

THE JOURNAL OF FEDERAL AGENCY ACTION

Editor's Note: Time to Modernize Regulations

Victoria Prussen Spears

Federal Deposit Insurance Corporation Should Modernize Its Regulations on Confidential Supervisory Information

Dustin N. Nofziger and Pinchus D. Raice

Securities and Exchange Commission Permits Mandatory Arbitration Clauses in Registration Statements

Eric Forni, Melanie E. Walker, Richard Zelichov, and Yan Grinblat

Federal Trade Commission Abandons Noncompete Rule and Signals Plan to Target Unlawful Noncompete Agreements Through Individual Enforcement Actions

Mark E. Terman, Martin S. Chester, Kathy L. Osborn, Anna M. Behrmann, Lauren W. Linderman, Erik A. Mosvick, Kristin M. Halsing, Jillian S.B. Lukacik, Charles F. Knapp, and Anna E. Sallstrom

Federal Communications Commission Proposes Modernization of Space and Earth Station Licensing

Julie Kearney, Emma Marion, and Caitlin Barbas

Food and Drug Administration Final Guidance on Alternatives to Inspections Signals Evolving Approach to Facility Oversight

Howard Sklamberg, Elizabeth Trentacost, and Ada Ohanenye

Hamstrung National Labor Relations Board Does Not Want States Grabbing Labor Power: Agency Challenges New York Law as More States Consider Similar Path

Eleanor F. Miller, Joshua D. Nadreau, and Alexander A. Wheatley

D.C. Circuit Recognizes Seven County's Abrogation of Sabal Trail

Deidre G. Duncan and Nathan R. Menard

HHS-OIG and ASTP Jointly Issue Information Blocking Enforcement Alert

Liz Lindquist, Lisa M. Re, and Jami Vibbert

Executive Order Seeks to Reshape Federal Grantmaking Policy and Oversight

Daniel Ramish, Jonathan Shaffer, and Jonathan Keller

The Journal of Federal Agency Action

Volume 4, No. 1 | January–February 2026

- 5 Editor's Note: Time to Modernize Regulations**
Victoria Prussen Spears
- 9 Federal Deposit Insurance Corporation Should Modernize Its Regulations on Confidential Supervisory Information**
Dustin N. Nofziger and Pinchus D. Raice
- 17 Securities and Exchange Commission Permits Mandatory Arbitration Clauses in Registration Statements**
Eric Forni, Melanie E. Walker, Richard Zelichov, and Yan Grinblat
- 23 Federal Trade Commission Abandons Noncompete Rule and Signals Plan to Target Unlawful Noncompete Agreements Through Individual Enforcement Actions**
Mark E. Terman, Martin S. Chester, Kathy L. Osborn, Anna M. Behrmann, Lauren W. Linderman, Erik A. Mosvick, Kristin M. Halsing, Jillian S.B. Lukacik, Charles F. Knapp, and Anna E. Sallstrom
- 29 Federal Communications Commission Proposes Modernization of Space and Earth Station Licensing**
Julie Kearney, Emma Marion, and Caitlin Barbas
- 35 Food and Drug Administration Final Guidance on Alternatives to Inspections Signals Evolving Approach to Facility Oversight**
Howard Sklamberg, Elizabeth Trentacost, and Ada Ohanenye
- 41 Hamstrung National Labor Relations Board Does Not Want States Grabbing Labor Power: Agency Challenges New York Law as More States Consider Similar Path**
Eleanor F. Miller, Joshua D. Nadreau, and Alexander A. Wheatley
- 47 D.C. Circuit Recognizes Seven County's Abrogation of Sabal Trail**
Deidre G. Duncan and Nathan R. Menard
- 53 HHS-OIG and ASTP Jointly Issue Information Blocking Enforcement Alert**
Liz Lindquist, Lisa M. Re, and Jami Vibbert
- 59 Executive Order Seeks to Reshape Federal Grantmaking Policy and Oversight**
Daniel Ramish, Jonathan Shaffer, and Jonathan Keller

EDITOR-IN-CHIEF

Steven A. Meyerowitz

President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Lynn E. Calkins

Partner, Holland & Knight LLP

Washington, D.C.

Helaine I. Fingold

Member, Epstein Becker & Green, P.C.

Baltimore

Nancy A. Fischer

Partner, Pillsbury Winthrop Shaw Pittman LLP

Washington, D.C.

Bethany J. Hills

Partner, DLA Piper LLP (US)

New York

Phil Lookadoo

Partner, Haynes and Boone, LLP

Washington, D.C.

Michelle A. Mantine

Partner, Reed Smith LLP

Pittsburgh

Ryan J. Strasser

Partner, Troutman Pepper Hamilton Sanders LLP

Richmond & Washington, D.C.

THE JOURNAL OF FEDERAL AGENCY ACTION (ISSN 2834-8818 (online)) at \$495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2026 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff

Publisher: David Nayer

Production Editor: Sharon D. Ray

Cover Art Design: Morgan Morrisette Wright and Sharon D. Ray

This journal's cover includes a photo of Washington D.C.'s Metro Center underground station. The Metro's distinctive coffered and vaulted ceilings were designed by Harry Weese in 1969. They are one of the United States' most iconic examples of the brutalist design style often associated with federal administrative buildings. The photographer is by XH_S on Unsplash, used with permission.

Cite this publication as:

The Journal of Federal Agency Action (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2026 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005

<https://www.fastcase.com/>

POSTMASTER: Send address changes to THE JOURNAL OF FEDERAL AGENCY ACTION, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in federal agency actions.

This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at
202.999.4777

For questions or Sales and Customer Service:

Customer Service

Available 8 a.m.–8 p.m. Eastern Time

866.773.2782 (phone)

support@fastcase.com (email)

Sales

202.999.4777 (phone)

sales@fastcase.com (email)

ISSN 2834-8796 (print)

ISSN 2834-8818 (online)

HHS-OIG and ASTP Jointly Issue Information Blocking Enforcement Alert

Liz Lindquist, Lisa M. Re, and Jami Vibbert*

In this article, the authors explain that recent federal actions signal an imminent uptick in federal scrutiny of compliance with the 21st Century Cures Act's information access rules.

The U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG) and Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP) recently jointly issued an alert (the Enforcement Alert) signaling, after an extended period of inaction, the federal government's intent to begin enforcing the information blocking regulations adopted under the 21st Century Cures Act (the Cures Act).

The Enforcement Alert followed an announcement the day before, via press release, by HHS Secretary Robert F. Kennedy Jr. that information blocking enforcement is a priority for the Trump administration.¹ Specifically, HHS described the press release as “a warning to actors still engaging in information blocking to come into compliance with the rules governing the flow of patient information” and encouraged stakeholders to report alleged information blocking to HHS-OIG's hotline.²

Taken together, these developments show the close coordination between HHS-OIG, ASTP, and HHS leadership with respect to information blocking matters. While HHS may continue information blocking education, it will also leverage enforcement to maximize compliance. The information blocking enforcement announcement is part of a broader push for greater healthcare data sharing. This past summer, the White House convened a meeting of technology leaders to encourage seamless data sharing for care coordination and create patient-centric digital health tools. The Office of Civil Rights affirmed an expansive definition of “treatment,” within the meaning of the Health Insurance Portability

and Accountability Act (HIPAA), when opining that a healthcare provider may disclose protected information, without consent, to participants in value-based care arrangements. This new initiative should also be viewed in the broader context of continued interest by the U.S. Department of Justice, HHS-OIG, and the relator's bar on health information technology security.³

Accordingly, in the near term, regulated entities should consider prioritizing related risk assessments and mitigation efforts as part of their compliance program activities to keep abreast of the evolving landscape.

What Is Information Blocking?

The Cures Act, enacted in 2016, generally prohibits information blocking by healthcare providers, certified health information technology (IT) developers, and health information networks and exchanges (HIN/HIEs) (collectively, regulated entities) unless the conduct falls within a statutory exception. The Cures Act also granted HHS-OIG authority to pursue penalties against actors who engage in information blocking.

“Information blocking” refers to practices that are likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception, and that:

- If conducted by a certified health IT developer or HIN/HIE, the developer or HIN/HIE knows, or should know, are likely to interfere with access, exchange, or use of EHI;
- If conducted by a healthcare provider, the provider knows are unreasonable and likely to interfere with access, exchange, or use of EHI.

Why Now?

On July 3, 2023, HHS-OIG issued a final rule with an effective date of September 1, 2023 (the 2023 Final Rule) to implement its authority under the Cures Act to investigate claims of information blocking and assess civil monetary penalties of up to \$1 million per information blocking violation (subject to inflation adjustments) by a certified health IT developer or an HIN/HIE. A “violation” is

defined in the 2023 Final Rule as a practice (i.e., an act or omission) that constitutes information blocking.⁴ A determination regarding what constitutes a “practice” will be made by HHS-OIG on a case-by-case basis per the particular facts and circumstances.⁵

In an example provided in the preamble to the 2023 Final Rule, HHS-OIG indicated that the enactment of a policy that establishes an information blocking practice is one violation, and each instance of enforcing that policy would constitute a separate violation. In such situations, CMPs could potentially add up to much more than \$1 million. HHS-OIG also indicated that it would consider factors such as the nature and extent of harm caused by the specific incident of information blocking, the number of patients and providers implicated and affected, and how long the information blocking lasted. Finally, developers with products certified by HHS’s Office of the National Coordinator could have their certifications terminated as a result of information blocking violations.⁶

On July 1, 2024, HHS issued a final rule (the 2024 Final Rule) to implement the Cures Act provision establishing penalties—referred to as “appropriate disincentives”—for certain healthcare providers determined by HHS-OIG to have committed information blocking. The disincentives for certain Medicare-participating hospitals and clinicians became effective July 31, 2024, while disincentives associated with the Medicare Shared Savings Program became effective January 1, 2025.

Although information blocking regulations enacted pursuant to the Cures Act have been in effect for more than a year, to date, HHS-OIG has not publicly released information about any investigation or enforcement action under such authorities. Indeed, the impetus for making information blocking a federal enforcement priority has not been clearly conveyed by the Trump administration. The increased scrutiny could, for example, be related to an increase in lawsuits against health technology companies.⁷ It could also simply be an attempt by the second Trump administration to differentiate its enforcement footprint from that of the prior administration.⁸

Compliance Is the First Line of Defense

The Enforcement Alert is intended to incentivize and enhance industry compliance, deter ongoing practices, address systemic barriers to data access, and ensure patients can freely access and

share their health records. For regulated entities considering potential next steps, comprehensive compliance and cybersecurity risk assessments, including a review of current information sharing practices, can help identify areas of risk and inform remediation and mitigation efforts.

In connection with publication of the 2023 Final Rule, HHS-OIG made it clear that it lacks the resources to investigate the large volume of complaints it anticipates receiving. Instead, HHS-OIG intends to prioritize cases of alleged information blocking that:

- Resulted in, are causing, or had the potential to cause patient harm;
- Significantly impacted a provider's ability to care for patients;
- Were of long duration;
- Caused financial loss to federal healthcare programs or other government or private entities; and
- Were performed with actual knowledge.

HHS-OIG indicated that it expects these priority enforcement areas to continue to evolve as it conducts investigations, and there is certainly nothing prohibiting it from conducting investigations outside of these priority areas. HHS-OIG also indicated that it intends to provide more information to stakeholders on its website on an ongoing basis. For the time being, however, the above-listed priority enforcement areas can be instructive for regulated entities as they design and conduct internal compliance assessments.

With respect to particular action items, potential next steps for regulated entities could include, for example:

- A review of policies, procedures, and practices affecting access, exchange, or use of EHI to confirm that they are consistent with the information blocking regulations and related laws (e.g., HIPAA and, for developers, ASTP's Health IT Certification Program requirements) (for example, a review of compliance hotline logs for complaints regarding data access).
- Train personnel responsible for negotiating and implementing collaborations, partnerships, and other arrangements with third parties (e.g., digital health companies and consumer-facing app developers) seeking access, exchange,

or use of EHI, to identify and avoid conduct that may lead to information blocking claims.

- Assess processes to create and retain records and other documents and information demonstrating the entity's compliance with the information blocking regulations (including any relevant exceptions).
- Interview and identify defense counsel to help navigate a potential OIG investigation so that the organization is prepared in the event of an actual investigation.

Notes

* The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at liz.lindquist@arnoldporter.com, lisa.re@arnoldporter.com, and jami.vibbert@arnoldporter.com, respectively.

1. HHS-OIG will pursue enforcement for information blocking complaints, and ASTP will scrutinize developers for practices that limit interoperability or impose hidden costs under its certification program.

2. HHS-OIG's Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in the U.S. Department of Health and Human Services' programs. See generally U.S. Department of Health and Human Services, "Submit a Hotline Complaint," at <https://oig.hhs.gov/fraud/report-fraud/>.

3. For example, in July, Illumina, a device company that produces genetics testing, paid \$9.8 million to resolve its False Claims Act liability related to cybersecurity failures. The federal government alleged that Illumina knew its software contained cybersecurity vulnerabilities yet failed to mitigate the risk. See U.S. Department of Justice, Office of Public Affairs, Press Release, "Illumina Inc. to Pay \$9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems," July 31, 2025, at <https://www.justice.gov/opa/pr/illumina-inc-pay-98m-resolve-false-claims-act-allegations-arising-cybersecurity>.

4. 88 Fed. Reg. at 42832.

5. *Id.* at 42832-42833.

6. *Id.* at 428323.

7. For example, Epic Systems is currently facing two lawsuits—one from health data platform Particle Health and one from managed services provider CureIS Healthcare—accusing the company of impeding access to patient data for anticompetitive purposes. See *Particle Health Inc. v. Epic Systems Corporation* (Case No. 1:24-cv-07174) (S.D.N.Y.); *CureIS Healthcare, Inc. v. Epic Systems Corporation* (Case No. 3:25-cv-04108) (N.D. Cal.).

8. See, e.g., U.S. Department of Health and Human Services, Press Release, “HHS Announces Crackdown on Health Data Blocking,” Sept. 3, 2025 (stating “[i]nformation blocking was not a priority under the Biden Administration. That changed under President Trump and Secretary Kennedy. ‘Unblocking the flow of health information is critical to unleashing health IT innovation and transforming our healthcare ecosystem,’ said Deputy Secretary of Health and Human Services Jim O’Neill. ‘We will take appropriate action against any [healthcare] actors who are found to be blocking health data for patients, caregivers, providers, health innovators, and others.’”), at <https://www.hhs.gov/press-room/hhs-crackdown-health-data-blocking.html>.