October 2024 – Vol. 40 No. 10
Published for Health Care Providers by ACA International
www.acainternational.org

PULSE

AGENCY OF CREDIT CONTROL

Minnesota Debt Fairness Act Requirements in Effect

Components of the comprehensive bill–including medical debt collection reforms related to spousal liability, credit reporting and consumer disclosures–took effect Oct. 1.

Several components of the Minnesota Debt Fairness Act related to medical debt collection reforms took effect Oct. 1, 2024.

Sections of the law, SF 4097, in effect include:

- Section 26 [62J.806], which requires health care providers to make their policy for medical debt collections available to the public and specifies health care providers' procedures to communicate with patients about medical debt owed and collecting medical debt, referrals to a collection agency and identifying the debt as uncollectible or satisfied.
- Section 126.14 – 131.9, with definitions enforceable by the attorney general on what qualifies as medical debt, such as a debt charged to a credit card.
- Section 134.1-144.9, which outlines that a spouse is not liable to a creditor for any debts of their spouse as well as garnishment provisions.

The bill also prohibits collecting parties from reporting a medical debt to a credit reporting agency (CRA), effective Oct. 1, 2024.

Great Lakes Credit and Collection Association (GLCCA) members recently discussed the implications of the Minnesota Fairness Debt Act on debt collection, including the expansion of the definition of a "collecting party," the eradication of spousal liability, and the complexities of medical debt reporting. They also addressed the potential impact of the new legislation on health care providers, the need for policy updates, and the implications of the new sliding scale for wage garnishment.

Health care provider clients working with agencies in Minnesota should review their policies and procedures on spousal communications under the Fair Debt Collection Practices Act. They should also ensure account notices are sent to the correct person, especially if clients are going to pursue collection lawsuits.

Sec. 78 [332C.02] (18) on prohibited practices under the Minnesota Debt Fairness Act also took effect Oct. 1, including an important distinction on disclosures.

Agencies contacting a Minnesota consumer by mail to collect a medical debt must identify the Minnesota Attorney General's general telephone number and state, "You have the right to hire your own attorney to represent you in this matter."

Continued on pg 2

This disclosure should be made by the creditor, debt collector and any new debt collector that takes the consumer's account.

Providers and agencies working in Minnesota should also discuss Sec. 27 [62J.807], which is about denial of health treatment or services due to medical debt.

"A health care provider must not deny medically necessary health treatment or services to a patient or any member of the patient's family or household because of current or previous outstanding medical debt owed by the patient or any member of the patient's family or household to the health care provider, regardless of whether the health treatment or service may be available from another health care provider," it states.

A provider may require the patient to enroll in a payment plan for the outstanding medical debt owed as a condition of providing medically necessary care.

Regarding credit reporting, it is prohibited to report a medical debt to a credit reporting agency (CRA).

CRAs are also prohibited from making a consumer report containing an item of information that it knows or should know concerns medical information or debt arising from the provision of medical care, treatment, services, devices, medicines; or procedures to maintain, diagnose, or treat a person's physical or mental health.

Agencies should closely review policies and procedures on credit reporting medical debt that originates outside of Minnesota, but that is owed by a Minnesota resident. The credit reporting prohibitions apply to debt collection agencies and debt buyers licensed under Chapter 332.

What's Next?

Section 332.3351 on out-of-state licensure exemptions was amended to include some level of reciprocity for states with similar licensing requirements and will take effect on Jan. 1, 2025.

Limitations on wage garnishment in Sec. 571.922 will take effect on April 1, 2025.

This report does not cover all the components of the law taking effect this year and next year.

ACA International will provide updates on the law in ACA Daily.

Ransomware Threats Rise in Health Care

Despite a fall in overall data breach costs, health care recovery costs averaged $9.77 million this year.

According to a recent 2024 IBM Cost of a Data Breach Report, the global average cost of a data breach increased by 10% this year, reaching $4.88 million. However, in the health care sector, data breach costs dropped by 10.6%, yet health care continues to face the highest breach recovery costs, averaging $9.77 million.

A key factor in this cost disparity is the rise of ransomware attacks, which nearly doubled between 2022 and 2023. High-profile incidents, such as attacks on Change Healthcare and Ascension, highlight how ransomware is pressuring health care companies to pay large sums to avoid disruption.

Why Ransomware Targets Health Care

Health care data is uniquely valuable not just financially, but also physically. Ransomware that encrypts patient information can cause critical delays in treatment, putting patient lives at risk. This urgency often forces health care companies to pay ransoms rather than risk operational failures, even without guarantees of data recovery. The pressure from both internal leadership and patient families further complicates the decision-making process, making health care organizations more likely to comply with attackers' demands compared to other industries.

Hackers primarily aim to encrypt and exfiltrate sensitive health care data, including electronic medical records (EMR), insurance details, financial information, and Social Security numbers. Disrupting access to these records can severely hinder health care operations, leading to regulatory issues and, in extreme cases, putting patients' lives in danger. Health care breaches have a unique severity compared to other sectors since compromised data can lead to significant physical harm, making it harder for health care providers to recover their reputations.

Continued on page 3

NEWS & NOTES

Health Equity Improvements Could Add $2.8 Trillion to U.S. GDP by 2040

A Deloitte report reveals that improving health equity could significantly boost the U.S. economy, potentially adding $2.8 trillion to GDP by 2040, and increasing corporate profits by an estimated $763 billion. The report suggests that addressing health disparities would also prevent 5 million people from leaving the workforce due to premature death or disability. Health inequities currently cost the U.S. $451 billion, mainly due to lost productivity and premature deaths, with direct medical costs tied to disparities amounting to $320 billion. If health disparities are not addressed, these medical costs could rise to $1 trillion by 2040.

Deloitte argues that businesses across sectors, including agriculture, manufacturing, retail, and technology, stand to gain economically by making health equity a priority in their operations and community engagement. Healthy employees are more productive, leading to higher output and reduced absenteeism. Given that 80% of health is influenced by social determinants, the report urges companies to join cross-sector efforts to improve health equity, as this will benefit both workforce productivity and economic growth.

Read more here.

Health Care CFOs Optimistic for 2024 Despite Financial Challenges

Health care chief financial officers are optimistic about financial growth in 2024, with 79% anticipating revenue increases and 78% expecting improved profitability, according to BDO's "2024 Healthcare CFO Outlook Survey" of 100 CFOs.

However, BDO warns that regulatory pressures, COVID-19 funding returns, and challenging bond and loan covenant agreements may temper these expectations. Concerns about covenant violations and limited cash reserves (only 35% of organizations have over 60 days of cash) indicate potential financial strain, prompting CFOs to focus on revenue cycle management, cost reductions, and operating model transformations. Technology and dealmaking are key areas of focus for health care finance leaders. Nearly half of CFOs plan to increase tech spending, particularly in AI and robotic process automation, which are being used to enhance efficiency in both front- and back-office operations. Generative AI, in particular, is gaining traction, with 98% of CFOs piloting its use and 46% building proprietary platforms. CFOs also have dealmaking high on their agenda, though challenges like due diligence and valuation gaps may complicate mergers and acquisitions this year.

Read more from the report here.

Ransomware Threats cont. from page 2

Additionally, most health care breaches are caused by external threats, with 52% of attacks attributed to malicious actors, compared to 26% from human error and 22% from IT failures. The most common methods include social engineering, phishing, business email compromise (BEC), distributed denial-of-service (DDoS) attacks, and botnets.

Health care's reliance on outdated technology and a shortage of IT security staff makes it more vulnerable to attacks, according to the IBM report. Only 14% of health care organizations report being fully staffed, with over half stating they need more help. These shortages create gaps in cybersecurity defense, leaving organizations susceptible to breaches that may remain undetected for extended periods.

The Rise in Ransomware

The success of recent attacks has emboldened cybercriminals. In early 2024, the BlackCat group attacked Change Healthcare, leading to a $22 million ransom payment and total projected losses exceeding $1.5 billion. Another attack in May 2024 struck Ascension, locking providers out of critical systems that track medication and treatment plans.

The increasing success of these attacks has led to a rise in both sophisticated and amateur hackers. Those with coding skills are developing their own ransomware, while others buy pre-made malware on the dark web. This trend is accelerating the frequency of ransomware incidents across the health care industry.

What's Next?

IBM suggests health care organizations can reduce ransomware risks through protection and detection strategies, including anti-spoofing and email verification tools to limit the reach of phishing attacks. By flagging certain high-risk phrases, organizations can prevent malicious emails from reaching users' inboxes.

Detection can also be enhanced using artificial intelligence and automated tools to identify breaches more quickly. Health care companies that implemented AI and automation saw breaches detected and contained 98 days faster than those that didn't, saving an average of nearly $1 million.

Read more here.

DATAWATCH

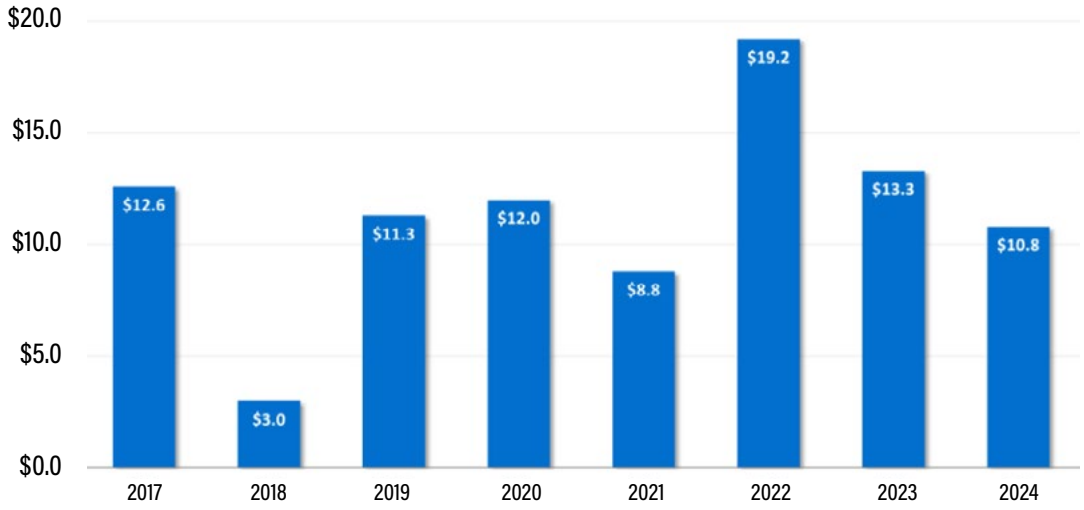
M&A Activity Slows Down in Q2 2024 But Features Significant Transactions

Kaufman Hall's latest quarterly M&A report finds that activity in the second quarter of 2024 slowed compared to the busy first quarter of the year, with only 11 announced transactions, a number below recent Q2 averages.

However, two mega mergers, where the smaller party had annual revenues of $1 billion or more, contributed to a significant increase in the average seller size by revenue. These large deals were strategically focused on gaining access to new technologies and supporting system reconfigurations, rather than simply pursuing scale.

Despite the lower number of transactions, the average seller size in Q2 was close to $1 billion, marking a 161% growth since 2017. The quarter's deals included a mix of acquirers, with three religiously affiliated, two academic, and six other not-for-profit health systems involved.

Total Q2 Transacted Revenue ($ in Billions) by Year, 2017 - 2024



Source: *M&A Quarterly Activity Report: Q2 2024.* https://tinyurl.com/3vbv47ua

PULSE

is a monthly bulletin that contains information important to health care credit and collection personnel. Readers are invited to send comments and contributions to:

Communications Department
ACA International
3200 Courthouse Lane
Eagan, MN 55121
comm@acainternational.org

ACA® INTERNATIONAL
The Association of Credit and Collection Professionals