

PRIMARY CARE CODING & REIMBURSEMENT

KEEP UP TO DATE ON
PRIMARY CARE CODING & REIMBURSEMENT

We help office managers, coders and providers
improve coding skills, boost reimbursement
and avoid denials.



HOSPITAL MANAGEMENT		FINANCE	HEALTHCARE IT	EHR
HEALTHCARE REFORM	REGULATORY	RESOURCE LIBRARY		EVENTS

HOME : [ELECTRONIC HEALTH RECORDS](#) | [EHR](#)

ELECTRONIC HEALTH RECORDS | EHR

5 steps for preventing the insider threat

by [Guest Author](#) [January 3, 2017](#) [0 Comments](#)



Digital communications and information technologies are reshaping modern healthcare. They're also opening



hospitals up to new security threats. In this guest post, Kon Leong, president, CEO and co-founder of a specialized provider of electronic content archiving software, offers five ways data protection and fraud prevention stakeholders can protect their facilities from the threat from within.

SUBSCRIBE TODAY

Get the latest and greatest healthcare news and insights delivered to your inbox.

CONNECT WITH US

PRIMARY CARE CODING & REIMBURSEMENT

**KEEP UP TO DATE ON
PRIMARY CARE
CODING & REIMBURSEMENT**

We help office managers, coders and providers
improve coding skills, boost reimbursement
and avoid denials.

SEE HOW

OUR CONTRIBUTORS

Electronic health records (EHR) have improved transferability and accessibility of patient information, allowing for better diagnostic accuracy and more efficient coordination of treatments and services. Smart monitoring devices give healthcare professionals real-time updates on patients, and various forms of digital communication, such as video chat, healthcare consultation apps and email, enable doctors to provide care for patients regardless of their location.

Ensuring security

But with all these new types of sensitive healthcare data being created, who's ensuring it's secured?

Healthcare data security initiatives are often determined by compliance regulations, which unfortunately have trouble keeping pace with [technology](#). More data and greater accessibility means greater opportunity for exploitation and, over the years, stolen healthcare records have become extremely valuable, with healthcare fraud causing financial losses in the [tens of billions](#) every year.

We know about the threat presented by the likes of anonymous hackers, activists and state-sponsored entities. But disturbingly, an inordinate portion of healthcare fraud is committed by bad or negligent employees within the healthcare system.

They come in many forms:

- A [low-level administrator](#) with high-level access, selling EHRs to a private practice or marketer
- A doctor intentionally overcharging or receiving kickbacks for performing an expensive procedure, and
- An ex-employee submitting false claims under a patient's identity.

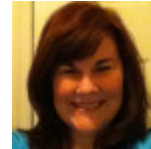
Data protection, fraud prevention

With that in mind, here's how data protection and fraud prevention stakeholders can rethink their defense strategies



JESS WHITE

Jess has written for several different print and online publications throughout her... [MORE](#)



RENEE COCCHI

Editor of Healthcare Business Tech, Renee has been writing for the medical... [MORE](#)

Keep up to date on

PRIMARY CARE
CODING & REIMBURSEMENT

**KEEP UP TO DATE ON
PRIMARY CARE
CODING & REIMBURSEMENT**

**WE HELP OFFICE MANAGERS,
CODERS AND PROVIDERS
IMPROVE CODING SKILLS,
BOOST REIMBURSEMENT
AND AVOID DENIALS.**

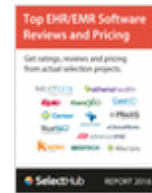
SEE HOW

Top Trending Resources

[Top Electronic Medical](#)

and account for the real threat to the healthcare system – the threat from within.

- 1. Training employees:** In order to implement a successful data protection strategy, employees have to be trained on best practices for use of EHR systems and handling of patient information, as well as recognizing and addressing inappropriate behavior. In certain cases, security risks arise from a negligent employee being influenced by a third party or another employee to release confidential information. Social engineering – the manipulation of others to obtain confidential information or to influence their behavior – is often a fundamental component of modern healthcare fraud, and inadequately-trained faculty only perpetuate its effectiveness.
- 2. Access controls:** Those who visit the doctor and notice an assistant entering their information into a computer or iPad might wonder who else has access to their information. This is a legitimate concern, and access controls are an essential component in data protection initiatives. According to [the Department of Health and Human Services](#), access controls are an effective method of preventing inappropriate access to EHRs, fraud schemes and false claims. Admin should only have access to files fundamental to their position, and access privileges should be regularly reassessed and updated to reflect management changes, such as reassigned employees.
- 3. EHR review and audit:** A simple step that every facility can take to reduce fraud is to assign specific employees to regularly review a sample of claims and EHRs for any suspicious activity. Organizations should also perform regular log audits of EHR systems, which is essential to mitigating the risks of employee misconduct. [According to the Centers for Medicare & Medicaid Services](#), during review, special attention should be paid to particular actions such as copy-pasting, and delayed alterations to records, which can be indicative of fraudulent behavior. Additionally, analytics technologies can identify when employees consistently view a particular type of record for



Records
(EMR)
Software
Reviews and
Pricing 2016--
Free Analyst

Report:

Interactive analyst report gives you comparison ratings... [Download Now >>](#)



Find the Best
2017 Practice
Management
Software -
Get FREE
Custom Price

Quotes:

Simplify your practice management software evaluation process in one... [Download Now >>](#)



Empowering
Healthcare
Companies
to Reach
Beyond the
Limitations

of QuickBooks:

Download this white paper to learn how NetSuite can help your Healthcare... [Download Now >>](#)

[Find the Best 2017 Electronic Medical Records \(EMR\) Software - Get FREE Custom Price](#)

longer than reasonably necessary or access an excessive number of files, behavior that may correlate with fraudulent activity.

- 4. Locking down all systems:** Important data can also be created outside of EHR systems, so these systems should be protected and monitored as well. For instance, file shares containing sensitive information present a security risk if left unmanaged, and thus file analysis should be performed to identify and remediate sensitive files. Remediation might include applying limited access privileges, retention policies or even deletion, and these actions should comply with ongoing data management policies so file analysis doesn't need to be performed repeatedly.
- 5. Email analytics:** Select communication patterns in emails can be indicative of misconduct. For instance, emails with particular words and word combinations, or correspondence patterns between particular members of the healthcare community that aren't necessary to one's job description, may suggest unlawful activity. Used in combination with additional behavioral metrics, unstructured analytics – the analysis of human-made data can be effective for detecting behavior that correlates with fraud. This requires information technology capable of accommodating and standardizing both structured and unstructured data.

Too many hospitals and providers haven't adjusted to the new breed of predator, or the modern security concerns that accompany the virtualization of healthcare records. For data protection stakeholders seeking to navigate the new landscape of healthcare data security, it will prove wise to have versatile data initiatives in place that can process and protect the entire spectrum of data sources.

Kon Leong is president, CEO and co-founder of [ZL Technologies](#), a specialized provider of electronic content archiving software for large enterprise environments. He's responsible for managing all aspects of the business, including strategy, finance, sales and marketing.



Quotes:

Simplify your electronic medical records software...

[Download Now >>](#)

[Get More Professional Resources: View All](#)

Categories: [Electronic Health](#)

[Records](#) | [EHR, Healthcare IT,](#)



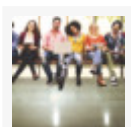
[Special Report](#)

Tags: [Access controls, data](#)

[prevention, EHR audit, employees,](#)

[fraud detection, internal threat](#)

Related Posts



How Millennials will change healthcare IT



Endpoint Rx: Healthcare delivery requires secure mobile technology



Hacking health care: Inside scoop to the most vulnerable vertical



Recovering from ransomware: Healthcare companies can still retrieve their data

Comments Community

 Login ▾

 Recommend  Share

Sort by Best ▾

Start the discussion...

Be the first to comment.

ALSO ON HEALTHCARE BUSINESS & TECHNOLOGY

Understanding the HIPAA conduit exception rule

1 comment • a year ago •

Mike — So is a BA responsible (non-complaint with HIPAA) if a

Prepare for another cybersecurity threat

1 comment • 2 years ago •

O11v3r — Further information for safeguarding against new

New facility takes No. 1 spot on U.S. News' Best

1 comment • 2 years ago •

Rajat Dhameja — Not surprising Mayo Clinic is at top spot in 2014. They

Avoid readmissions for homeless patients

1 comment • a year ago •

Shereese Maynard — I believe more support needs to be given to

 **Subscribe**

SUBSCRIBE TODAY

Get the latest and greatest healthcare news and insights delivered to your inbox.

Email Address

SUBMIT

ABOUT HEALTHCARE BUSINESS & TECHNOLOGY

Healthcare Business & Technology, part of the Catalyst Media Network, is a healthcare information brand focusing on trends and issues facing executives working in the healthcare industry. With nearly half a million reach and 92,000 newsletter subscribers holding a variety of positions in healthcare management, administration and IT we're focused on bringing the most relevant and up-to-date information surrounding the healthcare industry right to those directly involved in the field so they can perform at the top of their game and help provide better patient care.

COPYRIGHT © 2016 HEALTHCAREBUSINESSTECH.COM

[BACK TO THE TOP](#)