Arkansas HFMA

Regulatory Update

2022

Amie K. Wilcox and Tim C. Ezell

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Overview

- 2022 Updates
  - No Surprises Act
- 2023 Upcoming
  - HIPAA Revisions Expected

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Overview

- Reviewing the Big Ones
  - HIPAA
  - Stark and Anti-Kickback

Surprise Billing Rules

- Two Interim Final Rules were published, implementing the provisions of the No Surprises Act (signed into law as a part of the Consolidated Appropriations Act of 2021).
- Effective January 1, 2022

Surprise Billing Rules

- Applies to "balance billing" – billing the patient for the difference between the billed charge and the amount paid by their plan or insurance (usually for out-of-network charges)
- Does not apply to people with coverage such as Medicare, Medicaid, VA, Tricare (already prohibited balance billing)

Surprise Billing Rule

- Restricts surprise billing for patients in employer-sponsored and individual health plans who:
  - Receive emergency care;
  - Receive non-emergency care from out-of-network providers at in-network facilities; and
  - Receive air ambulance services from out-of-network providers

Surprise Billing Rule

- Prohibits out-of-network charges for items and services provided by an out-of-network facility *unless* certain notice and consent is given.
- Otherwise, patient cost-sharing is limited to the amount that would be charged for in-network care.
- For emergency care, Rule requires emergency services to be covered without any prior authorization and regardless of whether a provider or facility is in-network.

Surprise Billing Rule

- **Consent Exception** – may apply in limited cases; will not apply in some situations where surprise bills are likely (for example, ancillary services connected to non-emergency care such as anesthesia or radiology).
- Where it does apply, specific requirements exist regarding the content of notices and consents.

Surprise Billing Rule

- **Required Notice** – requires providers and facilities to make publicly available, post on a public website, and provide to individuals a one-page notice about the requirements of this Rule and how to report a violation.
- **Good Faith Estimates Required** – for uninsured or self pay patients. The Rule sets forth specific time frames this estimate is required to be furnished within. If patient is billed substantially in excess (at least $400 in excess) of estimate, will be subject to arbitration process.

Surprise Billing Rule

Independent Dispute Resolution Process Established

- Provider or Facility and Payers
  - To determine amount of payment owed to provider/facility as a result of treating patients as in-network for out-of-network charges
- Provider or Facility and Self Pay Patient
  - To determine amount of payment owed if substantially in excess of good faith estimate

Surprise Billing Rule

Independent Dispute Resolution Action	Timeline
Initiate 30-business-day open negotiation period	30 business days, starting on the day of initial payment or notice of denial of payment
Initiate independent dispute resolution process following failed open negotiation	4 business days, starting the business day after the open negotiation period ends
Mutual agreement on certified independent dispute resolution entity selection	3 business days after the independent dispute resolution initiation date
Departments select certified independent dispute resolution entity in the case of no conflict-free selection by parties	6 business days after the independent dispute resolution initiation date
Submit payment offers and additional information to certified independent dispute resolution entity	10 business days after the date of certified independent dispute resolution entity selection
Payment determination made	30 business days after the date of certified independent dispute resolution entity selection
Payment submitted to the applicable party	30 business days after the payment determination

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Required Notices

https://www.cms.gov/nosurprises/policies-and-resources/overview-of-rules-fact-sheets

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Polling Question 1

The Surprise Billing Rules Require:

1. Covered Providers to Post Required Notices on Website
2. Covered Providers to Provide Required Notices to Patients
3. Good-Faith Estimates to Uninsured or Self Pay Patients
4. All of the Above

FRIDAY | ELDREDGE & CLARK LLP
www.FridayFirm.com

Polling Question 2

The No Surprises Act Applies To:

1. Emergency Services
2. Physician Clinic Services
3. Out-of-Network Facilities
4. None of the Above

FRIDAY | ELDREDGE & CLARK LLP
www.FridayFirm.com

HIPAA Refresher

- The Privacy Rule
- The Security Rule
- Breach Notification
- Compliance & Enforcement

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Common Questions on HIPAA

- What is PHI?
  - Individually Identifiable Health Information (includes demographic information) relating to:
    - Individual's past, present or future physical or mental health or condition;
    - The provision of health care to the individual; or
    - The past, present, or future payment for the provision of health care to the individual
- How do I handle PHI? SECURELY!

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Common Questions on HIPAA

- When do I need a Business Associate Agreement?
  - You need a BAA when you are hiring a person or organization (other than your workforce) to perform a task on your behalf that involves the use or disclosure of PHI.
  - You do not need a BAA between two covered entities exchanging information for treatment purposes

The Privacy Rule

The Privacy Rule:

- Purpose – define and limit the circumstances in which an individual's Protected Health Information (PHI) may be used or disclosed by covered entities.
  - Required Disclosures – to individuals (or representative) when appropriately requested
  - Permitted Disclosures – purposes of treatment, payment, or health care operations, and where required by law.
  - Authorized Uses and Disclosures – with individual's authorization (for example, for marketing purposes or to employer the results of pre-employment physical)
- Limit Uses and Disclosures to the Minimum Necessary
- Required Notice of Privacy Practices
- Individual Rights

The Security Rule

- Requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Covered entities are required to:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance with their workforce.

The Security Rule

Administrative Safeguards

- Security Management Process
- Security Personnel
- Information Access Management
- Workforce Training and Management
- Evaluation

Physical Safeguards

- Facility Access and Control
- Workstation and Device Security

Technical Safeguards

- Access Control
- Audit Controls
- Integrity Controls
- Transmission Security

The Security Rule

Risk Analysis and Management

- A risk analysis process includes, but is not limited to, the following activities:
  - Evaluate the likelihood and impact of potential risks to e-PHI;
  - Implement appropriate security measures to address the risks identified in the risk analysis;
  - Document the chosen security measure and, where required, the rationale for adopting those measures; and
  - Maintain continuous, reasonable, and appropriate security protections.
- Ongoing process – regularly review records to track access to e-PHI and detect security incidents, periodically evaluate the effectiveness of security measures in place, and regularly reevaluate potential risks to e-PHI.

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Breach Notification

What is a breach?

- an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI

Breach Presumption

- an impermissible use or disclosure of PHI is *presumed* to be a breach unless the covered entity or business associate demonstrates that there is a *low probability* that the PHI has been compromised based on a risk assessment or at least the following factors –
  1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  2. The unauthorized person who used the PHI or to whom the disclosure was made;
  3. Whether the PHI was actually acquired or viewed; and
  4. The extent to which the risk to the PHI has been mitigated.

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Breach Notification

Breach Exceptions

1. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, *if* made in good faith and within the scope of authority.
2. Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. The information cannot be further used or disclosed.
3. The covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Breach Notification

Individual Notice

- Written notice without unreasonable delay and in no case later than 60 days following the discovery of the breach
- Must include a brief description of the breach, a description of the types of information involved, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches. Must also include contact information for the covered entity.
- If inaccurate addresses for 10 or more individuals, must provide notice on website or major print or broadcast media for at least 90 days.

Media Notice

- Must provide media notice in the state if more than 500 residents are affected – same 60-day requirement.

Notice to the Secretary

- 500 or more individuals – must notify Secretary within 60 days
- Fewer than 500 individuals – report on annual basis
- May also need to notify individuals as required by state Attorneys General

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Cybersecurity and HIPAA

Most Common Threats

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or theft of equipment or data
4. Inside, accidental or intentional data loss
5. Attacks against connected medical devices

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

HIPAA Common Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Maintain Identified Risk, e.g. Encrypt
- Lack of Appropriate Auditing
- Insider Threat
- Insufficient Cybersecurity Measures
- Insufficient Data Backup and Contingency Planning

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2021	Impermissible Uses & Disclosures	Access	Safeguards	Administrative Safeguards	Breach - Notice to Individual
2020	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Technical Safegards
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safegards

Penalties

- Structured on Culpability Level

- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Tier 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days

Takeaways

1. Perform a Risk Assessment – Engage a 3rd Party
2. Follow-up on the results of the Risk Assessment
3. Encryption is now the standard – not an option
4. Make sure you have written Business Associate Agreements in place! (these are necessary if sharing PHI with non-clinic)
5. Cyber Liability Coverage
6. Enforcement - https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html

Polling Question 3

If my organization does not run a Security Risk Assessment:

1. It won't matter as long as there is no breach;
2. I can defend an unfavorable finding if the Security Risk Assessment would have been too expensive;
3. It's okay if we ran one last year;
4. None of the above.

HIPAA PROPOSED REVISIONS

A Notice of Proposed Rule Making (NPRM) for modifications to the HIPAA Privacy Rule was published by the Department of Health and Human Services (HHS) in the Federal Register on January 21, 2021 closed commenting in 2022. The purpose of the proposed changes is to improve individual access to protected health information (PHI) and increase permissible disclosures of PHI with the intent of improving care coordination and case management.

Adds Definitions for Electronic Health Record (EHR) and Personal Health Applications

- Proposed EHR definition

  EHR means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized healthcare clinicians and staff. Such clinicians shall include, but are not limited to, healthcare providers that have a direct treatment relationship with individuals as defined at 164.501, such as physicians, nurses, pharmacists and other allied health professionals. For purposes of this paragraph, "health-related information on an individual" covers the same scope of information as the term "individually identifiable health information" (IIHI) as defined at 160.103.

Adds Definitions for Electronic Health Record (EHR) and Personal Health Applications

- Proposed personal health application definition (p. 47, 338)
  - An electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared and controlled by or primarily for the individual and not by or primarily for a covered entity or another party such as the application developer.
  - Further explanation: A personal health app is a service offered directly to consumers. The covered entity (CE) does not manage, share, or control the information nor does the application developer manage the information on behalf or at the direction of a healthcare provider or health plan (e.g., through a patient portal) or another party that collects or manages PHI for its own purposes (e.g., research organization).

Modifies Provisions on Individuals' Right of Access

- Strengthens individual right to inspect their PHI in person
  - Adds that individual can take notes, photos, videos to capture copies of their PHI in a designated record set (DRS).
  - Requires when PHI is "readily available" at the point of care or in conjunction with an appointment, provider is not permitted to delay the right to inspect.
  - Stipulates that providing a summary (even if patient agrees to it) does not replace a patient's right to a copy.

- Modifies implementation requirements and shortens CE response time
  - May still require an access request in writing but prohibits "unreasonable measures" that could impede access such as:
    - Filling out HIPAA authorization when access request is acceptable
    - Submitting request only in paper form, only in person or only through CEs portal
  - Changes response time to 15 calendar days (from 30 days), including a one-time 15-day extension
    - Requires policies and procedures for prioritizing urgent and other high priority access requests to limit need for 15-calendar day extension
    - Response time applies to individual requests and individual requests directed to third parties

FRIDAY | ELDREDGE & CLARK LLP
www.FridayFirm.com

- Addresses form of access
  - Addresses what constitutes "readily producible" form and format when providing requested copies of PHI
  - Addresses ePHI transmitted via a personal health application
  - Requires CEs to inform individuals about their right to obtain or direct copies of PHI to a third party when a summary or explanation is offered

- Addresses individual right of access to direct copies of PHI to third parties
  - Creates separate set of provisions to address individual right to direct copies to third party
  - Limits the right to direct transmission of copies of PHI to a third party to only electronic copies of PHI in an EHR
  - Requests can be oral or written if clear, conspicuous, and specific including requests submitted via an internet-based method such as personal health app
  - Creates new requirement that individuals may direct a provider or health plan to submit a request for an electronic copy of the individual's PHI in an EHR on behalf of the individual to a CE that maintains that individuals PHI

- Adjusts permitted fees for access to PHI

  Clarifies when ePHI must be provided **to the individual free of charge**

  - Individual inspects their PHI in-person which may include recording or copying PHI in a DRS with individual's own device
    - Must be free of charge
    - Inspecting PHI may include viewing the information on a patient portal, which could be made available in person for the individual at the point of care in conjunction with a healthcare appointment or at a medical records office

- Amends the fee structure for certain requests **requested by the individual for themselves**
- Access requests for **non-electronic copy of PHI** through other than an Internet-based method
  - Reasonable cost-based fee as currently defined in Privacy Rule, including labor, supplies, postage, and costs for preparing summary

- Access requests for **electronic copy of PHI** through other than an internet-based method
  - Reasonable cost-based fee limited to labor only for making electronic copies of the PHI and preparing a summary or explanation as agreed to by the individual
  - The costs for media and postage would not be allowed for providing electronic copies of PHI by any method
  - This is pursuant to section 13405(e) of the HITECH Act which states, "any fee that the CE may impose for providing an individual with a copy of such information (or a summary or explanation of such information) if such copy is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy
  - HHS understands that a CE may copy the PHI onto electronic media and mail to individual or use the export functionality of certified EHR technology to transmit ePHI. However, based on the plain reading of the HITECH statutory requirement, HHS is proposing to limit the fees

- Amends the fee structure for certain requests when an **individual directs PHI to a third party**
  - Individual directs **electronic copy of PHI in EHR** to third-party
    - Reasonable cost-based fee limited to labor only for making electronic copies of the PHI and preparing a summary or explanation as agreed to by the individual
    - Consistent with the 2020 Ciox Court Ruling, the rule proposes in 45 CFR 164.524(c)(3)(ii) to limit the right of an individual to direct copies of PHI to a third-party to only electronic copies of PHI in an EHR

- Individual directs **non-electronic copy of PHI in an EHR or electronic copies of PHI that is not in an EHR** to third parties
  - Fees not subject to the access fee limitations
  - Disclosure based on valid authorization vs access request (whether to an individual's family member, CE researcher or any other person)
  - Fees remain limited by the Privacy Rule's provisions on the sale of PHI at CFR 164.502(a)(5)(ii)(B)(2)(viii) and 45 CFR 164.502(a)(5)(ii)(A) and by applicable state law

- Adds new requirements for notice of access and authorization fees
  - Requires CEs to post fee schedules on their websites (if they have one)
  - Requires a CE to provide a copy of the fee schedule, upon request
  - Requires CEs to provide individualized estimates of fees for copies and an itemized list of actual costs for requests for copies, upon request
  - Does not prohibit requiring payment upfront before receiving copies
  - Does not propose to amend rule to require CEs to fulfill the requests of individuals by providing copies before fees are paid

FRIDAY ELDREDGE & CLARK LLP
www.FridayFirm.com

Prohibits CEs from imposing unreasonable identity verification measures

Unreasonable identity verification measures include:

- Requiring notarization of signature
- Requiring in person proof of identity when remote method could be used

Amends the definition of healthcare operations

Clarifies the scope to include individual-focused (in addition to current population-based) care coordination and case management activities.

Creates an exception to the minimum necessary standard for disclosures to or requests from health plans or CEs for individual-level care coordination and case management activities

Some disclosures for payment purposes are related to individual-level care coordination and case management activities. Disclosures for payment purposes are subject to minimum necessary and do not change.

Clarifies scope of CEs' ability to disclose PHI to certain third parties for individual-level care coordination and case management

Permits social services, community-based organizations, home and community-based service providers and similar third parties to facilitate individual-level care coordination and case management activities that constitute treatment or healthcare operations.

Encourages disclosures of PHI to help individuals experiencing substance abuse disorder including opioid use disorder, serious mental illness and in emergency circumstances

- Replaces "professional judgment" with "good faith belief" that the disclosure is in the best interest of the individual in five provisions
- Permits CEs to use or disclose PHI without having to determine if the threat is "serious and imminent" and instead whether it is "reasonably foreseeable" to avert a serious threat to health or safety

Eliminates/modifies Notice of Privacy Practice (NPP) requirements

- Eliminates requirement to obtain an individual's written acknowledgement of receipt of a direct treatment provider's NPP
- Replaces written acknowledgement with individual's right to discuss NPP with designated person
- Eliminates need to retain NPP for six years
- Modifies the content of the NPP

Permits disclosures to Telecommunications Relay Services (TRS) communication assistants

Modifies definition of Business Associate (BA) to exclude TRS providers.

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Navigating Fraud and Abuse Laws

- Stark and Anti-Kickback address financial incentives and over-utilization
- Two distinct laws – overlapping applications
- Financial relationships are highly regulated
- Both carry severe penalties for violations
- State laws limiting mark ups and other medical billing techniques

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

Stark Law

Purpose: limits physician referrals for when there is a financial relationship with the entity (includes anything of value provided).

Analysis:

1. Is there a referral from a physician for a designated health service (DHS)?
2. Does the physician (or an immediate family member) have a financial relationship with the entity providing the DHS?
3. Does the financial relationship fit within an exception?

Penalties – payment denial, monetary penalties, exclusion, and possible violation of the False Claims Act

Stark Law Compliance

1. Meet a Stark Law exception
2. Document financial relationships with referring physicians.
3. Have systems to ensure properly structured payments.
4. Watch out for lease problems.
5. Gifts can implicate the Stark Law too.

Anti-Kickback Statute

Purpose: prohibits asking for or receiving anything of value to induce or reward referrals of Federal health care program business.

Analysis:

1. Is there a referral relationship?
2. Is there something of value being exchanged?
3. Are there Federal health care program patients?
4. Is there intent to induce referrals?

Penalties: fines, program exclusion, prison time

Anti-Kickback Compliance

1. Use a Safe Harbor
2. The test is a "One Purpose" Test
   - the statute is violated if one purpose of the remuneration is to induce referrals, even if there are other legitimate purposes.
3. FMV for actual/necessary services

False Claims Act

Purpose: prohibits the submission of false or fraudulent claims to the Government.

Types of False Claims

- False Claim – patient does not exist, services not rendered
- Reverse False Claim – retained overpayments
  - A strong compliance program is necessary to identify potential overpayments.
  - An overpayment must be reported and refunded within 60 days of quantification.
  - Tasked with "reasonable diligence" to identify overpayments.

Safe Harbors

Stark

- Bona fide employment
- Personal services
- Rental of office space and equipment
- Isolated Transaction
- Physician Recruitment
- Indirect Compensation
- Fair Market Value (FMV)
- In-Office Ancillary Services
- Bona Fide Employment Relationships

Anti-Kickback

- Employment
- Personal Services and Management Contracts
- Rental of Office Space and Equipment
- Sale of Practice
- Practitioner Recruitment

Personal Services: Stark

- Stark Personal Services (42 CFR § 411.357(d))
  - Set out in writing, signed by the parties, specifies the services covered by the agreement;
  - Agreement must cover all services to be furnished by the physician (or immediate family member) (requirement for a master list of agreements if there are multiple in place);
  - Services must be reasonable and necessary for legitimate business purposes;
  - Term of each arrangement must be at least 1 year;
  - Compensation to be paid throughout the term if the agreement must be set in advance and is consistent with FMV.
  - Compensation must not be determined in a manner that takes into account the volume or value of referrals (exception for physician incentive plans).

Personal Services: AKS

- **AKS Personal Services and Management Contracts (42 C.F.R. 1001.952(d))** "remuneration" does not include payments made for personal services and management contracts as long as the following requirements are met:
  - Agreement is set out in writing, signed by the parties and is at least for one year;
  - Agreement covers all the services the agent is to provide for the term of the agreement and specifies those services;
  - If the services are periodic then the agreement must specify the length and schedule of such intervals;

Personal Services: AKS

- The aggregate compensation paid to the agent must be set out in advance, consistent with FMV and not determined in a way that takes the value or volume of referrals into account;
- The services cannot be promoting or counseling any activity that violates any state or federal law;
- The aggregate services do not exceed those reasonable and necessary to accomplish the commercially reasonable business purpose of the services.

In Office Ancillary: Stark Only

42 C.F.R. § 411.355(b) –

- DHS services that are provided by [1] a referring physician; [2] a physician who is a member of the group practice or [3] and individual who is supervised by the referring physician or another physician in the group practice (under Medicare's supervision guidelines).

In Office Ancillary: Stark Only

- DHS services must be provided in a centralized building or in the same building in which the referring physician furnishes physician services unrelated to DHS and;
- Such services must be billed by the physician performing or supervising the service; the group practice or a third party billing agent.

In Office Ancillary: Stark Only

New requirement: Any doctor providing PET, MRI, or CT in his/her office must give the patient a written statement explaining they may get the image elsewhere along with a list of alternative providers. See 42 C.F.R. § 411.355(b)(7).

Polling Question 4

If my organization comes close to meeting a Stark Exception, that's okay, as substantial compliance is all that is required.

1. True
2. False

FRIDAY | ELDREDGE & CLARK LLP
www.FridayFirm.com

Recent Stark Law Developments

Generally, Provider-Friendly

- Hospitals can pay a physician up to $5,000 per year without a written agreement;
- "Commercially reasonable" clarification – takes into account the type of entity
- "Volume/Value of Referrals" Clarification – becomes a mathematic equation consideration
- 90-day compliance period for written agreement

Recent Stark Law Developments

Value Based Arrangements

- Greater Risk = Greater Flexibility
- No fair market value requirement.

Polling Question 5

The following is true with regard to false claims:

1. Providers are tasked with "reasonable diligence" to identify overpayments.
2. If an overpayment is identified, there is no reason to report and refund – just fix the problem moving forward.
3. A retained overpayment is called a "Reverse False Claim"
4. Both 1 and 2.
5. Both 1 and 3.

FRIDAY | ELDREDGE & CLARK LLP

www.FridayFirm.com

www.FridayFirm.com

Questions?