The Future of Your Legacy System Data – Why Plan?

Donna M. Carter, PMP
Healthcare IT Consultant and CEO

Carter Consulting, LLC.

HIMSS CENTRAL & SOUTHERN OHIO Chapter

Why Decommission?

- Reduce organization costs
- Obsolete application
- Reduce system hardware or multiple systems
- Mergers resulting in moving data
- Legacy data scattered across multiple systems
- Need for standardized data analytics
- REPUTATION
- Compliance

DEFINITION

electronic protected health information (ePHI)

Electronic protected health information (ePHI) refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

There are 18 specific types of electronic protected health information, including patient names, addresses, Social Security numbers, email addresses, fingerprints or photographic images, among others. In addition, any past medical records or payment information is subject to the same degree of privacy protection.

Regardless of the type of electronic device -- PC, tablet PC or smartphone -- used to access electronic protected health information, users must abide by HIPAA Security Rule guidelines when handling both information at rest and that which is being transferred electronically, via email or file transfer.

Reputation:

THE WALL STREET JOURNAL. ≡ BUSINESS

DIGITAL + PRINT

TOP STORIES IN BUSINESS

1 of 12

Apple Woos App Developers

2 of 12

Next UAW Chief to Confront Wage Split

3 of 1

Ticketmaster Agrees to Tentative Settle...

BUSINESS

Target Now Says 70 Million People Hit in Data Breach

Neiman Marcus Also Says Its Customer Data Was Hacked

By PAUL ZIOBRO And DANNY YADRON CONNECT

Updated Jan. 10, 2014 8:36 p.m. ET

Target Corp.'s holiday data breach was bigger than the company had previously said, penetrating more systems and compromising a new set of personal information affecting up to 70 million people.

THE MUS TRA

PHIprivacy.net

Mar 24 2012

CVS Caremark mailing error exposes prescription information

Breaches, Pharmacy Records, U.S. breaches

Robert Weisman reports in *The Boston Globe*:

> CVS Caremark Corp. said Friday that it mistakenly sent letters to about 3,500 Tufts Health Plan members, giving them personal information about the medical conditions and medications of other members enrolled in a supplemental Medicare plan managed by Tufts.
>
> The mistake was due to an unspecified "programming error," CVS Caremark, pharmacy benefits manager for the Tufts Medicare Preferred Plan, said in a statement.
>
> [...]
>
> The "medication information" letters went out to the wrong addresses in late January and early February, mostly to members in Massachusetts. Each letter included another member's name, the name of a drug prescribed, and the general types of conditions that treatment is used for, according to CVS Caremark, based in Woonsocket, R.I.

CVS agrees to $250K data privacy resolution with Maryland AG

Author Name **Patrick Ouellette** | Date **August 30, 2013** | Tagged Administrative Safeguards, Health Data Breach, Health Data Encryption, Health Data Security, HIPAA, Patient Privacy, Pharmacy Data Breach, PHI, Physical Safeguards, State Patient Privacy Laws, Technical Safeguards

CVS Pharmacy, Inc. and Maryland CVS Pharmacy, LLC reached a $250,000 agreement this week with Attorney General Douglas F. Gansler's Consumer Protection Division because it didn't do enough protect patient data in the eyes of the AG.

This settlement also resolved allegations that CVS sold and offered for sale products after their expiration dates had passed, but it's noteworthy that it's taken five years since the original accusations that dated back to 2008 to resolve the issue. CVS has since said in a statement that it agreed to the settlement to avoid the time and expense of further legal proceedings.

Obamacare Website Targeted About 16 Times by Cyber Attacks

Nov. 13, 2013

By ALYSSA NEWCOMB and MATTHEW LAROTONDA via **WORLD NEWS**

The healthcare.gov website is shown, Nov. 13, 2013.

Healthcare.gov/ABC News

The troubled Affordable Care Act website has been subject to "a handful" of hacking attempts, including at least one intended to bring the site down, a Department of Homeland Security official told lawmakers today.

But considering that some federal websites get hundreds of cyber-assaults each day, the approximately 16 reported attacks on healthcare.gov is a surprisingly small number, experts said.

Cyber Attacks And Security Breaches In Healthcare

Do You Have The Right Security Program In Place?

April 24, 2013

Like it? Share it!

By barb white

Barb White
Director of Healthcare Solutions, AT&T
Find me on:

I read almost daily in the news about cyber attacks on U.S. banks, infrastructure, government agencies, and businesses. In fact, government agencies saw a more than 650% increase in cyber security incidents from 2006 to 2010, according to the **Government Accountability Office (GAO).** The GAO reports that a main reason for the increase is the failure of agencies to fully implement their IT security programs.

To me, this means that many of the incidents could be preventable.

Although healthcare organizations are not often a primary target of hackers, electronic data in the healthcare sector is among the most vulnerable according to multiple reports, including **a year-long investigation by *The Washington Post***. In fact, of all data breaches in the United States, healthcare entities accounted for **the highest percentage of incidents**, more than one-third of all data breaches in the country. One study reports that an astounding **94% of healthcare entities** have experienced security or privacy breaches with their data.

And we're not even talking about sophisticated cyber attacks over the Internet, but compromised data due to human error. A majority of healthcare security breaches have resulted from stolen and lost devices, such as laptops, desktops and smartphones — which often are not encrypted or even password-protected.

Despite frequent warnings from the Department of Health and Human Services and the U.S. Department of Homeland Security, the healthcare industry lags behind other sectors in implementing some of the basic security precautions when it comes to protecting patient data.

Of healthcare organizations surveyed in a **2012 study on cyber crime**, fewer than half performed an annual security risk assessment — the most effective way to detect a security breach. In fact, 52% of the organizations that conduct one of these audits discover a security breach as a result.

Healthcare IT News

Published in partnership with HIMSS

Erin McCann, Associate Editor

Erin McCann is Associate Editor at *Healthcare IT News*. She covers healthcare privacy and security, meaningful use, ambulatory care and healthcare policy. Follow Erin on Twitter @EMcCannHITN and Google+

Homeland Security has tip for healthcare

'Risk management never ends.'

November 15, 2013

Data breaches and cybersecurity threats in healthcare are going to happen. It's virtually unavoidable. What can be avoidable, however, are the messy consequences of substandard risk assessment strategies and inadequate threat response.

Department of Homeland Security's Jason Gates, an analyst in the industry, engagement and resilience branch within the Office of Cybersecurity and Communications, spoke at a virtual event Thursday about how healthcare organizations can work to mitigate the effects of a cybersecurity attack and lessen the risk of actually having one.

Healthcare IT News

Published in partnership with HIMSS

News Blog White Papers Webinars Jobs More

EHRs Meaningful Use Privacy & Security HIE ICD-10 Interoperability Mobile CPOE Policy & L

Erin McCann, Associate Editor

Erin McCann is Associate Editor at *Healthcare IT News*. She covers healthcare privacy and security, meaningful use, ambulatory care and healthcare policy. Follow Erin on Twitter @EMcCannHITN and Google+

Data attacks on healthcare flying high

March 12, 2014

In the realm of privacy and security, heeding snooping employees and encrypting portable devices isn't enough in healthcare these days. Criminal attacks on hospitals are on a huge upward trend, with a whopping 100 percent reported increase just from four years ago. That's according to a new Ponemon Institute study released today.

This year, 40 percent of healthcare organizations have reported a criminal data attack. And, business associates who are not yet compliant with HIPAA in addition to those employees given the green light to use their unsecured devices certainly are not helping these numbers, say Ponemon officials.

Healthcare IT News

Published in partnership with HIMSS

Erin McCann, Associate Editor

Erin McCann is Associate Editor at *Healthcare IT News*. She covers healthcare privacy and security, meaningful use, ambulatory care and healthcare policy. Follow Erin on Twitter @EMcCannHITN and Google+

HIPAA data breaches climb 138 percent

February 6, 2014

When talking HIPAA privacy and security, the numbers do most of the talking.

Take 29.3 million, for instance, the number of patient health records compromised in a HIPAA data breach since 2009, or 138 percent, the percent jump in the number of health records breached just from 2012.

At $1.2M photocopy breach proves costly

HITECH notification rule leads to settlement after CBS News story

November 10, 2013

From the December 2013 *print issue*

The U.S. Department of Health and Human Services has settled with Affinity Health Plan, a New York-based managed care plan, for HIPAA violations to the tune of $1,215,780 after a photocopier containing patient information was compromised.

Affinity filed a breach report with the HHS Office for Civil Rights on April 15, 2010, as required by the Health Information Technology for Economic and Clinical Health Act, say HHS officials. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

CBS Evening News informed Affinity officials that, as part of an investigatory report, the television network had purchased a photocopier – previously leased by Affinity – that contained confidential medical information on its hard drive. Affinity estimated that up to 344,579 individuals might have been affected by this breach.

Healthcare IT News

Published in partnership with HIMSS

News Blog White Papers Webinars Jobs More

EHRs Meaningful Use Privacy & Security HIE ICD-10 Interoperability Mobile CPOE Policy &

Erin McCann, Associate Editor

Erin McCann is Associate Editor at *Healthcare IT News*. She covers healthcare privacy and security, meaningful use, ambulatory care and healthcare policy. Follow Erin on Twitter @EMcCannHITN and Google+

Kaiser Permanente sends out breach letters after email gaffe

'We offer our sincerest apology that this unfortunate incident occurred.'

OAKLAND, CA | September 13, 2013

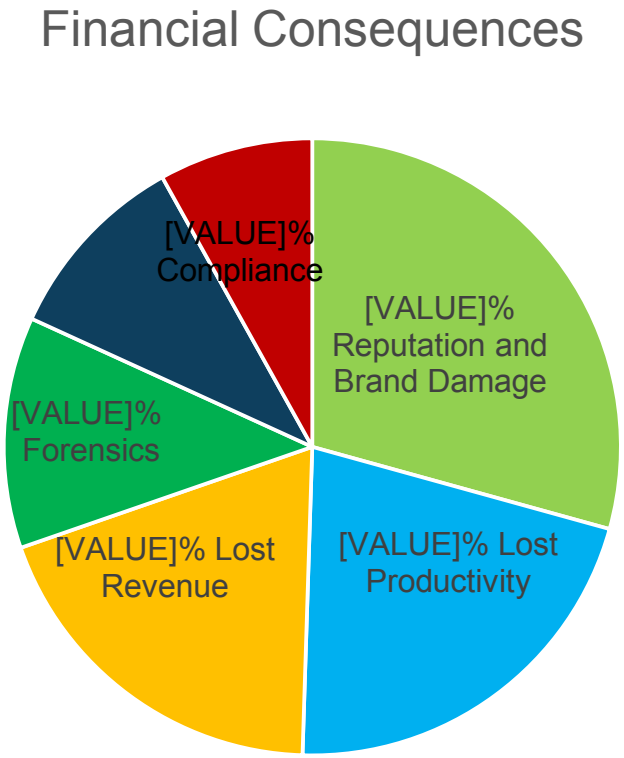
Health giant Kaiser Permanente is notifying 670 patients of a HIPAA privacy breach after an emailed attachment containing the protected health information of patients was sent to a recipient outside the Kaiser network.

The attachment was accidentally emailed by a Kaiser employee to a member of a pilot wellness screening competition back in May. "While the recipient was intended and authorized to receive the summary competition information, some of your personal information related to the competition was accidentally included in another location within the same file," a Sept.10 letter to affected patients read.

Data Breaches According to IBM

Data breaches are among the most common and costly security failures in organizations of any size.

In fact, studies show that companies are attacked an average of 16,856 times a year, and that many of those attacks result in a quantifiable data breach.



Legacy System Definition

- Legacy System: is an old method, technology, computer system or application program that may or may not being used in the organization and has an historical role.
- Run on obsolete hardware, difficult and costly to maintain, improve or expand.
- Vulnerabilities exist due to older operating systems and lace of security patches being available or applied. Backwards compatibility concerns.

Historical Data

- Historical Data usually resides on legacy systems inside legacy software
- Data may contain financial, clinical, and analytical content
- Due to compliance, legal and retention requiring periodic access and usability

Your Responsibility

- Protect it – HIPAA ePHI privacy compliance
- Retrieve it – business intelligence, analytics, legal or patient request
- Encrypt it – security – malicious attracts
- Store it – house or host the data content
- Secure it – HIPAA security compliance

Compliance

- HIPAA
- SOX
- CMS
- CLIA
- JCAHO
- IRS Audits
- Retention Policies
- FBI
- Department of Homeland Security – Cybersecurity

Cost to Consider

- Regulatory compliance audits
- System maintenance fees
- Application support fees
- Network costs
- Storage location
- Nontangible costs – credibility, trust due to a breach, reputation

Developing a Business Strategy

- Identify the business need
- Develop a cost benefit analysis
  - Tangible and non tangible cost
- Outline a solution – customized to your organization

Best Practice For a Data and System Migration Solution

- Plan
- Analysis
- Design
- Validation/Test
- Implement Strategy
- Optimize
- Decommission

However beautiful the strategy, you should occasionally look at the result ~

WINSTON CHURCHILL

Quality Assurance

- Enterprise Integration
- Application Testing
- Data Conversion
- Data Validation

Enterprise Integration

- Specification Requirements Meetings
- Specification Technical Documentation
- HL7 Standards and Segment Validation
- Content Validation based on data requirements
- Interface Engines
- Centralized and Decentralized Engines – the quantity impacts scope

Data Validation

- Testing Methodology
- Various phases/cycles of testing
- Automated vs. Manual Testing Products
- Compliance Consideration - ePHI

Trust and Credibility

- Cyber crime has increased 100% in four years
- Data breaches are becoming more public knowledge and increasing daily
- Data security is essential to credibility in healthcare and instrumental in keeping patients engaged
- Cyber crime has tangible and intangible cost which organizations need to consider

How Can We Help?

- Issue identification
- Solution recommendation
- Current state analysis
- Cost analysis and ROI review
- Project planning
- Technical expertise
- Future state projections
- Interoperability validation
- Implementation guidance
- Compliance oversight
- Verification of actual decommissioned product