.com/reports/RS22310.html. A list of other waivers under Section 1135 is at https://www.phe.gov/emergency/news/healthactions/section1135/Pages/default.aspx.

30 Secretary of Health and Human Services, Waiver or Modification of Requirements Under Section 1135 of the Social Security Act (March 13, 2020), https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx. In the same document, the Secretary also announced other waivers and modifications of existing requirements unrelated to HIPAA. Those actions are not the subject of this analysis.

The last clause provides that the waiver applies in specific circumstances, namely:

> ..."only with respect to **hospitals** in the **designated geographic area** that have **hospital disaster protocols in operation** during the time the waiver is in effect." [*note: emphasis added*]

This is the same language HHS Secretaries have used when they announced previous HIPAA waivers. For emergencies based on natural disasters, the limitation to hospitals within specific and narrow designated geographic areas places appropriate bounds on the scope of the waiver.

However, the use of the statutory public health emergency waiver authority for HIPAA in response to COVID-19 presents several novel circumstances.

- First, the COVID-19 public health emergency is nationwide.
- Second, the emergency is likely to continue for a significant period of time, perhaps for a year or more. At this stage, it is not predictable when the emergency might end.
- Third, since the emergency is nationwide, it is not clear that limiting the waivers to "hospitals…that have hospital disaster protocols in operation" is sufficient to meet all COVID-19 needs of health care providers. It is possible that HHS used the existing formulaic language when invoking the HIPAA waiver without considering its application to the COVID-19 circumstances.

The broad application of statutory waivers to all patients during natural disasters may follow from the apparent goal of simplifying administrative activities in emergency circumstances. As invoked for the COVID-19 emergency, the statutory waiver is not limited to COVID-19 patients, although there may not always be a practical way to distinguish between patients based on diagnosis. The 72 hours allowed by the statutory waiver limits unwelcome consequences that may result.[31]

One may question whether a time-limited waiver that may work for natural disasters should apply for a longer term (or at all) to a nationwide emergency caused by a pandemic. One may also question whether application of some or all waivers to hospitals makes sense for the COVID-19, because hospitals are not the only health care providers responding to the emergency. In addition, the need for all of the statutory waivers to be available in all emergency circumstances needs to be revisited. In short, whether the statutory waivers are or were properly tuned to the need is the core issue to consider. Some relevant arguments on all sides follow.

- Is a 72-hour waiver meaningful, even in local natural disasters? If a health care provider in the immediate aftermath of a tornado failed to comply with the HIPAA notice requirements, it is unlikely that HHS would take any action for the failure. Whether the period of the waiver should be zero (i.e., no waiver) or longer than 72 hours is an open question.
- If the statutory waivers are time-limited for natural disasters, would a different time limit for some or all of the five types of statutory HIPAA waivers make sense for a pandemic?
- Will the waivers that make sense for natural disasters necessarily also make sense for nationwide pandemics or other foreseeable emergencies?
- In any circumstance, should waivers apply only to hospitals and not to other health care providers?
- The first statutory waiver provision allows for waiver of the requirement to obtain a patient's agreement to speak with family members or friends involved in the patient's care (45 CFR 164.510(b)). As

31 Nothing requires hospitals covered by a waiver to deny all patients the rights waived. The concern, however, is that many hospitals will take the path of least resistance and use the waivers broadly.

it stands, the existing regulation gives health care providers considerable flexibility in making professional judgments about disclosures to family or caregivers. Is more flexibility really needed for emergencies or is the current provision already adequate to the need?

- The second statutory waiver provision allows for waiver of the requirement to honor a request to opt out of the facility directory (45 CFR 164.510(a)). The case for this waiver may be stronger in natural disasters, but the argument for it may not extend to longer-term emergencies.
- The third statutory waiver provision allows for waiver of the requirement to distribute a notice of privacy practices (45 CFR 164.520)). Here too, the case for this waiver may be stronger in the aftermath of a natural disaster than over a longer-term period such as a years-long pandemic.
- The fourth statutory waiver provision allows for waiver of the patient's right to request privacy restrictions (45 CFR 164.522(a)). Frankly, this right imposes no obligation on a HIPAA covered entity to acknowledge or even respond to a patient request so that it makes little difference whether a patient can use exercise the "right" or not. The World Privacy Forum explains this at greater length in the Patient's Guide to HIPAA, FAQ 52, *Why is the Right to Request Restrictions Almost Meaningless*?[32]
- The fifth statutory waiver provision allows for waiver of the patient's right to request confidential communications (45 CFR 164.522(b)). For some patients, this right may be so important at all times that its absence may be life-threatening. Consider the victim of domestic violence who does not want a bill or notice to go to their batterer. A youth obtaining treatment for sexual activity may also feel threatened in various ways if information about that treatment goes to a parent. Certainly, any long-term suspension of this right is highly questionable.
- Are there other provisions of the HIPAA privacy and security rules for which a waiver in emergencies would be appropriate? The administrative waiver for telehealth is an example of a waiver that might have been foreseen and planned for in advance. Are there more like this?
- HIPAA waivers cover all patients. That may make sense following natural disasters. But for the current pandemic, many patients receiving treatment do not have COVID-19, and it may be that waiving their privacy rights is inappropriate. The interests of those patients must, of course, be balanced against the overall needs of health care operations during emergencies. This issue becomes more pressing if a waiver lasts more than 72 hours.

It is a necessary premise that all rights provided under the HIPAA rules remain important and should be restored at the earliest opportunity. All patients, including COVID-19 patients, deserve the rights granted by the rules when the need for the waiver diminishes. As suggested above, it is not necessarily a foregone conclusion that all five provisions should always be always be waived for the same length of time in every emergency.

32 World Privacy Forum, *A Patient's Guide to HIPAA* at FAQ 52, https://www.worldprivacyforum.org/2019/03/hipaa/#c89.

Concluding Assessment of the Statutory HIPAA Waiver:

Under the circumstances at the time of announcement of the statutory waivers, it is understandable that HHS followed the "traditional" way of invoking the HIPAA waivers. It would be unduly harsh to judge the Secretary differently for taking the same action as in the past, especially because questions about the exercise of that authority did not arise.

Still, there is a need to balance all of the concerns raised, including administrative issues that arise when adjusting the waivers. Identification of bright lines may not be possible in all cases, so judgment is essential when making determinations. HHS could do more here to sort through these issues in advance of the next emergency and make recommendations to the Congress for amending Section 1135. The Secretary's use of the statutory waiver passes muster, but needs attention.

B. The OCR Administrative Waiver for Telehealth

OCR's judgment under the emergency circumstances created by the COVID-19 crisis that a clear, broad, and immediate waiver was appropriate to allow for use of telehealth activities was a fair professional judgment. The Telehealth waiver usefully distinguished somewhat between communications facilities, ruling out the use by health care providers of public facing facilities (some by name).

Certainly, the importance of telehealth to the practice of medicine during the pandemic emergency is not in dispute here. There are, however, some issues about the communications facilities the waiver allows. The waiver applies to "widely available communications apps, such as FaceTime or Skype, when used in good faith for any telehealth treatment or diagnostic purpose, regardless of whether the telehealth service is directly related to COVID-19." The extent to which these widely used communications facilities have adequate privacy and security controls in place received considerable after-the-fact press attention[33] and the providers of the facilities made some improvements addressing the concerns.

Nor is there a reason to question coverage of the waiver for all telehealth treatment or diagnostic purposes regardless of COVID-19 status, or the application of the waiver to all health care providers. The pandemic presented a major disruption to traditional health care and many other activities. The requirement of *good faith* has little additional meaning for most health care encounters, but in this context, it seems largely unobjectionable. A *good faith* test applies in multiple instances in existing HIPAA rules.

It is not clear, however, what provisions of the HIPAA privacy, security or data breach rules the waiver covers. It is apparent that many, if not most, HIPAA covered entities would not have the ability to conduct in real time the security reviews and assessments otherwise required for the use of new technologies. The need to allow for telehealth activities was immediate, so a waiver of at least some parts of the HIPAA security rule seems reasonable. How far does the waiver extend? OCR stated that it would not "impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth." This statement is not as clear as it should have been.

It is not clear, for example, if the waiver covers data breach obligations. There may be no reason to waive requirements to report and mitigate a telehealth data breach, especially given the known security issues with

33 See, e.g., Allen St. John, *It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too* (April 30, 2020) (Consumer Reports), https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/.

the telehealth services approved by the waiver. Similar questions could be raised about other HIPAA requirements.

Emergency circumstances may justify much, and perhaps even all, of the ambiguity in the Telehealth waiver. It is a guess that the pandemic caught OCR flatfooted and without any advance preparation. It is nevertheless justifiable to criticize OCR for not anticipating the possibility of a pandemic (or other types of emergency circumstances) and not planning for the need to relax HIPAA rules. A Telehealth waiver could have been prepared in advance with a more specific description of the waiver.

Indeed, is advisable for OCR to identify in advance a range of possible needs for HIPAA waivers, to solicit public comment for any proposals, and to make informed adjustments to waivers that meet both the circumstances and the needs of HIPAA covered entities. To realize that it is possible to anticipate, one need only look at Section 1135 of the Social Security Act, where the Congress identified and authorized specific HIPAA waivers in advance. Clearly, however, those waivers are inadequate for a pandemic. That the Congress did a limited job of providing for waivers does not excuse OCR for not doing better.

Concluding Assessment of the Telehealth Waiver:

Providing immediate support for telehealth activities during the pandemic was important, and that need largely overcame the real and significant concerns about the potential breadth of the waiver. However, there will eventually be a need to "clean up" after the pandemic. There may be lingering and variable privacy and security consequences for stakeholders related to the Telehealth waiver, depending on which telehealth technologies they used. Overall, the waiver was necessary, but it could have been limited in useful ways.

C. The OCR Administrative Waiver for Business Associate Activities

The need for the Business Associate waiver is much less apparent than the need for the Telehealth waiver. OCR offered the following justification for the Business Associate waiver:

> This Notification was issued to support Federal public health authorities and health oversight agencies, like the Centers for Disease Control and Prevention (CDC) and Centers for Medicare and Medicaid Services (CMS), state and local health departments, and state emergency operations centers who need access to COVID-19 related data, including PHI. The HIPAA Privacy Rule already permits covered entities to provide this data, and today's announcement now permits business associates to also share this data without risk of a HIPAA penalty.
>
> "The CDC, CMS, and state and local health departments need quick access to COVID-19 related health data to fight this pandemic," said Roger Severino, OCR Director. "Granting HIPAA business associates greater freedom to cooperate and exchange information with public health and oversight agencies can help flatten the curve and potentially save lives," Severino added.[34]

This explanation is not convincing. HIPAA business associates process PHI under the terms of their contracts with covered entities. Unless specifically authorized by their covered entities to share data with public health

34 HHS Press Release, *OCR Announces Notification of Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency* (April 2, 2020), https://www.hhs.gov/about/news/2020/04/02/ocr-announces-notification-of-enforcement-discretion.html.

authorities or health oversight agencies, business associates generally have no prior relationship with or prior history of conveying PHI to those agencies and authorities. Even if a public health authority or health oversight agency has a history of interacting with a particular health care provider, it may not have a relationship with the provider's business associates or necessarily have any way to authenticate either the business associates themselves or any data they provide. Any transfer of PHI from a business associate, no matter how well intentioned, could raise questions about the value, accuracy, and authenticity of any particular disclosure. Could a recipient really rely on data relayed directly from business associates? Would a public health recipient face new problems of identifying, authenticating, and integrating data from dozens, hundreds, or thousands of business associates?

The grant of authority given by the waiver to business associates gives the impression of an unfocused "do something" response in the hope that it might help somehow. The waiver raises a series of significant questions about different aspects of the authority given to business associates and the consequences of actions by business associates.

On the positive side, the Business Associate waiver is specific, covering three identified provisions of the privacy rule relating to business associate contracts and activities. The Business Associate waiver also establishes a good faith standard as did the Telehealth waiver.

Less positively, the Business Associate waiver includes a requirement for notice by a business associate to its covered entity within ten days after a use or disclosure occurs or, in the case of continuing activities, ten days after commencement of the use or disclosure.

What types of business associates can use the authority in the OCR waiver?

A HIPAA covered entity may have many business associates. Examples include: electronic health record (EHR) providers, paper shredding services; medical billing and coding services; website hosting and management services; cloud service providers; answering services; mobile app providers; software as a service providers; texting services; messaging services; practice management software providers; various technology companies; printing and mailing services; transportation services; consultants; accountants; lawyers; and others.

Business associates for many health care providers include a wide variety of organizations large and small. Some business associates are well-known technology companies as well as other service providers who support health care activities and many other activities, including the processing of consumer data by commercial data brokers and marketers. Some business associates provide cloud services that cover all of a HIPAA covered entity's health record processing activities. The level of risk depends on how business associate contracts limit the actions allowed by business associates. A question the pandemic has put before the Congress and policymakers is the risk that business associates could take PHI in their possession, combine it with other data they have about consumers, and use it directly to contact for the "public health activity" of locating and contracting patients deemed to be at great risk for COVID-19.

Many business associates have no experience or expertise in public health, research, data analysis, or other activities of relevance to responding to the 2020 coronavirus pandemic. Yet all have the same broad authority under the OCR waiver to decide for themselves whether and how to make use of the information they process on behalf of a covered entity. A service that collects paper patient records for shredding from a hospital has the same authority under the waiver as a company that maintains EHRs for that hospital. Both the shredding company and the EHR provider have the same ability under the OCR waiver to use patient records or to disclose them "for public health and health oversight activities." There is no requirement that a business associate either have or rely upon professional expertise in making decisions about data use and disclosure for public health or health oversight purposes.

What new privacy risks result from the Business Associate Waiver?

Protected Health Information transferred to a public health authority or health oversight agency is not protected by the HIPAA privacy, security, or business associate rules. When a HIPAA covered entity discloses PHI to anyone who is not a HIPAA covered entity, HIPAA no longer applies to the PHI. This has always been true for disclosures by covered entities. HIPAA rules do not follow the data.

While some public health agencies operate in part as HIPAA covered entities, many have functions that are not subject to HIPAA. It would be unusual for a health oversight agency to function as a HIPAA covered entity. As a result, identifiable health information transferred to a public health agency or a health oversight agency may not be covered by any privacy law in the hands of the recipient.[35] The information could be used and further disclosed without any privacy controls or restrictions. But the terms of routine transfers by HIPAA covered entities to public health or health oversight agencies are more likely to be established as distinguished from those resulting from ad hoc disclosures by a business associate.

The Business Associate waiver does not even limit disclosures *to* public health authorities or *to* health oversight agencies. A business associate could apparently disclose patient records to anyone it believed "in good faith" could make a contribution to the emergency. A commercial data broker that profits from collecting and disclosing consumer information could conceivably be an intermediary by offering to collect and merge data for public health analysis. A business associate could make a good faith disclosure to a company, not knowing the company was posing as an intermediary that turned out to be a Medicare fraudster who promised to use the data for a public health purpose.

A distinguishing feature of health care providers is that they operate under medical ethics principles independent of HIPAA. So, even when HIPAA authorizes disclosures, a health care provider would presumably apply those principles when deciding how to disclose PHI in response to the COVID-19 emergency. However, a business associate or health oversight agency is not necessarily subject to the same or any formal ethical principles and therefore might act without the restraint that we expect from health care providers. In short, allowing business associates and public health agencies to make their own decisions about the benefits and consequences of PHI disclosures raises significant new risks.

Why does the waiver allow uses and disclosures by health oversight agencies?

Health oversight agencies include auditors, civil, and criminal investigators, and others whose functions do not involve treatment, public health activities, or research. For example, the Medicare Inspector General is a health oversight agency whose functions include criminal investigations. States may have similar offices. It is not immediately apparent why disclosure to any or all of these health oversight agencies would be particularly helpful to responding to the pandemic. Few are likely to have relevant expertise.

Why the delay in notice to the covered entity?

The waiver allows a business associate to use or disclose information for the specified purposes without any advance notice to or consultation with the covered entity that hired the business associate in the first place.

---

35 In the case of federal agencies, personally identifiable data would likely be subject to the Privacy Act of 1974, 5 U.S.C. § 552a, https://www.law.cornell.edu/uscode/text/5/552a. The Act only applies to information retrieved by personal identifier, and this may not always be the case with data used for public health or health oversight purposes. For example, some public health data may be highly aggregated and not contain PHI or identifiers. PHI disclosed to state and local agencies would likely be subject to state and local privacy laws, but the laws vary from state to state, and some states have no applicable privacy laws.

Notice to the covered entity is not required for ten calendar days. Thus, a business associate that maintains patient records for a major health care institution could disclose *all* of those records on June 3 and not provide notice until June 16. Given the ease with which electronic records can be transferred, and given that a large health provider such as a national or regional hospital chain could have millions of records, a ten-day delay is a long period of time to have PHI in transit without knowledge of that activity.

The waiver could have provided for a shorter period; required concurrent or advance consultation; or given the covered entity authority to veto any proposed use or disclosure. There is some evidence that not all health care providers are comfortable allowing business associates to independently decide about the sharing of patient data.[36]

When would the Business Associate Waiver not work?

A business associate can only use PHI in accordance with a business associate agreement and in accordance with the HIPAA rules. The HIPAA security rule establishes an addressable specification that a covered entity or business associate "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate."[37] While this specification does not mandate use of encryption, an addressable specification must be assessed to determine if it is a reasonable and appropriate safeguard.[38]

The Business Associate waiver did not waive the requirement to assess encryption, and a business associate subject to the rule and making a new disclosure of PHI to a new recipient might and probably should conclude that an assessment of the need for encryption was necessary. For this reason, a prudent business associate might be unable to disclose data quickly and might decline to make a disclosure at all. If a business associate took the time to make the assessment, it would also have time to consult with and obtain approval from the covered entity whose data was at issue.

Another reason the waiver may have no effect is because OCR cannot abrogate contractual limits imposed by covered entities on business associates. OCR waived enforcement of the HIPAA requirement that "business associate may use or disclose PHI only as permitted or required by business associate contract." However, a covered entity can still enforce its contract, and OCR has no say in unregulated contractual matters between a covered entity and its business associates. A business associate contract that limits use and disclosure remains in force as a matter of contract law, even if OCR chooses not to enforce the restriction in the HIPAA rule.

Further, covered entities, seeing what OCR did with the Business Associate waiver, will likely revise their contracts at the next opportunity to flatly prohibit uses and disclosures not expressly approved by the covered entities, to require advance notice, or to give the covered entities veto power. It is probable – but unknown – that many business associate contracts written by covered entities already contain language with some of these restrictions. Much depends on the relative size and importance of covered entities and business associates. In some cases, larger business associates impose their own terms on smaller covered entities.

Finally, the Business Associate waiver does not affect any restrictions under state law. In general, HIPAA[39]

---

36 Meeting, National Committee on Vital and Health Statistics 45 (March 25, 2020) (Comments of Committee Member Jacki Monson), https://ncvhs.hhs.gov/wp-content/uploads/2020/05/Transcript-Full-Committee-Meeting-March-25-2020.pdf.

37 45 C.F.R. § 164.312(e)(2)(ii).

38 Id. at § 164.306(d)(3)(i).

39 Pub. L. 104–191, title II, § 264, Aug. 21, 1996, 110 Stat. 2033, https://www.law.cornell.edu/uscode/text/42/1320d-2.

allows state laws that provide more stringent stronger privacy protections to remain in place.[40] If a state law prevents a business associate from using or disclosing PHI as provided by the Business Associate waiver, the waiver does not override that restriction.

Concluding Assessment of the Business Associate Waiver:

OCR issued a Business Associate waiver with significant problems. This waiver does not pass muster. The OCR Business Associate waiver is poorly limited, fails to define the problem that it sought to address, exposes patient records to new forms of privacy invasion, and does not consider the actual effects in the real world. If a business associate casually uses the authority that the waiver grants, there is a chance that PHI protected under HIPAA will leak into the wrong hands. It is impossible here to assess the reasons why OCR issued the waiver, but the reasoning and justification for the waiver does not rise to the same level of importance or necessity of other HIPAA waivers. In the long run, the effect of the badly considered Business Associate waiver may be that covered entities will use their business associate agreements to prevent OCR from doing anything similar in the future.

OCR failed to uphold its responsibilities to patients and to the health care system when it issued the Business Associate waiver. This waiver in particular is more likely to be injurious to patients and to patient privacy than helpful in responding to the pandemic. If grades were awarded for the quality, necessity, and responsibility of waivers, the Business Associate waiver would receive a failing grade.

D. The OCR Community-Based Testing Sites HIPAA Waiver

The OCR Community-Based Testing Sites (CBTS) waiver applies to mobile, drive-through, and walk-up sites that only provide COVID-19 specimen collection or testing services to the public. These services may be provided by health care providers covered by the HIPAA health privacy and security rules, including some large pharmacy chains, and their business associates. The waiver allows HIPAA covered entities and business associates to avoid compliance with any and all HIPAA rules in connection with the "good faith" participation in the operation of a Community Based Testing Site during the COVID-19 public health emergency.

The press release for the CBTS waiver included this justification:

> This Notification was issued to support certain covered health care providers, including some large pharmacy chains, and their business associates that may choose to participate in the operation of a Community Based-Testing Site (CBTS), which includes mobile, drive-through, or walk-up sites that only provide COVID-19 specimen collection or testing services to the public.
>
> "We are taking extraordinary action to help the growth of mobile testing sites so more people can get tested quickly and safely," said Roger Severino, OCR Director.[41]

The waiver applies to all health care providers and business associates that participate in the operation of a CBTS. It appears the waiver covers *all* provisions of HIPAA without restriction. This is understandable to some extent, but there are many provisions of HIPAA for which a waiver is not needed or appropriate. Further, it is not clear if the waiver of all HIPAA requirements applies only to the CBTS sites themselves, or if

40 42 U.S.C. § 1320d-2 note; 45 C.F.R. § 160.202 (definition of *more stringent*).

41 HHS Press Release, OCR Announces Notification of Enforcement Discretion for Community-Based Testing Sites During the COVID-19 Nationwide Public Health Emergency (April 9, 2020,) https://www.hhs.gov/about/news/2020/04/09/ocr-announces-notification-enforcement-discretion-community-based-testing-sites-during-covid-19.html.

they apply broadly to all operations of any covered entity or business associate that participates in a CBTS.

Some COVID-19 specimen collection or testing services may not be provided by HIPAA covered entities, and these sites are not subject to the HIPAA privacy and security rules. These sites may not be covered by any privacy rules at all. The waiver has no effect on these sites.

To its credit, OCR suggested specific reasonable safeguards that a CBTS should undertake. These are:

- Using and disclosing only the minimum PHI necessary except when disclosing PHI for treatment.
- Setting up canopies or similar opaque barriers at a CBTS to provide some privacy to individuals during the collection of samples.
- Controlling foot and car traffic to create adequate distancing at the point of service to minimize the ability of persons to see or overhear screening interactions at a CBTS. (A six-foot distance would serve this purpose as well as supporting recommended social distancing measures to minimize the risk of spreading COVID-19.)
- Establishing a "buffer zone" to prevent members of the media or public from observing or filming individuals who approach a CBTS, and posting signs prohibiting filming.
- Using secure technology at a CBTS to record and transmit electronic PHI.
- Posting a Notice of Privacy Practices (NPP), or information about how to find the NPP online, if applicable, in a place that is readily viewable by individuals who approach a CBTS.[42]

What privacy risks does the Community Based Testing Sites HIPAA Waiver raise?

The April 9 HIPAA waiver introduces privacy and trust challenges, with the potential to create problems specifically relating to the public trust of Community Based Testing Sites.

All HIPAA privacy and security rules are waived, not just selected rules. The lack of limits opens the door to new privacy consequences for patients. The waiver to too broad and unfocused. Luckily, in some circumstances, state health privacy laws will continue in force so that some violations of disclosure limitations and other bedrock privacy rules may remain in force. Standard principles of medical ethics may also provide some protections for privacy. Each CBTS must figure out the applicability of other law on its own.

Privacy buffer zones are not required. Those getting tested may not want to have neighbors, passersby, the news media, or other onlookers know or record their visit to the testing site or the fact of their testing. The waiver does encourage health care providers to maintain a "buffer zone" to prevent members of the media or the public from observing or filming individuals who approach a CBTS, and to post signs prohibiting filming. A better drafted waiver might have required a buffer zone unless significantly impractical.

The waiver "encourages" health care providers to use and disclose only the minimum identifiable health data necessary as provided by the HIPAA privacy rule. However, a health care provider that chooses to allow public viewing of the tests or even to announce test results in a manner that allows the public or press to hear the results would not be sanctioned as a result of the waiver. The "good faith" standard is inadequate, and the waiver of all use and disclosure rules is simply unnecessary.

---

42 Department of Health and Human Services, Enforcement Discretion Regarding COVID-19 Community-Based Testing Sites (CBTS) (announced April 9, 2020), https://www.hhs.gov/sites/default/files/notification-enforcement-discretion-community-based-testing-sites.pdf.

Concluding Assessment of the CBTS Waiver:

The need for testing is undisputed, but the waiver could have been clearer and more limited. OCR should have expressly stated that the waiver only covered activities at CBTS sites and not to unrelated activities of a covered entity or business associate. In addition, the waiver should have covered only necessary parts of the HIPAA rules. There is no need, for example, to waive all the restrictions on use and disclosure that do not relate to CBTS activities. There are questions as well about not applying security rules to the waiver. The waiver met a need, but it could have been narrower in scope.

V. Preparing for the Future

In time, the COVID-19 emergency will end. In time, other public health emergencies will arise, some familiar and some new. The experience presented by the COVID-19, in particular the nationwide application of the health emergency and the length of the emergency, calls for a reassessment of the content of existing HIPAA waivers, statutory and administrative, and of the process by which HHS develops and adopts HIPAA waivers.

Many things in law and regulation will eventually change as a result of the COVID-19 pandemic. The scope of the Secretary's statutory authority to waive HIPAA rules belongs on that list. So does the ability of OCR to issue administrative HIPAA waivers. These waiver matters need not be the first thing on that list nor the last, but there is nevertheless work to be done.

A. Tasks for HHS

The most important change needed for HIPAA waiver authority is advanced planning. HHS should:

1. Review the existing statutory authority and the need for clearer statutory authority.
2. Assess the effect of and need for all HIPAA waivers (statutory and administrative) in order to determine if the same waivers are likely to be needed in the future.
3. Seek comment from all relevant stakeholders in the health care system to ascertain their views and their needs.
4. Develop and draft specific prospective waivers that might be needed under predictable circumstances and seek comment from stakeholders.
5. Adjust the HIPAA rules if appropriate to avoid the need for reliance on waivers.
6. Make suitable recommendations to the Congress for legislation on waiver authority. However, HHS should not seek unrestricted waiver authority.

B. A Process Forward

To make progress, it will be necessary for HHS to work with all stakeholders, including providers, patients, public health authorities, privacy experts, and others. An important and well-respected multistakeholder statutory advisory committee at HHS already exists; this is the National Committee on Vital and Health Statistics (NCVHS), whose members have expertise in a wide range of health and health data activities. The NCVHS is a crucial resource to utilize in finding a careful middle ground.[43] Importantly, NCVHS has a subcommittee on Privacy and Confidentiality.

The Secretary should ask the NCVHS to do the fact-finding and assessments suggested here. Recommendations from the Committee to the Secretary could form the basis for legislative proposals; propose adjustments to HIPAA rules; and provide drafts of possible HIPAA waivers for use in predictable circumstances in the future, including time or other limits on waivers. The Committee could -- and should -- conduct public hearings or other consultations in order to solicit views from stakeholders. The Committee could also provide continuing oversight of HIPAA waivers as needed in the future.

The development of better HIPAA waiver policies and standards should await fact-finding and consultation with all relevant stakeholders. Nevertheless, some ideas can be offered now for consideration by policy makers.

1. Prepare for past and future emergencies: Reconsideration of how well past waivers worked will provide some insight into how to adjust the waiver process and substance. Identifying other possible emergencies will help to prepare better for the future. Possibilities include a different type of pandemic; systemic and long-term hacking of major health care computers, networks, and payment systems; major financial failures in the health care industry and related industries; part of the United States becoming uninhabitable on a long term basis; invasion of the United States by a foreign power; and collision with a comet.[44]
2. Identify developments likely to require changes to the HIPAA rules rather than waivers. Changes to HIPAA rules are always possible through the usual rulemaking process, and that process can take years. Operating under the experience of some waivers may identify the need for rule changes, and it may be useful to consider how to manage moving from waiver to rule once an emergency ends.
3. Prepare a "shelf waiver" process. The Securities and Exchange Commission allows companies to file "shelf registrations" for the issuance of securities in the future.[45] The process minimizes both administrative preparation and cost while providing significant flexibility to companies. The same idea could apply to waivers prepared through an advance and public policy process. HHS could predict future needs for waivers under different circumstances, ask stakeholders to help draft the specifics of appropriate waivers, and then put the waivers "on the shelf" to await the need. The

---

43 42 U.S.C. § 242k(k), https://www.law.cornell.edu/uscode/text/42/242k. In the interest of full disclosure, one of the authors of this report (Gellman) served a term as a member of the NCVHS, and both authors testified before the Committee on several occasions.

44 See, e.g., "Deutsche Bank: 33% Chance of 'Massive' Disaster Worse Than COVID", NewsmaxFinance (July 9, 2020), https://www.newsmax.com/finance/streettalk/deutsche-bank-massive-disaster-covid/2020/06/19/id/973059/. Possibilities identified by the bank include major influenza pandemic killing more than two million people; a globally catastrophic volcanic eruption; a major solar flare; or a global war,

45 17 C.F.R. § 230.415, https://www.ecfr.gov/cgi-bin/text-idx?SID=eb7386953dbe591d7eb1eab26cce4463&node=se17.3.230_1415&rgn=div8.

Congress might approve the "shelf waiver" process and give HHS more ability to use waivers that went through that process. This would be a better alternative than giving HHS a blank check to waive any HIPAA rule as it sees fit.

4. It seems likely that different types of waivers (including allowing for variations in the scope and length of applicability) may be needed for different emergencies. The statutory waivers that last for 72 hours may not be useful in pandemic emergencies.

5. No matter how good advance planning may be, there still may be circumstances that are unforeseen. It may be appropriate to give HHS time-limited authority in these cases. One approach would grant authority under a high standard (e.g., "essential to protect public health") with a limitation that a waiver can only remain until the Congress has an opportunity to review HHS actions. The rapid congressional response to COVID-19 shows that prompt action by the Congress is possible, although it will be prudent to make sure that process does not triumph over substantive needs in emergencies. A waiver for unforeseen circumstances might remain in place unless ratified by the Congress within two months.

6. Require HHS to consult with and obtain approval from other federal or state agencies and from health care institutions. This should be an absolute requirement for advance waiver planning. There still might be a role for seeking broader approval in unforeseen circumstances. HHS could be required to seek approval from a selection of state public health authorities, from the NCVHS, from HHS components other than OCR, or from selected health care institutions most affected by the circumstances that generated the need for a waiver.

7. To the extent that waivers are mere guidance, the waivers may be rescinded by a subsequent administration. In theory, those who took actions relying on the waivers might be in legal jeopardy if there is a later determination that the waivers were inappropriate or unlawful. Some attention should be paid to the risks undertaken to those who rely on waivers. Clearer statutory authority could resolve these concerns.

8. There will come a time when the COVID-19 waivers are no longer needed. The Secretary needs to consider the transition from having waivers to not having waivers. For example, it seems likely that as a result of the experience with the current pandemic, telehealth will remain as a much more routine part of medicine than before. Yet HHS cannot turn off the waiver and expect HIPAA covered entities to complete overnight all appropriate tasks connected with continuing telehealth activities. With the emergency behind us, health care providers can and should be required to undertake the necessary security assessments for telehealth. There may be other tasks under the security rules as well. However, there is likely to be a need for a transition period once the COVID-19 emergency ends. Some needed assessments of telehealth facilities might be done by HHS for covered entities rather than leaving each covered entity to undertake the same assessment of the same technologies.

C. Tasks for the Congress

The Congress needs to rethink the statutory waiver authority allowed under Section 1135 of the Social Security Act. A revised waiver statute can and should clear up the legality of the administrative waivers discussed above. Assuming that HHS acts in the next few years, the time for congressional action should be after the Secretary completes a review of waiver authority. If HHS does not act, then the Congress should either direct action or take the matter in its own hands.

The existing authority given to the Secretary of HHS is perhaps both too broad and too narrow at the same

time. Some of the existing provisions that the Secretary can waive under the statute probably continue to make sense in a short-term emergency. For example, waiving the notice requirement may be justifiable for administrative reasons following a natural disaster. However, the provision allowing an individual to ask for confidential communication protects a vital interest for those who need it. Emergency or not, there may be no reason to allow health care providers to deny categorically a request from a teenager to protect information about sexual activities from a parent or to honor a request from a victim of domestic violence to not share information with a batterer. Certainly, any waiver of that provision should be as short-term as possible.

It is not the goal here to make final judgments about the authority that the Secretary should have to waive provisions of HIPAA. A good thing about the existing waiver law is that it is specific and limited. Giving the Secretary unrestricted authority to waive any or all provisions of HIPAA would be a poor choice, especially seeing how poorly the Office of Civil Rights acted during the COVID-19 emergency. Of course, a problem with limited authority is the risk that the statute will not foresee all possible needs. There is clearly a dilemma here, and more thought about a solution is both appropriate and necessary. One possibility is that there may be a need to distinguish between types of emergencies and the length of time that waivers may remain in place.