The Cure to Improve and Protect Health Care Records

BY SCOTT BAGWELL

"Priorities are the same across industries—minimize risk and cut costs while making systems and processes function better. Just as the financial industry had to adjust to a move to electronic transactions, so, too, does the health care industry."

MEDICAL identification theft has increased by 21.7% since 2013 and, over the past two years, 65% of health care organizations have experienced a cyber attack, according to a Ponemon Institute study sponsored by the Medical Identity Fraud Alliance. These numbers are disconcerting, and reflect a dangerous new pattern in cyber crime, as identity thieves expand their targets from the financial sector into health care. What is more unsettling is the vulnerability of this data to things as simple as human fallibility. Indeed, according to the Department of Health and Human Services, 94% of health care data breaches are the result of simple human transgressions.

In the health field, information security vulnerabilities are even more concerning because these security slips, hacks, and instances of compromised data overshadow the enormous potential for the good that Big Data holds for health care. Digitizing health records promises to bring the computing power of Big Data to bear on tough health care problems. A digital system streamlines patient data, improves the quality and ease of care, and reduces costs at a time when health care expenditures are soaring.

From the moment a prospective patient arrives for treatment or accesses his or her patient portal remotely, it is data that accurately can determine what insurance or financial assistance benefits may be available. It is identity-matching tools that can confirm whether that person is, in fact, the individual he or she claims to be. Further, it is data that can assess the risk of a patient's remote interaction by analyzing device and usage characteristics. These interactions are logged, analyzed, and correlated across the millions of other websites being accessed in the banking, financial services, and other industries. By looking for patterns in this enormous dataset, anomalies and outliers can be detected that may indicate someone inappropriately trying to gain access into these systems.

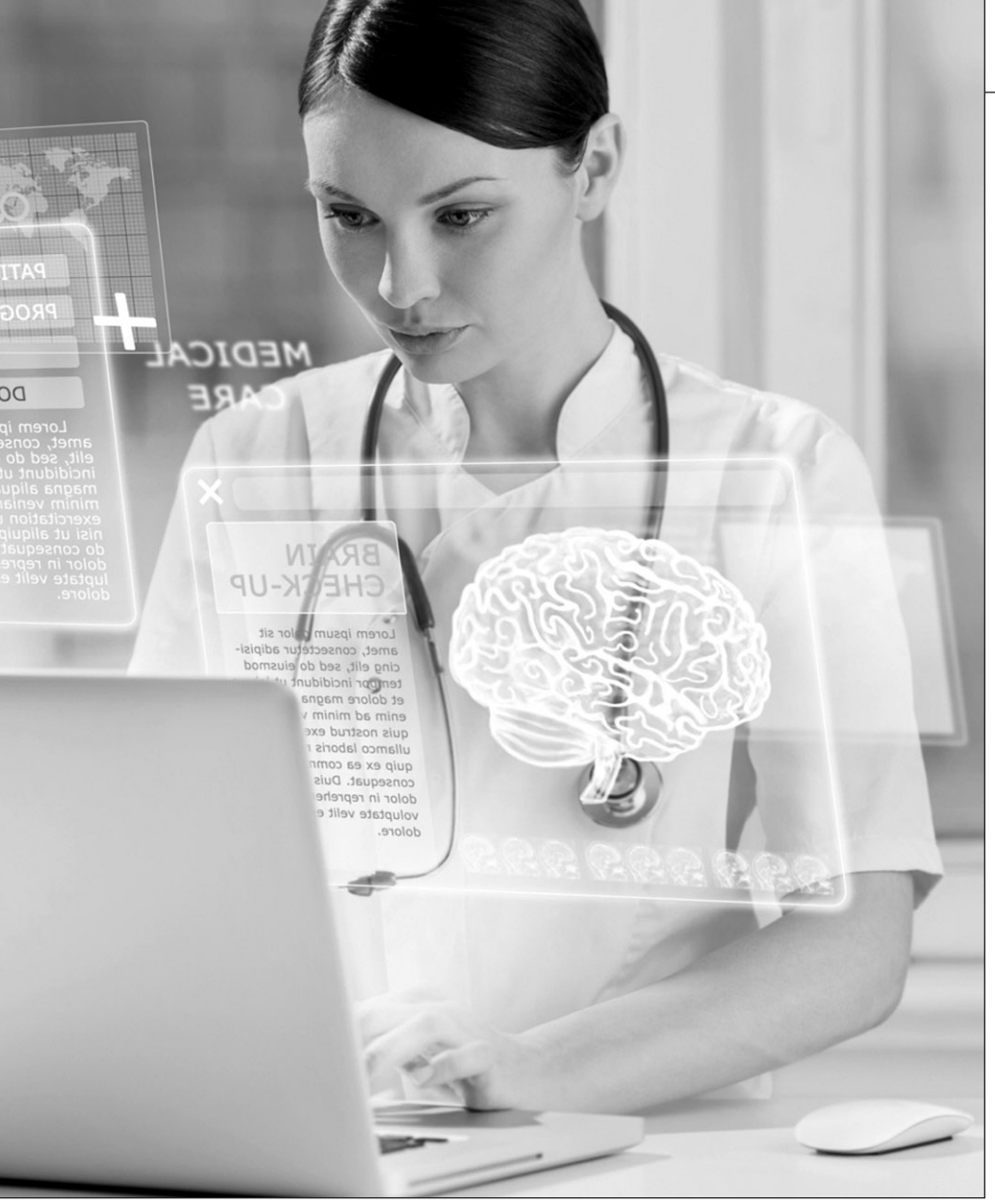
However, the rapid shift to digital and the legislative and policy changes put in place to encourage electronic health records have caused issues of their own. The Hi-Tech Act, which offered financial incentives to invest in technology, along with the process changes brought by the Patient Protection and Affordable Care Act, have coincided with dramatic technology advances.

While these portals are improving patient engagement and offering greater efficiency, security requirements often are at odds with the patient experience. To comply with the Health Insurance Portability and Accountability Act (of 1996) and protect patients, health care organizations are being required to tighten security policies. However, these requirements and additional security can deter patient use and make the consumer experience complicated.

The speed of this shift also has created security and privacy risks. For hospital executives and IT administrators, there barely has been time to understand the digital transformation of their information, let alone prioritize their task lists. Providers have moved so rapidly into the digital space that many failed to deploy the same robust security measures taken by their banking counterparts. The scramble to digitize patient records has been handled in such a piecemeal fashion that it has left systems and data vulnerable to attack.

So vulnerable that, according to Reuters, the FBI released a private notice to the health care industry warning providers that their cyber security systems are lax compared to other sectors. The memo reportedly stated, "The health care industry is not as resilient to cyber intrusions compared to financial and retail sectors, therefore the possibilities of increased cyber intrusions is likely."

A survey conducted by the health care Information and Management Systems Society maintains that 64% of health care information technology leaders cite "a lack of appropriate cyber security personnel" as the top barrier to mitigating cyber threats. A lack of financial resources is a barrier for 60% of executives, while 42% cite "too many emerging and new threats to track." In other words, a majority of the survey respondents felt the tools they cur-



rently have available are not sufficient to protect against the growing number of complex threats and vulnerabilities both today and in the future.

Today's unprecedented access to information is not helping. Patients now can review their health information from almost anywhere thanks to the widespread use of patient portals and mobile devices. With providers, payers, pharmacies, labs, and patients all having access to sensitive records, information security becomes vulnerable to the weakest link in the data chain.

Moreover, health records are extremely valuable targets. On the black market, one Medicare number can sell for close to $500—compared to $10 for a stolen credit card number. The jump in value is to be expected when you consider all the information at stake. These records include names, birth dates, Social Security numbers, policy numbers, and billing information that can be used for a number of illicit—and profitable—activities. With medical information, hackers can open multiple credit lines, create fraudulent identifications, and purchase medical equipment or pharmaceuticals—and, because some health data theft can go undetected for months, so, too, can the theft.

What is the solution? How do we bring Big Data capabilities to the health industry in a way that is safe and secure? Should security trump the shift to digital records and online access? Absolutely not. The data being collected and created holds so much potential to improve health systems—and there are tools to harness it and use it for good.

Given the potential impact on patient quality of care—when a medical identity is stolen and used by another to receive treatment, medical records can become commingled and the result can be life-threatening—basic password protection is insufficient. The recommended approach is a multilayered solution that incorporates multiple measures, including the seamless integration of device recognition, identity proofing analytics, and fraud management.

Indeed, the same tools that harness Big Data also can minimize the potential for fraud and data theft and help protect the data that promises to improve health outcomes. Other major industries—including financial services, telecommunications, and insurance—have been using Big Data and analytics for years to protect their online portals, minimize risk, and reduce fraud losses.

When applied in a health care setting, it is these same techniques that will enable professionals to gain insights that can be turned into actions to protect patient data. For example, there are tools that allow systems to authenticate patients during enrollment without burdening them with long wait times or complex processes. These identity-matching tools can confirm whether a patient or a physician is who he or she claims to be. At the same time, analyzing data and usage characteristics can assess the risk of a patient's remote interaction more effectively.

These sorts of systems and tools offer patients convenience and protection whenever and however they want to access their portal information and, when unusual activity does occur, the system automatically alerts staff. One solution leverages a robust and time-tested matching algorithm and enforces accuracy standards to establish a universal patient identifier, enabling health care systems with disparate databases, systems, and data formats to share a single view of the patient to improve the safety, speed, and quality of patient care—and this also helps to reduce health care expenses.

In a report sponsored by IBM, it was estimated that, around the world, a health care breach costs an average of $363 for every exposed record. In the U.S., the number jumps to $398. In contrast, the average cost of a data breach across all industries is $154. Health and finance specialists predict that medical identity theft will cost the industry $5,600,000,000 this year alone.

The broad deployment of health care portals and the lucrative nature of the data they hold nearly ensure that they increasingly will be targeted by cyber criminals in coming years. Health care-related data breaches already are 10 times more frequent than data breaches in the financial services sector, and medical identity theft accounts for 43% of all identity theft. Utilizing new technology offers multiple linking and search tools for correlating devices and impersonated identities and linking their activities to help safeguard consumers and systems.

Priorities are the same across industries—minimize risk and cut costs while making systems and processes function better. Just as the financial industry had to adjust to a move to electronic transactions, so, too, does the health care industry. The same security that protects the billions of transactions and trillions of dollars that are moved digitally needs to assure the public that its health information is protected. These same approaches should be undertaken in health care to protect our health records better and ensure that we can build a Big Data capability that ultimately will improve patient outcomes. ★

Scott Bagwell *is president of Experian Health, Costa Mesa, Calif.*