KHSC
Kansas Health Service Corporation
Celebrating 40 Years

***KHSC Newsletter***
***May 2025***

## How Ablepay Is Changing the Landscape Related to Patient Receivables

AblePay, one of the newest KHSC-endorsed business partners, is now working with seven Kansas hospitals to positively impact the collection of patient-responsibility amounts from health services. AblePay, based in Allentown, PA, helps bridge the health care affordability gap by boosting revenue for providers while offering patients savings of up to 13 percent on out-of-pocket expenses, flexible payment terms with savings, and 0 percent interest extended payment options. Additionally, AblePay provides advocacy services to assist patients with billing inquiries. AblePay is significantly changing the financial landscape for our KHA members and their patients. One great example of their solution is highlighted below.

## Ephraim McDowell Health Case Study: Improving Revenues and Patient Relationships with AblePay

Ephraim McDowell Health serves patients in six counties in Central Kentucky through three hospitals (two being critical access) and 48 outpatient centers. They have more than 1,700 employees and have 282 million in annual net revenue.

With revenues declining and the cost of collecting patient out-of-pocket responsibility steadily rising, Ephraim McDowell Health searched for a way to improve its patient post-insurance collections.

Ephraim McDowell selected AblePay's unique process to increase revenue, decrease the cost of collections, while also enhancing the experience for their patients. By assuming all payment risks, AblePay not only eliminated the unpredictability of patient payments but also all the associated costs. This positively impacted the health system while patients benefited from the savings, flexible payment options, a convenient payment portal, and billing advocacy provided by AblePay.

The results of the Ephraim case study with AblePay included:

- 106 percent increase in collection rate compared to their historical collection rate.
- 48 percent increase in out-of-pocket revenue per patient.
- 46.2 percent of patients who enrolled in AblePay paid zero on prior bills.
- Days to collect decreased from 107 days to 14 days for AblePay members.

* Statistics Based on Actual Ephraim McDowell Patients Before and After Becoming AblePay Member

To learn more about how to implement AblePay in your hospital, please reach out to Shelly Soupir at shelly.soupir@ablepayhealth.com or (402) 651-2103.

**Price Transparency Compliance Issues Gain Focus in D.C.**
In late February, CorroHealth, a trusted partner of KHSC, deployed an advanced bot to meticulously review all member price transparency files. This initiative was guided by the Centers for Medicare & Medicaid Services' guidelines and utilized the CMS validator tool to ensure compliance. The findings from this review have highlighted several issues that could potentially attract CMS's attention for a compliance review.

The bot conducted a thorough examination focusing on four key areas:

- Placement of the machine-readable file: Ensuring the file is correctly positioned for easy access.
- Compliance with CMS mandated MRF file format: Verifying that the file format adheres to CMS specifications.
- 2024/2025 MRF compliance via CMS validator: Checking future compliance requirements using the CMS validator tool.
- General MRF Accessibility: Assessing the accessibility of the MRF through CMS bots and site crawlers.

The urgency of this matter is underscored by the Feb. 25 Executive Order on health care pricing information, which has brought compliance with these rules back into focus. Executive Order 13877 mandates the disclosure of actual prices for items and services, rather than estimates, within the next 90 days. Additionally, it requires organizations to stay vigilant about forthcoming regulatory changes, including updates to guidance, proposed regulatory actions and enforcement policies.

To address these compliance issues promptly, CorroHealth will proactively reach out to those members whose files were flagged by the bot review. They will provide detailed insights into the findings and guide your organization through the necessary steps to achieve compliance. For further assistance, you can also schedule a meeting with our CorroHealth representative, Violet Archuleta-Chiu.

**Protecting Kansas Health Care Providers : How the Fund Safeguards Kansas Health Care**
KAMMCO is committed to supporting Kansas health care providers by ensuring they have the resources and protections necessary to deliver quality patient care. The Kansas Health Care Stabilization Fund has been a critical safeguard for health care providers and patients.

The latest KAMMCO *Vital Sounds* newsletter article includes a deep dive into the Fund and understanding why it remains an essential part of the Kansas health care landscape. Here's a brief overview of its impact. The article is in the Q1 *Vital Sounds* edition here: https://www.kammco.com/vital-sounds/2025q1/.

**The Fund was Created in Response to a Crisis**
The Fund was created in response to the medical malpractice insurance crisis of the late 1970s and 1980s. Rising insurance costs threatened to drive health care providers out of practice, which could have severely impacted patient access to care.

To address this issue, Kansas lawmakers established the Kansas Health Care Stabilization Fund, designed to ensure health care providers could continue practicing with the liability protection they need.

**How the Fund Works**
The Fund is financed entirely by participating health care providers, without using tax dollars, and offers several key benefits:

- Mandatory Liability Coverage: All qualified health care providers must carry a defined minimum amount of liability insurance coverage.
- A Layer of Financial Protection: An independent fund that provides one of the layers of the required amount of professional liability coverage.
- Guaranteed Access to Insurance: The Kansas Health Care Providers Insurance Availability Plan ensures that every qualified health care provider in Kansas has access to liability insurance, even if the provider cannot receive insurance in the private market.
- Limits on Non-Economic Damages: A statutory cap on non-economic damages in malpractice lawsuits is intended to help maintain stability in the liability system.

**Why This Matters for Kansas Health Care**
The Fund is crucial in maintaining a balanced and sustainable liability environment in Kansas. Without it, we could see the same challenges other states have faced—rising costs, provider shortages and decreased access to care. By offering reliable coverage and legal protections, the Fund helps secure future health care in Kansas.

**Learn More**
For a more detailed look at how the Fund safeguards the Kansas medical community, read *Kansas Fund Safeguards Providers*.

**SunRx Continues to Lead the Way on 340B Education and Resources**
SunRx is excited to introduce a new 340B Spotlight Series! This series offers and presents a brief overview of 340B solutions and services for consideration in managing your 340B strategy. These on-demand videos aim to offer valuable insights to aid decision-making, compliance and optimize your 340B pharmacy program.

Be sure to attend the multi-state 340B Day event on June 12 in Springfield, Missouri.

**Advanced Primary Care Management: What It Is and Frequently Asked Questions**
As of 2025, the Centers for Medicare & Medicaid Services will reimburse practices for offering their new program, Advanced Primary Care Management. Advanced Primary Care Management is a preventative care program for Medicare patients, offered by providers who serve as the patients' focal point of care.

ChartSpan, a care management organization and KHSC partner, has received hundreds of questions about the program. Here are a few of them–and for answers to more questions, you can view the full article here.

Advanced Primary Care Management Services

**Who Is Eligible for APCM?**
Providers can offer APCM to Medicare patients they provide primary care for. There are three levels of APCM:

- Level 1: For patients with one or fewer chronic conditions
- Level 2: For patients with two or more chronic conditions
- Level 3: For patients with two or more chronic conditions and Qualified Medicare Beneficiaries

**What Does APCM include?**
APCM must include multiple service elements:

- Consent: Explain the program to patients, ask patients for their consent to enrolll and record their consent
- Initiating visit: Required for patients who haven’t seen their provider within the past three years
- 24/7/365 access to care: phone or text line for health questions
- Ability to schedule successive appointments with the same care team
- Care in alternative ways, such as home visits or expanded hours
- Comprehensive care management: systematic assessment of medical and psychosocial needs, systems to provide preventative care, and medication reconciliation
- Patient-centered care plan: Available electronically and created in collaboration with patients

- Management of care transitions: Oversee transitions from the hospital, ER, or a skilled nursing facility to home and follow up with patients within seven days
- Community-based care coordination: Form relationships with other practitioners, home- and community-based services to assist patients
- Enhanced communication: Provide multiple patient communication methods, including secure messaging, email, online patient portal, or phone
- Population-level management: Ability to stratify patients into three levels of APCM and identify appropriate, targeted interventions
- Performance measurement: Will be evaluated based on quality measures

**Advanced Primary Care Management Services for All Practices**
Advanced Primary Care Management could improve outcomes for Medicare patients, helping them avoid unnecessary hospitalizations and enhance their quality of life. However, the program requires advanced stratification and quality reporting abilities, as well as in-depth, personalized care management. If you'd like to learn more about effective, compliant APCM, you can view our full article on APCM here. To discuss this further, contact Chris Miller at chris.miller@strategichealthcareadvisors.com or (816) 588-4650.

**KHA Workers' Comp Fund: Strength and Longevity for Kansas Hospital Workers' Compensation Needs**
What Makes the KHA Workers' Compensation Fund Unquietly Different?
For 34 years, the KHA Workers' Compensation Fund has stood out from other carriers – and it's not just our history. As a member-owned organization, KHAWCF focuses on its members' success and safety. Here's why we continue to be unquietly different:

**Strength in Numbers**
With more than 75 health care organizations across Kansas, our members form a powerful network.

**Longevity and Loyalty**
It's not just about being a member. It's about staying a member. Eighty-seven percent of our members have been with us for more than 10 years, and nearly half (46 percent) have trusted KHAWCF for more than 25 years. This loyalty speaks volumes about the value we strive to bring.

**Sustainability**
For years, we've been able to give back to our members. A total of $3 million has been returned to members in dividends, ensuring you benefit from the Fund's success.

**Performance You Can Trust**
The average experience modification (mods) rate of our members is 0.91. This shows our collective commitment to safety and risk management.

**Safety Is a Priority**
Every member has access to our in-house Program Safety Manager, who works closely with the Fund Administrator to identify risk areas by reviewing injury histories in member organizations. This proactive approach helps to reduce claims, lead to better loss history and lower experience mods.

If you want more information about the KHA Workers' Compensation Fund, please contact Steve Poage, spoage@kha-net.org or Ronni Anderson, kanderson@khsc.org at (785) 233-7436.

**Protect Your Hospital from Limited Resources for Compliance Issues: Let Healthdox Help**
U.S. hospitals lose more than $1 trillion annually, with $20 billion tied to compliance failures and unreported incidents. Smaller hospitals face even greater challenges due to limited resources. HealthDox offers a suite of nin customizable solutions that help hospitals streamline compliance, mitigate risk and enhance operational efficiency. Our automation-driven tools reduce administrative burdens and provide real-time insights to keep hospitals ahead of regulatory risks.

We offer tailored AI-based SaaS solutions, including the Risk Incident AI Solution Enterprise, designed to improve incident management and operations. This system provides AI-driven risk scores to identify potential incidents and risks proactively. They also provide customized Power BI dashboards to reflect real-time data.  Their solutions are designed to help health care organizations improve patient safety and operational efficiency.

For more information, visit www.healthdox.com or contact@HealthDox.com. Let's improve patient care and operational performance together!

**Six Ways Legacy Systems Expose Health Care Organizations to Security Risks**
What is a legacy system? A legacy system refers to an information system that is considered outdated or obsolete. Commonly used legacy systems include electronic health records, billing systems and various administrative tools that were implemented years ago and have not undergone updates or have been replaced with newer information systems.

*Cyberattacks in health care continue to cause significant turbulence. The U.S. Department of Health and Human Services Office of Civil Rights reported a 264 percent increase in health care ransomware attacks over the past five years. Hospitals and health care organizations are facing a massive increase in ransomware worldwide, and especially in the United States, with a 73 percent increase in attacks. These attacks on critical systems force the cancellation of surgeries, exams and sometimes even halt the entire health system's operations. The impact of recovering from a breach includes the actual cost of time, equipment and consultants, plus the challenges of reputation repair. To fight off cybercrimes before they happen, a health care organization should examine its weak links, starting with its legacy systems.*

Electronic health record systems have an important and expanding responsibility to enable interoperability (record sharing) between providers, payers, patients and other users. However, many EHRs, developed years ago, are not able to deliver on current and future needs and will be upgraded or replaced.

Upgrading or replacing an EHR is only part of the solution. Currently, 73 percent of health care providers still use legacy information systems, and the average organization has nearly 1,000 unique applications in use. Beyond the technical limitations, legacy systems are a leading bad practice for health care security, according to the Cybersecurity and Infrastructure Security Agency. Health care is a leading target for cyberattacks, and legacy technology is reported as the third-biggest security challenge facing health care cybersecurity programs.

It is imperative to review the entire IT landscape for security risks and make necessary changes. Six significant security risks lurking in legacy systems.

- **Easy Back-Door Entry** – Unsupported or end-of-life systems with silos of data stored in outdated systems are the easiest entry points for hackers. Network servers are the target for more than 50 percent of all hacking-related breaches. Poor security protocols and weak infrastructure make it easy for a hacker to gain access to a legacy system and then move freely throughout the network. There can be upwards of 30-40 legacy systems running in maintenance mode at a health system that is the equivalent of having unlocked doors and windows ripe for an attack.
- **Lack of Vendor Support** – With outdated systems, there often is a lack of regular security updates, which leaves them open to cyberattacks. A lack of support from the manufacturer means a lack of available security patches.
- **Technical Risk** – Legacy software kept running in read-only mode is ripe for corruption, breakdown, cyberattack or even internal threats. There may also be a lack of internal system experts who are familiar with how to operate the legacy system, which can further complicate workflows.
- **Non-Compliance with HIPAA** – Legacy systems may not be HIPAA compliant, which increases the risk of potential breaches and leaves the organization vulnerable to penalties and sanctions. The HIPAA Security Rule requires covered entities and their business associates to implement safeguards that reasonably and appropriately secure electronic patient health information that these organizations create, receive, maintain or transmit. Legacy systems can make patient and other records vulnerable during a cyber or phishing attack.
- **Absence of Monitoring Capabilities** – Many legacy systems are not equipped to monitor and audit user activity, data access and use. Most older systems were designed for easy data access, as security was not as big a factor when the systems were implemented.

- **Internal Threats** – Legacy systems often have limited security protocols, which create an opportunity for employee mistakes or insider threats. These two categories are responsible for most health care system breaches. The average health care organization has 31,000 sensitive files (which is about 20 percent of all files and include HIPAA-protected information, financial data and proprietary research) that are open to everyone in the organization.

**How to Improve Cybersecurity Preparedness for a Health Care Organization**
The first step is to follow the HIPAA Security Toolkit. This will help the organization take stock and manage its ongoing risk. The next critical step is to become HITRUST CSF certified. This globally recognized standard provides a comprehensive, flexible and efficient approach to regulatory standards compliance and risk.

With these two frameworks in place, it is recommended to centralize legacy data into an active archive like HealthData Archiver®. This helps ensure the organization meets regulatory requirements that can include record retention of six to 30 years or more while also allowing legacy systems to be decommissioned. A streamlined portfolio offers a host of security, cost and other benefits.

The Harmony Healthcare IT team of data extraction and migration experts have helped hundreds of health care delivery organizations decommission legacy systems and safely consolidate patient, employee and business records from more than 550 different clinical, financial and administrative software brands.

For more information about securing legacy health care data and deflecting cyberattacks, check out this white paper: *Security Focus Creating a Legacy Data Management Plan* and the 10 privacy and security questions to ask an archiving partner. With 87 percent of health care's security issues in the last 12 months involving a third-party breach, it is critical to scrutinize every supporting organization and utilize best practices for third-party risk management.

Beyond the obvious reasons to take cybersecurity seriously, the Department of Health and Human Services released 10 essential and 10 enhanced cybersecurity performance goals designed to better protect the health care sector from cyberattacks. The guidance is expected to include financial penalties in the form of reduced payments to certain hospitals that fail to meet cybersecurity standards beginning in fiscal year 2029.

If you are ready to move forward with a legacy data management strategy, we are ready to help. Let's connect. Patrick Regan at pregan@harmonyIT.com or (406) 853-3087.