October 2019 – Vol. 35 No. 10
Published for Health Care Providers by ACA International
www.acainternational.org

pulse

Costs of Data Breaches Growing Across Health Care Industry

Enforcement of data security practices and breach prevention is an increased focus at HHS.

The costs of data breaches in the health care industry are extensive for providers, insurance companies and business associate partners in the accounts receivable management industry.

"I've seen estimates of over $5 billion in costs to the health care industry annually," Lisa Rivera, a partner at Bass, Berry and Sims who focuses on health care security, said in an article from *Healthcare Finance* titled "Healthcare's Number One Financial Issue is Cybersecurity."

After a data breach earlier this summer, the parent company for American Medical Collection Agency (AMCA), Retrieval-Masters Credit Bureau Inc., filed for Chapter 11 protection after a data breach leading to possible unauthorized access to consumers' personal, financial and medical information, ACA International previously reported.

AMCA, in a statement provided to ACA, said it continues to investigate the data incident resulting from an unauthorized user's access to the company's system that reportedly impacted millions of patient records.

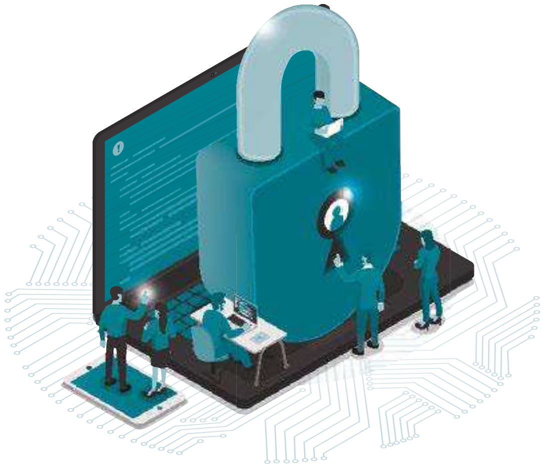
The ongoing and extensive impact of the AMCA data breach and those impacting other industries is another sign that data breach prevention policies and procedures and cyberattack responses need to be airtight and reviewed on a regular basis.

"Every sector of business has attacks, but health care is experiencing the largest growth of cyberattacks because of the nature of its information," Rivera said in the *Healthcare Finance* article. "It's more valuable on the dark web."

Tim Dressen, ACA's communications consultant, reports in the August issue of *Collector* magazine that the number of enforcement actions and their settlement amounts will likely grow as the U.S. Department of Health and Human Services (HHS) seeks to penalize organizations that fail to sufficiently protect patient data.

In 2018, the Office of Civil Rights at HHS settled 10 Health Insurance Portability and Accountability Act (HIPAA) cases and was granted summary judgment in another, Dressen reports. Together, these enforcement actions totaled $28.7 million, surpassing the agency's previous record of $23.5 million in 2016.

In the first half of this year, HHS was already investigating well over 100 reported HIPAA breaches affecting 500 or more people by health care providers and their business associates.



There are growing risks with protecting consumer, patient and client data, but ACA has resources to help mitigate those risks and stay on top of regulations and trends in health care collections.

Certified Instructors Leslie Bender, IFCCE, CCCO, CIPP/US, chief strategy officer and general counsel at BCA Financial Services Inc., and Michael O'Meara, president, The O'Meara Law Office PS, led the CORE Curriculum Seminar, Data Security and Privacy I, in September to provide tools necessary to implement effective policies and procedures.

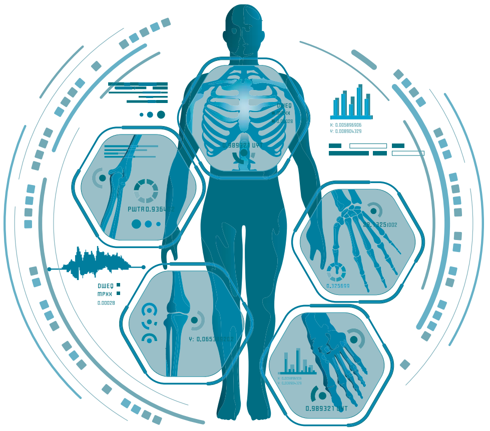
The webinar included guidance on how to notify consumers in the event of a data breach and explore essential

continued on page 2

WASHINGTON UPDATE

Trump Executive Order Opens Door for Hospital Price Transparency

CMS Takes Action to Implement Key Elements of Trump's Plan to Empower Patients with Price Transparency and Low Costs



The Centers for Medicare & Medicaid Services in July proposed a rule that would require hospitals to make pricing information publicly available. It is CMS's position that the rule would increase competition by enabling patients to shop for health care that meets their needs and budgets.

The proposed rule follows President Donald Trump's June Executive Order that "lays the foundation for a patient-driven health care system," according to a press release issued by CMS. Trump's executive order states, "Opaque pricing structures may benefit powerful special interest groups, such as large hospitals and insurance companies, but they generally leave patients and taxpayers worse off than would a more transparent system."

Indeed, a statement released by Alex Azar, secretary of U.S. Department of Health and Human Services, noted that "healthcare leaders across the political spectrum have been talking about this need for real transparency for years. This proposal is now the most significant step any president has ever taken to deliver transparency and put patients in control of their care."

The proposals for calendar year 2020 include changes that would require hospitals to take the following actions:

- Make public "standard charges" for all items and services provided by the hospital.
- Publish standard charges on the internet in a machine-readable file that includes common billing or accounting codes and a description of the item or service. This provides a common framework for comparing standard charges from hospital to hospital.
- Publish payer-specific negotiated charges for common shoppable services (e.g., x-rays, outpatient visits).

To ensure that hospitals comply with the requirements, the rule proposes new enforcement tools including monitoring, auditing, corrective action plans and civil monetary penalties of $300 per day.

Additional information, including a list of public comments submitted, may be found on the federal register website at www.federalregister.gov or (https://tinyurl.com/y5zywwhs, comments were due Sept. 27, 2019) or at CMS's website at www.cms.gov. To read President Trump's executive order, visit www.whitehouse.gov and search for "Executive Order on Improving Price and Quality Transparency in American Healthcare to Put Patients First."

Cost of Data Breaches *cont. from page 1*

safeguards and strategies to develop a Data Security Compliance Program.

In an interview with Dressen, Bender outlined why it is important to have a full understanding of where your sensitive data are stored and how it's transmitted.

"You may think you keep everything in your collection software, but do you really?" Bender asked. "Where are all the places in your organization where nonpublic information is allowed to reside? Is there any data stored in spreadsheets? Do employees have Notepad on their computers, where they may have copied and pasted information? Is there anything preventing them from sending nonpublic consumer data using email?"

There are all important questions to ask and the focus of ACA's CORE curriculum on data security and privacy.

In a separate webinar titled, CORE Curriculum: Healthcare Collection Management, certified Instructors Beth Conklin, account executive at State Collection Service Inc., and Irene Hoheusle, vice president of collections and education at Account Recovery Specialists Inc., discussed the difference between health care collections and other collection practices and specific strategies in self-pay and Medicare accounts.

Hoheusle also recently discussed tips to approach health care collections and training on ACA Cast.

Meanwhile, more coverage on Protecting Health Care Data is also available in the August issue of *Collector* magazine.

ACA also recently updated SearchPoint™ documents on credit reporting and hospital collection practices for members.

Links of interest: Healthcare Finance News may be accessed at: www.healthcarefinancenews.com

Learn more about ACA's events and seminars at www.acainternational.org under the events tab (check out the Training Zone), while *Collector* magazine and ACA Cast may be accessed via the homepage.

DATA PRIVACY

Poll Shows a Majority of Americans Worry About Hackers

While study respondents express misgivings about data privacy when it comes to social media and internet search engines, they believe their private health information will more likely remain secure.

Given the constant news about data breaches that compromise personal information, it is no wonder that Americans are increasingly squeamish about being hacked.

A new poll conducted by POLITICO and the Harvard T.H. Chan School of Public Health found that a majority of American adults worry about hackers gaining access to their Social Security number and credit card information. When asked about which institutions they trust to protect their personal information, health care organizations such as doctor's offices and hospitals ranked high, while most poll respondents expressed little trust that internet search engines and social media companies would keep their information safe, the study titled "Americans' Views on Data Privacy & E-Cigarettes," said.

More than half of adults said they were very concerned that unauthorized people may gain access to their Social Security number (63%) or their credit card number (57%).

Among users of social media, 13% said they were very concerned that content they have posted on sites like Facebook, Twitter or Instagram in the past may come back to harm or embarrass them in the future, and 14% were somewhat concerned.

The poll also asked a series of questions about data privacy as it applies to health information or products that adults may have searched for privately online. Among adults who said they have searched for health information or health products online, 30% were very concerned that a company would use their search information to try to sell them medical products or treatments. More than a quarter (28%) said they were very concerned such information may make it harder for them to get medical care, and one in four (25%) said they were very concerned that private search information may come back to hurt their chances of getting a job or health insurance, according to the study report.

Many Americans do not just search for health information online; they also obtain personal health information through patient portals. These secure websites give patients 24-hour access to their health information from anywhere in the world with an internet connection. The poll found that about a quarter (23%) of adults have ever set up a patient portal. When asked what they use their patient portal for, the vast majority (81%) of adults said say they used theirs to see test results. More than half (59%) have used it to schedule an appointment, while 42% had requested a prescription refill and 40% received advice about a health problem using their patient portals. The study also showed that most respondents did not express a great deal of concern about potential hacking of patient portals.

About one in four (26%) patient portal users said they were very concerned that unauthorized people may be able to gain access to the private information contained in their portal. Meanwhile, 15% of users said they were not concerned about such a scenario at all.

NEWS & NOTES

Humana to expand in-network offerings to MA customers in Michigan hospital group

Humana reached an agreement in August with the Michigan-based hospital network McLaren Health Care to expand in-network options for the insurer's Medicare Advantage customers. The agreement represents the latest effort by Humana to attempt to expand in MA, a business that has grown for the insurance giant beyond expectations this year. McLaren is a network of 14 hospitals located in Michigan. Humana already contracted with six of the hospitals in the system to offer in-network options for MA and now has an agreement to add in-network access for eight more. Read more here: https://tinyurl.com/y3tgzeot

NTY: Inside NC's Effort to Change Health Care

The Tar Heel state "has embarked on one of the country's most ambitious efforts to transform how health care is defined and paid for," according to a New York Times article titled, "Inside North Carolina's Big Effort to Transform Health Care." North Carolina is in the early stages of turning away from the traditional fee-for-service model, in which doctors and hospitals are paid for each office visit, test or operation, according to writer Steve Lohr. Instead, providers will often be paid based on health outcomes like controlling diabetes patients' blood sugar or heart patients' cholesterol. The better the providers do, the more they can earn. If they perform poorly, money could eventually come out of their pocket, Lohr reports. The entire article may be accessed by clicking here: https://tinyurl.com/y53dmypw

datawatch

Americans' Lack of Trust in Institutional Data Security, by Party

(percentage who say they have a great deal of trust in institutions to keep their information secure)

	Total	Dems	Reps	Inds
Your doctor's office	34	36	37	31
Your primary bank	29	29	29	28
Hospitals you use	24	28	26	19
Health insurance companies	17	22	17	13
Your cellphone carrier or operating system	12	11	11	15
Credit card companies	12	13	18	5
Your personal or work email provider like Gmail or Outlook	11	9	16	11
Online retailers like Amazon or Walmart	11	7	15	13
The federal government	9	9	9	11
Internet search engines like Google	7	7	7	8
Social media companies like Facebook, Twitter or Instagram	3	3	3	2

Source: POLITICO/Harvard T.H. Chan School of Public Health

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
P.O. Box 390106
Minneapolis, MN 55439-0106
comm@acainternational.org

Note: Requests for reprints or additional information on material herein must be made through the ACA International member who sponsored your receipt of this publication.

Do we have your correct name, title and address? Please advise your sponsor of any corrections.

This information is not to be construed as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure that this information is up to date as of the date of publication. It is not intended to be a full and exhaustive explanation of the law in any area. This information is not intended as legal advice and may not be used as legal advice. It should not be used to replace the advice of your own legal counsel.

ACA®
INTERNATIONAL
The Association of Credit and Collection Professionals