

*This HHS-approved document is being submitted to the Office of the Federal Register (OFR) for publication and has not yet been placed on public display or published in the Federal Register. This document may vary slightly from the published document if minor editorial changes are made during the OFR review process. The document published in the Federal Register is the official HHS-approved document.**

**Individuals using assistive technology may not be able to fully access information in this document. For assistance, please contact the Office for Civil Rights at (800) 368-1019 or (800) 537-7697 (TDD).*

Billing Code: 4153-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

45 CFR Parts 160 and 164

Enforcement Discretion Regarding Online or Web-Based Scheduling Applications for the Scheduling of Individual Appointments for COVID-19 Vaccination during the COVID-19 Nationwide Public Health Emergency

AGENCY: Office of the Secretary, HHS.

ACTION: Notification of Enforcement Discretion.

SUMMARY: This Notification is to inform the public that the Department of Health and Human Services (HHS) is exercising its discretion in how it applies the Privacy, Security, and Breach Notification Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act (“HIPAA Rules”). As a matter of enforcement discretion, the HHS Office for Civil Rights (OCR) will not impose penalties for noncompliance with regulatory requirements under the HIPAA Rules against covered health care providers or their business associates in connection with the good faith use of online or web-based scheduling applications for the scheduling of individual appointments for COVID-19 vaccinations during the COVID-19 nationwide public health emergency.

DATES: This Notification of Enforcement Discretion is effective immediately, but will have retroactive effect to December 11, 2020, and will remain in effect until the Secretary of HHS determines that the public health emergency no longer exists, or upon the expiration date of the public health emergency, including any extensions (as determined by 42 U.S.C. 247d),¹ whichever occurs first.

FOR FURTHER INFORMATION CONTACT: Rachel Seeger at (202) 619-0403 or (800) 537-7697 (TDD).

SUPPLEMENTARY INFORMATION: HHS is informing the public that it is exercising its discretion in how it applies the Privacy, Security, and Breach Notification Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)² and the Health Information Technology for Economic and Clinical Health (HITECH) Act³ (“HIPAA Rules”) during the nationwide public health emergency declared by the Secretary of HHS.⁴

I. Background

¹ Public Health Emergency Determination issued by HHS Secretary, pursuant to Section 319 of the Public Health Service Act, on January 31, 2020, with retroactive effective date of January 27, 2020. The public health emergency determination was renewed most recently on January 7, 2021, with an effective date of January 21, 2021.

<https://www.phe.gov/emergency/news/healthactions/phe/Pages/covid19-07Jan2021.aspx>. For more information, see <https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx>.

² Pub. L. 104-191, 100 Stat. 2548 (August 21, 1996). 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)(3)(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)(3)(B) & (d)(3).

³ Title XIII of the American Recovery and Reinvestment Act, Pub. L. 111-5, 123 Stat. 226 (February 17, 2009).

⁴ See Determination that a Public Health Emergency Exists by the HHS Secretary, pursuant to Section 319 of the Public Health Service Act (January 31, 2020), *available at* <https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx> (Determination of January 31, 2020). See also Renewal of Determination That a Public Health Emergency Exists (January 7, 2021), *available at* <https://www.phe.gov/emergency/news/healthactions/phe/Pages/covid19-07Jan2021.aspx>

The Office for Civil Rights (OCR) at HHS is responsible for enforcing certain regulations issued under HIPAA and the HITECH Act, to protect the privacy and security of protected health information (PHI), namely the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”).

During the COVID-19 national emergency,⁵ which also constitutes a nationwide public health emergency,⁶ certain covered health care providers,⁷ including some large pharmacy chains and public health authorities,⁸ or their business associates acting for or on behalf of such providers, may choose to use online or web-based scheduling applications (collectively, “WBSAs”) for the limited purpose of scheduling individual appointments for COVID-19 vaccination. For the purposes of this Notification, a WBSA is a non-public facing online or web-based application that provides scheduling of individual appointments for services in connection with large-scale COVID-19 vaccination. “Non-public facing” means that a WBSA, as a default, allows only the intended parties (*e.g.*, a covered health care provider, the individual or personal representative scheduling the appointment, and a WBSA workforce member, if needed to provide technical support) to access data created, received, maintained, or transmitted by the WBSA. For the purposes of this Notification, a WBSA does not include appointment scheduling

⁵ See Presidential Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak (Mar 13, 2020), *available at* <https://www.whitehouse.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/>.

⁶ Determination of Jan 31, 2020.

⁷ See 45 CFR 160.103 (definition of “covered entity”).

⁸ See 45 CFR 164.501 (definition of “public health authority”). The HIPAA Rules only apply to a public health authority if it is a HIPAA covered entity or business associate. For example, a county health department that administers a health plan, or provides health care services for which it conducts standard electronic transactions (*e.g.*, checking eligibility for coverage, billing insurance), is a HIPAA covered entity. A public health authority that does not meet the definition of a covered entity or business associate is not subject to the HIPAA Rules. *See also* OCR FAQ, “Are state, county or local health departments required to comply with the HIPAA Privacy Rule?” <https://www.hhs.gov/hipaa/for-professionals/faq/358/are-state-county-or-local-health-departments-required-to-comply-with-hipaa/index.html>.

technology that connects directly to electronic health records (EHR) systems used by covered entities.

The HIPAA Privacy Rule permits a business associate of a HIPAA covered entity to use and disclose PHI to conduct certain activities or functions on behalf of the covered entity, or provide certain services to or for the covered entity, but only pursuant to the explicit terms of a business associate contract or other written agreement or arrangement under 45 CFR 164.502(e)(2) (collectively, “business associate agreement” or BAA), or as required by law. During the COVID-19 public health emergency, covered health care providers need to quickly schedule large numbers of individuals for appointments for COVID-19 vaccination and may use WBSAs to do so. Some of these applications, and the manner in which HIPAA covered health care providers or their business associates use the applications, may not fully comply with the requirements of the HIPAA Rules. Additionally, the vendors of such applications may not be aware that HIPAA covered health care providers are using their products to create, receive, maintain, or transmit electronic protected health information (ePHI), and that a WBSA vendor may, as a result, meet the definition of business associate under the HIPAA Rules.⁹

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, including WBSA vendors meeting the definition of a business associate, in connection with the good faith use of a WBSA for scheduling appointments for individuals for COVID-19 vaccination during the COVID-19 nationwide public health emergency, as described below.

II. Who/What is covered by this Notification?

⁹ See 45 CFR 160.103 (definition of “electronic protected health information”).

This Notification applies to all HIPAA covered health care providers and their business associates¹⁰ when such entities are, in good faith, using WBSAs to schedule individual appointments for COVID-19 vaccination.

This Notification also applies to all vendors of WBSAs whose technology is being used by a covered health care provider or its business associate to schedule individuals to receive a COVID-19 vaccine. OCR will exercise enforcement discretion with regard to WBSA vendors regardless of whether the WBSA vendor has actual or constructive knowledge that it meets the definition of a business associate under the HIPAA Rules as described in this Notification.

III. What are reasonable safeguards that covered health care providers and their business associates should consider implementing?

OCR encourages covered health care providers and their business associates using WBSAs in good faith for the scheduling of individual appointments for COVID-19 vaccination to implement reasonable safeguards to protect the privacy and security of individuals' PHI. OCR recommends that covered health care providers and their business associates consider the following recommended reasonable safeguards:

- Using and disclosing only the minimum PHI necessary for the purpose (*e.g.*, an individual's name and phone number may be the minimum necessary PHI for scheduling the appointment).
- Using encryption technology to protect PHI.
- Enabling all available privacy settings (*e.g.*, adjusting WSBA calendar display settings, as needed, to hide names or show only individuals' initials instead of full names on calendar screens).

¹⁰ See 45 CFR 160.103 (definition of "business associate").

- Ensuring that storage of any PHI (including metadata that constitutes PHI) by the vendor is only temporary (*e.g.*, the PHI is returned to the covered health care provider or destroyed as soon as practicable, but no later than 30 days after the appointment).¹¹
- Ensuring the WBSA vendor does not use or disclose ePHI in a manner that is inconsistent with the HIPAA Rules (*e.g.*, does not engage in the sale of ePHI¹² collected from individuals using the WBSA to schedule a COVID-19 vaccination).

Although covered health care providers and business associates are encouraged to implement these reasonable safeguards when using a WBSA to schedule individuals for appointments for COVID-19 vaccination, OCR will exercise its enforcement discretion and not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers or their business associates in connection with the good faith provision of COVID-19 vaccination during the COVID–19 nationwide public health emergency. Failure to implement the recommended reasonable safeguards above will not, in itself, cause OCR to determine that a covered health care provider or its business associate failed to act in good faith for purposes of this Notification.

Covered health care providers and their business associates that seek additional privacy protections for ePHI collected while using WBSAs are encouraged to use application vendors that represent that their WBSAs support compliance with the HIPAA Rules and that the vendors will enter into BAAs in connection with the use of their WBSAs.

Note: OCR does not endorse, certify, or recommend specific technology, software, applications, or products.

¹¹ Once the WBSA vendor securely returns or destroys the ePHI (as determined by its arrangements with the covered health care provider), the WBSA vendor is no longer a business associate to that covered health care provider.

¹² See 45 CFR 164.502(a)(5)(B)(2).

IV. Who/What is not covered under this Notification?

This Notification does not apply to activities of a covered health care provider and its business associates other than the scheduling of COVID-19 vaccinations. Other activities, such as the handling of PHI unrelated to the scheduling of COVID-19 vaccinations, are not included within the scope of this exercise of enforcement discretion. Potential HIPAA penalties still apply to all other HIPAA-covered operations of the covered health care provider and its business associates, unless otherwise stated by OCR.¹³

Additionally, this Notification does not apply to a covered health care provider or business associate when it fails to act in good faith. For example, OCR will not consider a covered health care provider or business associate to be acting in good faith with respect to the use of a WBSA for the scheduling of individual appointments for COVID-19 vaccination where the covered health care provider or business associate uses a WBSA:

- Whose terms of service prohibit the use of the WBSA for scheduling health care services or state that the WBSA may sell personal information that it collects.
- To conduct services other than scheduling appointments for COVID-19 vaccination (*e.g.*, to determine individuals' eligibility for COVID-19 vaccination).
- Without reasonable security safeguards (*e.g.*, access controls) to prevent the PHI from being readily accessed or viewed by unauthorized persons.
- To screen individuals for COVID-19 prior to individuals' in-person health care visits.

V. Collection of Information Requirements

This Notification of Enforcement Discretion creates no legal obligations and no legal rights. Because this notice imposes no information collection requirements, it need not be

¹³ OCR's Notifications of Enforcement Discretion and other materials relating to the COVID-19 public health emergency are available at <https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html>.

reviewed by the Office of Management and Budget under the Paperwork Reduction Act of 1995
(44 U.S.C. 3501 *et seq.*).

Dated: January 19, 2021