

April 26, 2024

**27th Annual Michigan Rural Health Conference:
*Health Law Update***

Agenda

- Special Rural Status
- Hospital Price Transparency
- Rural Emergency Hospitals
- Assault on Health Care Workers/Volunteers
- Informed Consent
- 340B Contract Pharmacy
- General Compliance Program Guidance
- Information Blocking
- Impact of Change Healthcare



Special Rural Status

■■ HALL
■■ RENDER
KILLIAN HEATH & LYMAN



Background

- On April 10, 2024, CMS released the 2025 Inpatient Prospective Payment System (“IPPS”) **Proposed Rule** (“Proposed Rule”).
- The Proposed Rule confirms CMS will adopt updated labor market area delineations based on the 2020 Census, taking effect on October 1, 2024.
- Stakeholders should review whether they are in a county affected by the updated delineations and assess any potential impact on Medicare reimbursements.
- The Proposed Rule is scheduled to be published in the Federal Register on May 2, 2024.



Updated Labor Market Area Delineations

- The updated labor market delineations will often result in changes to the wage index applicable to hospital reimbursement.
- As hospitals enter and leave various labor markets, the area wage index for a given market will change, and such changes could have a positive or negative impact on bottom-line reimbursement.
- In the 2020 IPPS Final Rule, CMS finalized a policy of a 5% cap on any decrease hospitals may experience in their wage index from the prior fiscal year.
- Hospitals negatively impacted by the 2020 Census updates will be protected by this policy if their wage index would otherwise decrease by more than 5% from FFY 2024.



Special Rural Status

- A category of hospitals that may be particularly affected by the updated delineations are ones the Medicare program requires to be located in a rural area (“Special Rural Status”).
- Such hospitals include critical access hospitals (“CAH”), sole community hospitals (“SCH”), rural referral centers (“RRC”) and Medicare-dependent, small rural hospitals (“MDH”).
- CMS allows CAHs in counties changing from rural to urban a two-year grace period to reclassify as rural in order to maintain their CAH status.



Special Rural Status (cont.)

- CMS does not have a provision for SCHs, RRCs or MDHs similar to the one for CAHs, so these hospitals could lose their Special Rural Status unless they act before October 1, 2024.
- These hospitals can often reclassify from urban to rural in order to maintain their Special Rural Status but should ensure doing so will not result in other reimbursement consequences.
- Depending on the circumstances, it is possible that changing to an urban area is more advantageous for Special Rural Status hospitals than the status itself.



Practical Takeaways

- Hospitals with Special Rural Status located in a county that will change from rural to urban, or rural to Lugar, should consider steps to maintain its Special Rural Status if that is indeed advantageous.
- CAHs have a two-year period to reclassify from urban to rural to maintain Special Rural Status, but other Special Rural Status hospitals have until the effective date of the new delineations, which is October 1, 2024.
- Hospitals in counties that will change from urban to rural can consider determining eligibility for Special Rural Status.
- Hospitals in counties affected by the updated labor market delineations can assess whether new geographic reclassification opportunities are available.



Hospital Price Transparency

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

Background

- Since January 2021 CMS has required hospitals to publicly post pricing information in two ways:
 - A machine-readable file (MRF) for all items and services; and
 - A consumer-friendly shoppable-services file for 300 common items and services or via a Price Estimator Tool
- Codified at 45 CFR part 180
- Penalties for non-compliance range from \$109,500 to \$2,007,500 for a full year of compliance
- 2024 OPPS Final Rule included significant updates to price transparency rule



Purpose of Rule and Updates

- Purpose of Price Transparency Rule
 - Help patients shop for healthcare services
 - Provide data to employers, researchers, and policy officials
 - Increase competition among healthcare providers to bring down costs
- Purpose of Updates
 - Standardization
 - Increase transparency to the public
 - Reduce hospital compliance burden
 - Improve monitoring and enforcement



New CMS Template and Data Elements

- Hospitals must:
 - Adopt a CMS template layout for the machine-readable file (JSON or CSV)
 - Encode the standard charge information using the CMS technical specifications and data dictionary
- Similar, but not identical to, existing CMS-developed voluntary sample formats
- Standardization over flexibility
- Effective Date is July 1, 2024
- GitHub® repository with technical instructions and guidance



Estimated Allowed Amount

- New Data Element Requirement
- Reflects an estimated dollar value when a standard charge is based on a percentage or algorithm
 - Historical Allowed Amount (i.e., average reimbursement in dollars that is received from the payer in the past for an item or service)
- Supplements (does not replace) the payer-specific negotiated charges for all items and services
 - Must still post the payer-specific negotiated rate which will be
 - Standard dollar amount;
 - Standard algorithm or percentage; or
 - Hybrid (includes a standard dollar amount plus additional variables)
- Effective Date is January 1, 2025



Compliance Statement

- Template Language for MRF:
 - *To the best of its knowledge and belief, this hospital has included all applicable standard charge information in accordance with the requirements of 45 C.F. R. §180.50 and the information encoded in this machine-readable file is true, accurate and complete as of the date indicated in this file*
- Not intended to be a guarantee of perfection, but a statement of assurance to consumers and CMS that hospital made a good faith effort to ensure data displayed is true, accurate and complete
- Effective July 1, 2024
- Good Faith Effort
 - Hospitals must make a good faith effort to ensure the standard charge information encoded in the MRF is true, accurate and complete as of the date indicated in the MRF
- Effective January 1, 2024



Root Folders & Links on Homepage

- Public Website that Hosts MRF includes the following:
 - A .txt file in the root folder that includes
 - the hospital location name that corresponds to the MRF
 - the source page URL that hosts the MRF
 - a direct link to the MRF
 - hospital point of contact
 - A link in the footer on its website, including homepage, that
 - is labeled “Price Transparency”
 - links directly to the publicly available web page that hosts the link to the MRF
 - Effective Dates January 1, 2024



Enforcement Date – January 1, 2024

- Good Faith Effort 45 CFR 180.50(a)(3)(i)
- Txt file 45 CFR 180.50(d)(6)(i)
- Footer link 45 CFR 180.50(d)(6)(ii)



Enforcement Date – July 1, 2024

- Comply with CMS Template Version 45 CFR 180.50(b)(2)(i)(B)
- Post MRF Date 45 CFR 180.50(b)(2)(i)(B)
- Post Hospital Information 45 CFR 180.50(b)(2)(i)(A)
 - name, location(s), address(es), & license information
- Post Standard Charge Information
 - gross charge & discounted cash price 45 CFR 180.50(b)(2)(ii)
 - negotiated rate
 - payer name & plan name 45 CFR 180.50(b)(2)(ii)(A)
 - standard charge method 45 CFR 180.50(b)(2)(ii)(B)
 - payer specific negotiated charge/rate AND whether dollar, percentage or algorithm 45 CFR 180.50(b)(2)(ii)(C)
 - de-identified minimum and maximum negotiated charge 45 CFR 180.50(b)(2)(ii)



Enforcement Date – July 1, 2024 (cont.)

- Item & Service Information
 - General Description 45 CFR 180.50(b)(2)(iii)(A)
 - Setting 45 CFR 180.50(b)(2)(iii)(B)
- Coding Information
 - Billing/Accounting Code 45 CFR 180.50(b)(2)(iv)(A)
 - Code Type 45 CFR 180.50(b)(2)(iv)(B)
- Affirmation in the MRF 45 CFR 180.50(a)(3)(ii)



Enforcement Date – January 1, 2025

- Estimated Allowed Amount 45 CFR 180.50(b)(2)(ii)(C)
- Drug Unit of Measurement 45 CFR 180.50(b)(2)(iii)(C)
- Drug Type of Measurement 45 CFR 180.50(b)(2)(iii)(C)
- Coding Information
 - Modifiers 45 CFR 180.50(b)(2)(iv)(C)



Monitoring and Enforcement

- Current state
 - CMS evaluates complaints from public and conducts own reviews and audits
 - Hospitals notified of noncompliance via a warning letter, followed by a request for a corrective action plan before civil monetary penalties
 - CMS publicly posts CMPs
- Updates (supplement, do not replace current state)
 - CMS may require an authorized official to certify contents of MRF during assessment
 - Hospitals must acknowledge receipt of warning notices
 - CMS may notify system leadership of hospital compliance actions
 - CMS may publicize hospital specific assessment activities, compliance actions, and notifications to system leadership





Rural Emergency Hospitals (REHs)

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

(Not Much of an) Update

- A tracker of participating hospitals published by the Cecil G. Sheps Center for Health Services Research is available at: <https://www.shepscenter.unc.edu/programs-projects/rural-health/rural-emergency-hospitals/>
- 23 Hospitals have converted to REHs since January 2023
 - Still only 1 in Michigan
- Michigan is the only state with a Medicaid plan amendment to pay for REH services like a hospital
- Previous analyses by hospitals likely remain unchanged





Assault of Health Care Workers and Volunteers

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN



Background

- Through the passage and signing of House Bill 4520 (“HB 4520”) and House Bill 4521 (“HB 4521”), there has been an increase to financial penalties for those committing violence in the health care workplace.
- Bipartisan laws amend the Michigan Penal Code by doubling fines imposed on persons who harass and/or assault health care professionals and medical volunteers on the job.
- HB 4520 and HB 4521 went into effect on March 5, 2024.



Background (cont.)

- The enactment of HB 4520 and HB 4521 represents the growing trend of the federal government and state governments protecting health care workers from workplace violence.
- In February 2023, the Occupational Safety and Health Administration (“OSHA”) reported in its **“Prevention of Workplace Violence in Healthcare and Social Assistance” Issues Document** that health care workers face *almost a six times greater* chance of being injured from workplace-violence-related injuries compared to employees in the overall private sector.



HB 4520 and HB 4521- Increased Penalties

- Under HB 4520, the financial penalty for individuals who assault health care workers or medical volunteers on the job increases up to \$1,000.
- HB 4520 also doubles the financial penalty for aggravated assault, a misdemeanor, from \$1,000 to \$2,000.
- Under HB 4521, an individual who assaults a health care worker or volunteer on the job faces jail time of up to four years and a fine of up to \$4,000.
- *NOTE: HB 4520 and HB 4521 do not protect a health care worker or on-the-job volunteer from assault committed by a patient receiving treatment or care from such health care worker or volunteer.*



Practical Takeaways

- Health systems and hospitals are now required under HB 4520 and HB 4521 to post signs in a prominent and visible location that state that a person (other than the patient receiving treatment) who assaults a health worker or medical volunteer is subject to enhanced fines, and a patient receiving treatment is still subject to prosecution.
- Health systems and hospitals should adhere to this posting requirement and review their policies and procedures related to providing a safe environment for their staff and patients.



Informed Consent

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

Overview

- On April 1, 2024, the U.S. Department of Health and Human Services (“HHS”), through CMS released a **memorandum** to state survey agency directors highlighting revisions and clarification to the Hospital Interpretive Guidelines for Informed Consent (the “Guidance”).
- The Guidance clarifies informed consent requirements for the performance of pelvic, breast, prostate and rectal examinations (referred to in the Guidance as “sensitive exams”), particularly on patients under anesthesia.



Background & Updated Guidance

- The Guidance more closely aligns CMS survey practices with updates in state law.
- Specifically, the Guidance:
 - Requires surveyors to confirm that a hospital's informed consent policy and process, as well as the hospital's informed consent forms, contain elements and information that allow for a patient, or the patient's representative, to make fully informed decisions about their care.
 - Clarifies that a properly executed informed consent form must include the name of the specific procedure or medical treatment for which consent is being given, as well as the name of the practitioner who is performing the procedure.



Background & Updated Guidance (cont.)

- The Guidance also:
 - Provides that a well-designed consent form, as well as hospital policy and process for informed consent, should alert patients to the following:
 - Whether providers other than the operating provider, including other physicians, residents, medical students, advanced practice provider students and other applicable students will be performing important tasks related to surgery or examinations or invasive procedures for educational and training purposes.
 - Clarifies that “examinations or invasive procedures” for which the above information should be provided include, but are not limited to, breast, pelvic, prostate and rectal examinations, as well as others specified by state law.



Practical Takeaways

- Hospitals and health care providers should consider undertaking the following actions in response to the Guidance:
 - Closely monitor ongoing developments in state law related to informed consent for sensitive exams, as this is an area of rapid change;
 - In 2023, the Michigan Senate introduced Senate Bill 44 (SB 44) which addressed restrictions on invasive examinations without consent
 - The last available update for [SB 44](#) indicates that it was referred to the Committee on Health Policy on 11/08/2023



Practical Takeaways (cont.)

- Hospitals and health care providers should consider undertaking the following actions in response to the Guidance:
 - Assess the processes by which medical students, residents, fellows and other medical learners are trained to conduct sensitive exams to ensure compliance with the Guidance, relevant state law and HIPAA;
 - Review current medical staff and other policies and processes related to informed consent, and revise them as necessary to ensure compliance with the Guidance and relevant state law;
 - Review informed consent forms and revise them as necessary to ensure compliance with the Guidance and relevant state law;
 - Ensure that the operating room and other procedural area timeout processes include confirming whether the patient has provided informed consent to the performance of sensitive exams; and
 - Educate educational leadership, teaching physicians, residents, fellows, medical students, other medical learners and staff on the requirements imposed by the Guidance and state law and on any necessary changes to the informed consent process.





340B Contract Pharmacy

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

Contract Pharmacy – Manufacturer Restrictions

Background

- In 2020, drug manufacturers began restricting 340B contract pharmacy shipments
- Began with Eli Lilly
- Now, 25 total manufacturers

Manufacturers' Central Complaint

- So-Called Duplicate Discounts
 - Manufacturer paying a rebate to an insurer/PBM for a drug it already sold at the 340B price
 - Some are prohibited by statute (Medicaid)
 - Occur rarely; processes in place to prevent them
 - Some are prohibited by manufacturers' contracts with commercial payors

Exceptions and Conditions

- Most manufacturers have some exceptions (wholly owned pharmacies; single contract pharmacies)
- Some manufacturers permitting shipments if covered entity provides claims-level patient data directly to manufacturer or Second Sight Solutions
 - Second Sight is owned by Berkeley Research Group, a Pharma-aligned consultancy
 - Manufacturers are using data to deny payor rebates

Contract Pharmacy – Manufacturer Restrictions

Government Response

- Congress, HRSA, and HHS Office of General Counsel highly critical of manufacturer actions
 - HRSA sent enforcement letters to 9 manufacturers informing them restrictions unlawful
 - HRSA referred seven manufacturers to OIG for Civil Monetary Penalty application
 - OIG has taken no public action so far

Manufacturer Litigation

- At least eight manufacturers plus PhRMA (trade group) have sued HHS
- Cases have been mixed; two appeals pending; one decided in manufacturers' favor (3rd Cir.)

House Bill 5350 of 2023

- [House Bill 5350](#) proposes to enact the following protections for 340B contract pharmacies by prohibiting manufacturers from taking the following actions:
 - Deny, prohibit, condition, discriminate against, refuse or withhold 340B pricing for, or otherwise limit the dispensing, purchase, ordering, delivery, or receipt of a drug purchased by a 340B entity, **including, but not limited to, a drug purchased to be dispensed or administered under a contract pharmacy arrangement.** OR
 - **Prohibit a pharmacy from contracting or participating with a 340B entity** by denying 340B pricing on, or the pharmacy's access to, a drug that is manufactured by a manufacturer or based on a pharmacy's relationship with a 340B entity.
- The [MI Legislature's bill page](#) indicates that as of 1/1/24, the Bill was referred to Committee on Insurance and Financial Service.





General Compliance Program Guidance Updates

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

GCPG 2023 Overview

- **General Compliance Program Guidance (“GCPG”)** issued by OIG in November 2023
- More specifically, it addresses:
 - *Key federal authorities for entities engaged in health care business;*
 - *The seven elements of a compliance program;*
 - *Adaptations for small and large entities; and*
 - *Other compliance considerations, OIG processes, and resources.*
- Much of what is covered is not new to the health care compliance industry
- **Reinforces best practices and recommendations from previous OIG guidance**, as well as insights learned from Corporate Integrity Agreements (“CIAs”)
- **OIG will no longer publish updated or new CPGs in the Federal Register.**
 - OIG will publish Industry Segment-Specific CPG (ICPGs) for different types of providers, suppliers, and other participants in health care industry subsectors
 - Existing CPGs will remain available but be archived when ICPGs are issued



Compliance Officers - UPDATE

- If CCO serves as Privacy Officer, then sufficient staff for privacy functions are needed
- **The entity should ensure the compliance officer does NOT:**
 - Lead or report to the entity's legal or financial functions;
 - Provide the entity with legal or financial advice or supervise anyone who does;
 - Become responsible, directly or indirectly, for the delivery of health care items and services or billing, coding, or claim submission; or
 - Become involved in functions such as contracting, medical review, or administrative appeals.



Compliance Committee - UPDATE

- The Compliance Committee aids and supports the Compliance Officer in implementing, operating, and monitoring the compliance program.
- The entity should ensure that the committee:
 - Is properly trained in its roles and responsibilities
 - Is actively involved in the implementation of the compliance program:
 - Analyzing the legal/regulatory requirements
 - Reviewing and revising policies and procedures
 - Monitoring and recommending internal systems and controls
 - Reviewing and assessing education and training
 - Conducting the annual risk assessment, etc.
- Create subcommittees as appropriate
- The Compliance Officer:
 - Periodically provides report to the Board assessing committee's performance;
 - Examines how the entity implemented the committee's decisions and recommendations



Risk Assessment - UPDATE

- **Formal Compliance Risk Assessment:**
 - **Conducted and implemented by the Compliance Committee.**
 - Compliance, audit, quality, and risk management functions coordinate to conduct a joint risk assessment
- **Between Compliance Risk Assessments:**
 - The Compliance Officer should continue to scan for unidentified or new risks
 - **Data Analytics**
 - Entities should consider using data analytics to identify compliance risk areas
 - All entities, regardless of size, should have access to the data they generate, either directly or through a third party, such as a billing contractor.
 - All entities should be able to compare standard metrics of their health care operations internally to determine whether there are any outliers in any particular area of focus.
 - Larger entities or those with more capabilities or resources should run more sophisticated data analytics processes to assess any compliance risks presented by their operations.

Quality & Patient Safety Considerations - NEW

- **Integrate quality and patient safety oversight into compliance processes**
- **Board Responsibilities**
 - Require regular reports from compliance and senior leadership responsible for quality and patient safety
 - Use a **quality dashboard to assist it in monitoring** the entity's quality performance, including patient safety.
- **Compliance Officer Responsibilities**
 - Include members responsible for quality assurance and patient safety.
 - Receive regular reports from senior leadership on quality, patient safety, and, for provider entities and physician practices, adequacy of patient care.
 - Establish and implement a **program for performing quality audits and reviews** – the program should:
 - audit and review quality and patient safety incidents;
 - conduct root-cause analyses;
 - design or approve corrective action plans; and
 - track the implementation and effectiveness of the plans.
 - Assess staffing for nursing, therapy, and other clinical services to ensure that the entity has the appropriate quantity, quality, and composition of care providers.
- **Compliance Committee Responsibilities**
 - Develop productive working relationships with clinical and quality leadership, sharing information and work and advising on compliance matters;
 - Be informed about any internal quality audits and incident reviews; and
 - Have the resources to conduct the quality compliance audits discussed above, either individually or in collaboration with Internal Audit or outside resources.



Adaptations for Small and Large Entities

OIG recognizes that compliance programs may differ based on the size of the entity.

Compliance Programs for Small Entities

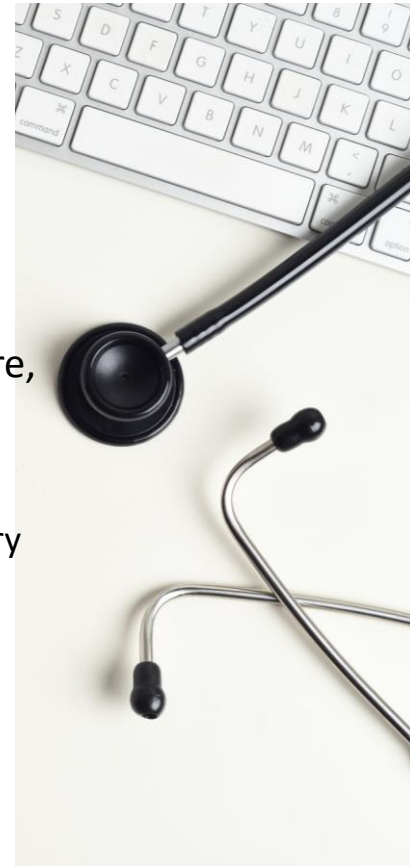
While still encompassing the seven elements discussed above, a small entity's compliance program should be **structured so that the entity can gain the benefits and protection** of a compliance program **within the constraints** under which the **entity operates**.

Compliance Leadership for Large Entities

Health care **board members** should consider the **size and complexity** of their organizations in reviewing the **scope and adequacy** of the entity's compliance program.

New Entrants in the Health Care Industry

- **New entrants include:**
 - Technology companies
 - New investors
 - Organizations providing non-traditional services in health care settings
- Business practices common in other sectors create compliance risk in health care, including potential criminal, civil, and administrative liability
- **New entrants are often unfamiliar with**
 - The unique regulations and business constraints that apply in the health care industry
 - The range of Federal and State government agencies that regulate health care and enforce fraud and abuse laws
- **New entrants should gain a solid understanding of**
 - **The Federal fraud and abuse laws**
 - The critical role an effective compliance program plays in preventing, detecting, and addressing potential violations
- Health care organizations themselves entering **new arenas.**
 - Need to understand **new risk areas associated with new and different lines of health care business**





Information Blocking

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN

Information Blocking vs. HIPAA

Cures Act - Information Blocking Rule	HIPAA – Privacy Rule
<p><u>Prohibits</u> an Actor from interfering with access, exchange or use of EHI, unless an exception applies.</p>	<p><u>Permits</u> Covered Entities to disclose PHI for Treatment, Payment and Healthcare Operations</p>
<p>Actor – means health care provider, health IT developer of certified health IT, health information network or health information exchange.</p>	<p>Covered Entity – Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, associated with the federal healthcare system is a Covered Entity</p>
<p>Electronic Health Information (EHI)* - electronic PHI that would be included in a designated record set without respect to whether such information is in the possession of an entity subject to HIPAA (excluding psychotherapy notes and information compiled for litigation). Excludes psychotherapy notes and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding</p>	<p>Protected Health Information (PHI) – "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.</p>

What is “Information Blocking”?

“Information Blocking” means a practice that:

- Except as required by law or specified by the Secretary pursuant to rulemaking, is **likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information**; and
 - If conducted by a health information technology developer, exchange, or network, such developer, exchange, or network **knows, or should know**, that such practice is likely to interfere with, prevent or materially discourage the access, exchange or use of electronic health information; or
 - If conducted by a health care provider, such provider **knows that such practice is unreasonable** and is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.



Who: “Actors”

Health Care Provider

A health care provider is a: hospital; skilled nursing facility; nursing facility; home health entity or other long term care facility; health care clinic; community mental health center; renal dialysis facility; blood center; ambulatory surgical center; emergency medical services provider; federally qualified health center; group practice; pharmacist; pharmacy; laboratory; physician; practitioner; provider operated by or under contract with the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization; rural health clinic; covered entity under 42 U.S.C. 256b; ambulatory surgical center; therapist; and **any other category of health care facility, entity, practitioner, or clinician determined appropriate by the HHS Secretary.**



What: “Electronic Health Information”

Electronic health information (EHI)

Electronic Protected Health Information as defined in 45 CFR 160.103 to the extent that it **would be included in a designated record set** as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI shall not include:

- Psychotherapy notes as defined in 45 CFR 164.501; or
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

From **April 5, 2021 to October 6, 2022**, EHI was limited to information/data elements available in the **USCDI version 1**. It has since expanded to include all EHI.



INFORMATION BLOCKING EXCEPTIONS

Exceptions that involve not fulfilling requests to access, exchange, or use EHI

1) Preventing Harm Exception (45 C.F.R. 171.201)

2) Privacy Exception (45 C.F.R. 171.202)

3) Security Exception (45 C.F.R. 171.203)

4) Infeasibility Exception (45 C.F.R. 171.204)

5) Health IT Performance (45 C.F.R. 171.205)

Exceptions that involve procedures for fulfilling requests to access, exchange or use EHI

6) Manner Exception (45 C.F.R. 171.301)

7) Fees Exception (45 C.F.R. 171.302)

8) Licensing Exception (45 C.F.R. 171.303)

Exceptions That Involve Practices Related to Participation in The Trusted Exchange Framework and Common Agreement

9) TEFCA Manner Exception (45 C.F.R. 171.403)



Impact of Change Healthcare (so far)

■ ■ HALL
■ ■ RENDER
KILLIAN HEATH & LYMAN



Incident Overview

- Change Healthcare is a prominent health care technology and services provider that is owned by Optum and part of the UnitedHealth Group (UHG).
- Change Healthcare is the largest health administrative network in the United States, providing a variety of services such as claims processing, billing, pharmacy requests, and clearinghouse functions to health care providers and health plans.
- It has been estimated that Change Healthcare alone processes half of the medical claims in the United States and handles more than 15 billion transactions annually.



Incident Overview (cont.)

- On February 21, 2024, Change Healthcare experienced a significant cyberattack that resulted in them shutting down all of their computer systems.
- While this incident certainly raises serious concerns about the privacy and security of sensitive patient information, its primary impacts have been operational and financial.
- The immediate effects of the incident have included delays in filling prescriptions at pharmacies, interruptions in processing and paying health claims, stalled precertification processes and disruptions in cash flow that in some cases could threaten an organization's ability to deliver the full continuum of care, make payroll or even remain in operation.



Recent Developments

- It appears the hackers have begun to sell patient data and certain legal documents which they claim were stolen in the cyberattack.
- On April 15, cybercriminals reportedly leaked contracts and patient data purportedly stolen in the cyberattack.
- The “RansomHub” cybercriminal group posted on the dark web on April 16 that it put information obtained in the hack up for sale.
 - The information appears to contain legal documents (trader partner agreements), bills for services to providers, Medicare claim information (which includes sensitive PII), payment information, and more.
- There are (unconfirmed) reports that UnitedHealth Group has allegedly already paid another ransomware group \$22 million, and other insurers may have been contacted by the cybercriminals attempting to exploit ransom payments



Recent Developments

- On April 16, the U.S. House Energy and Commerce Committee held a hearing about the cyberattack.
- According to reports, no UHG representatives were present at the hearing.
- The hearing included testimony from various experts about the general state of healthcare cybersecurity, including several recommendations for improving government and private sector security mechanisms.



Key Considerations

- Key Considerations for hospitals and health systems include:
 - Contractual Rights and Remedies;
 - Reimbursement Compliance;
 - Financial Assistance;
 - Privacy;
 - Security; and
- Other Considerations - There are a variety of other practical steps that affected health care organizations should consider taking, including:
 - Consider notifying your insurance carrier if you plan to file an insurance claim for financial losses arising from this incident, which could be available to organizations that have coverage for contingent business interruption caused by a third party.
 - Anticipate the possibility that Change Healthcare will go through bankruptcy, lawsuits from providers and lawsuits from patients as a result of this breach (these have already begun).
 - Identify alternatives, either to act immediately or as contingency planning.

Hall Render Articles

- [Main Articles/Webinar Page](#)
- [Price Transparency Rule](#)
- [Sensitive Examination Informed Consent](#)
- [Special Rural Status](#)
- [Change Healthcare Cybersecurity Incident](#)
- [Penalties for Assaults of Health Care Workers](#)

Questions?

For more information on these topics visit hallrender.com.



Andrew Heberling - Attorney, Hall Render
aheberling@hallrender.com

