How a strong compliance culture affects whistleblowers

an interview with Stephen Cohen
Former Associate Director, Enforcement Division
Securities and Exchange Commission;
Partner, Sidley Austin LLP

See page 16

25
Auditing the hospital 340B drug program
Matthew Atkins

32
Engaging the board in compliance
Marti Arvin

37
The Internet of Medical Things: Cybersecurity and diabetes device risks
Miles Johnson, Scott Thiel, and Jennifer Mitchell

45
Using consultants is fraught with danger—choose wisely
Paul P. Jesep

This article, published in Compliance Today, appears here with permission from the Health Care Compliance Association. Call HCCA at 888-580-8373 with reprint requests.
The SEC’s whistleblower program has been a force multiplier for its enforcement efforts as evidenced by the fact that they’ve surpassed $142 million in awards in cases yielding nearly $1 billion in financial remedies.

See page 19

ARTICLES

51 [CEU] Creating and maintaining a culture of confidentiality by Carlos A. Cruz and Melissa J. Mitchell

HIPAA was enacted before the social media revolution, but training on privacy and security policies must keep pace with changing times.

56 Compliant retention of research records by Molly J. Dowden, Linda M. Jaros, and Jeffrey M. Joyce

Archiving and retention requirements may vary, so be sure your archive tracking system covers both on- and off-site storage.

61 Chronic care management: New risks, new opportunities by Ryan Haggerty, Ryan J. DeMerlis, and Peter A. Khoury

Payments for CCM services are intended to support care management for Medicare beneficiaries who have more complex and time-consuming multiple chronic conditions.

65 The other annual work plan, Part 3 by Anne Van Dusen, Walter E. Johnson, and Frank Ruelas

Why physical fitness should be an integral part of your personal development plan every year.

68 [CEU] Confidentiality: 42 CFR Part 2 versus HIPAA by Dorothy P. Pickles

The rules for disclosing protected health information are different for substance abuse programs.

73 Cyber criminals’ hot commodity: Pediatric patient data by Robert Lord

Children in the United States are 51 times more likely to have their identity stolen than adults.
Electronic health records (EHRs) have become a prime target for cyber criminals, with many experts agreeing that the healthcare industry is considerably behind other industries when it comes to cybersecurity. The increasing number of successful attacks on patient data is evidence that criminals are taking advantage of healthcare’s inadequate security, and it is the patients who are feeling the greatest effects of a hospital data breach.

Unfortunately, pediatric patient data is not only more vulnerable, it is also quite valuable on the Dark Web, making it an easy and profitable asset for criminals. In the case of pediatric patients, the threat is even greater, because the medical records of these young patients provide criminals a blank slate upon which they can build a false identity. This—combined with the fact that medical identity theft of pediatric patients is incredibly hard to detect—means that criminals have a much longer time period with which to profit from the stolen information, costing the victim hundreds of hours and thousands of dollars.

The Dark Web is a scary place for patient data
Protected health information (PHI) is incredibly valuable to cyber criminals for two main reasons:

1. This information can be used for a wide variety of illegal purposes. Criminals can use the information to obtain prescription drugs, have costly medical procedures, or purchase expensive medical equipment. They can also use it to commit tax fraud or obtain Medicare and Medicaid. Complete medical “ID kits” can be sold for anywhere from $500 to as much as $1,200 on the Dark Web, depending on the market and how much information is included.

2. Medical identity fraud can be very difficult to detect; it can go undiscovered for months or even years. This enables criminals more time to use or sell the

Robert Lord (Robert@protenus.com) is Co-founder and CEO of Protenus in Baltimore, MD.
information before the breach is discovered and the information begins to lose its value.¹

Oftentimes, patients do not realize that their medical information has been stolen until they do a credit check when they turn 18 years old or apply for a credit card or student loan. Only then do they notice the suspicious debts and costly bills in their name from when criminals have used their information. Criminals know that parents are not routinely examining their children’s credit reports looking for abnormal activity; it is only upon the child’s coming-of-age that the destruction is uncovered.

Because this type of data breach is hard to detect, it makes their information much more valuable to cyber criminals. They can use this time to build a detailed, false identity on the “blank canvas”² provided by the child’s medical records. Criminals have continued to realize how valuable this information is, and the last few years have seen an increase in the theft and misuse of pediatric patient data. A study by Carnegie Mellon CyLab found that 10% of a 40,000-child sample had someone else using their Social Security number. “The primary drivers for such attacks are illegal immigration (e.g., to obtain false IDs for employment), organized crime (e.g., to engage in financial fraud), and friends and family (e.g., to circumvent bad credit ratings, etc.).”³ “Almost half (47%) of medical identity theft occurs when a family member takes a relative’s health insurance card or other ID—or when people knowingly share their health information or IDs with someone they know.”⁴

According to a 2011 study by the Ponemon Institute,⁵ children in the United States are 51 times more likely to have their identity stolen than adults, making pediatric patient data protection something our healthcare systems need to be paying extra attention to and taking measures to curb the threats to their young patients.

The potential fallout
Unfortunately, the potential effects of a data breach of pediatric patient data can be devastating. In a survey of medical identity theft victims, Ponemon Institute found that 65% had spent an average of $13,500 to resolve the identity theft.⁶ This number covers a range of potential costs, including paying healthcare bills made in their names, recovering their health insurance, and paying attorney fees. Money, however, is not the only concern; medical identity victims often spend months trying to put their lives back together. In the same survey, Ponemon also found that it took over three months and 200 hours to finish resolving the issue.

When a healthcare organization does not have the proper security measures in place, it is the patients who pay the heaviest price. Oftentimes, the number of affected records runs into the hundreds of thousands or even millions, but it is important to remember that each of those records belongs to a person, a person whose life has just been turned upside down by the theft of their personal and sensitive information. And the effects of a health data breach are magnified even further in pediatric patients, whose information—once stolen—can be abused on a consistent basis before the breach is discovered. Imagine how much more time and money these victims must spend putting their lives back together after their information has been sold and resold for 10 or even 15 years before it is detected, and all when the patients had little or no say in the decisions regarding the security of their private information.

Building a culture of trust and accountability
It is important for organizations to create clear lines of accountability for safeguarding patient
health data, a feat best accomplished through the collaboration and definition of roles for privacy and security teams. These teams must collectively decide on the technologies, procedures, and educational initiatives that will best protect pediatric data.

But it’s not all about those hard-working and often under-resourced privacy and security groups. Ultimately, a workforce-wide culture of trust, supported by technology that reinforces this culture and holds EHR users accountable, is a must when treating pediatric patients. Parents and healthcare organizations should be able to focus primarily on treating these delicate patients without also having to worry about whether their sensitive medical data is being compromised and maliciously used.

**Practical actions for privacy and compliance teams**

Armed with a deeper understanding of the topic, the following are some practical steps privacy and compliance teams can take to better protect pediatric patient health data:

- **Know who your pediatric patients are** through some form of systematic review of patient records. If possible, add extra scrutiny due to the elevated risk these patients face.

Step up manual audits of this pool of patients and, if possible, use the proactive monitoring programs available to help augment your team’s efforts.

- Understand pediatric clinical care and its unique nature. It will have different clinical workflows and people involved in care, scheduling, billing, etc. Ask a volunteer from the compliance team, who is passionate about pediatric patients, to become the team expert on these differences.

- Educate the workforce on the sensitivity of these records through a dedicated campaign to remind people of risks to vulnerable populations.

---