Compliance is supply chain's business too: Building a more secure supply chain

Received (in revised form): 18th March, 2016

Jackie McGuinn

has nearly a decade of experience in the healthcare industry with expertise in marketing, operations and clinical care. She currently serves as Strategic Marketing Senior Manager at Global Healthcare Exchange (GHX), where she is responsible for identifying and understanding important challenges faced by healthcare providers and suppliers to aid innovation efforts. Some essential areas in which she has conducted market research include business intelligence, Health Insurance Portability and Accountability Act (HIPAA) compliance, vendor management, credentialing and supply chain automation. Prior to joining GHX, she served as sales effectiveness director for Vendormate and product marketing director for Greenway Health, gaining both clinical and operational experience in healthcare. Her earlier positions outside of healthcare focused on engineering optimisation of manufacturing processes, facilities layout and other operational improvements. She has presented on healthcare supply chain and compliance topics at the Association for Healthcare Resource & Materials Management (AHRMM) Annual Conference, Integrated Delivery Network (IDN) Summit and other industry leading events. She earned a Bachelor's degree in Industrial Engineering from the Georgia Institute of Technology.

Strategic Marketing, GHX, 3445 Peachtree Road NE, Suite 300, Atlanta, GA 30326, USA
Tel: +1 404-949-1344
Email: jmcguinn@ghx.com

Abstract Healthcare organisations rely on medical suppliers to deliver products that are critical to safe and effective patient care. But while suppliers are instrumental to care delivery, they can also be a source of risk. This paper examines ways in which supplier relationships can threaten patient privacy and safety, as well as impact a provider's accreditation status and revenues. We also present statistics showing how these threats are growing as healthcare becomes more digital. From there, we describe how healthcare organisations can protect themselves, their staff and their patients by building compliance into their supply chain processes. Readers will gain knowledge about:

- Industry regulations that require healthcare organisations to manage their supplier relationships, and the penalties for non-compliance;
- how patient data has become more vulnerable to attacks as a growing number of healthcare organisations transition to interoperable electronic health records (EHRs), including recent statistics on healthcare industry data breaches;
- the significant risk that business associates can present to patient privacy and the responsibility of healthcare organisations to mitigate this risk; and
- seven steps that healthcare organisations can take to integrate compliance into their supply chain processes to protect patient privacy, accreditation status and revenues

KEYWORDS: healthcare data breaches, electronic protected health information (ePHI), vendor credentialing, healthcare supply chain, business associates, HIPAA

INTRODUCTION: A NETWORK WITH INHERENT RISKS

On any given day—weekend or weekday, holiday or non-holiday—U.S. hospitals are open to serve those in need of healthcare. A network of clinicians and support staff works harmoniously to deliver the patient experience, helping many with recovery and saving lives. Behind the scenes are numerous moving parts and pieces operated by supply chains to help create this seamless experience. Need a bandage? Got it. Need gloves? No problem. Supply chain professionals strive to keep the flow of care uninterrupted by having the right supplies at the right time and at the right cost.

An extension to this network are the many suppliers that work with supply chain teams to provide the needed products and services from medical equipment to pharmaceuticals, to food services and so much more. These suppliers are invaluable to patient care delivery, but a wrong player added to this mix could wreak havoc and cause significant disruptions to the flow. New meaning is given to the idea that 'an ounce of prevention is worth a pound of cure'.

Suppliers can present varying levels of risk to the healthcare providers and the patients they serve—from supplier representatives that come into face-to-face contact with patients in a facility, to business associate organisations that can inadvertently leak patients' protected health information (PHI) through data breaches.

This paper examines the risks to patient privacy and safety inherent to healthcare provider–supplier relationships, including the growing threats that come with a more digital healthcare environment. It will make the case for why a healthcare organisation's supply chain team is in an ideal position to collaboratively manage supplier compliance, and offer best practices for mitigating risk and improving patient safety.

'Supply chains cannot tolerate even 24 hours of disruption. So if you lose your place in the supply chain because of wild behavior you could lose a lot. It would be like pouring cement down one of your oil wells.' — Thomas Friedman, *New York Times* columnist and Pulitzer Prize winning author

WHAT YOU DO NOT KNOW CAN HURT YOU

Healthcare firms and employees interact with thousands of suppliers on a daily basis through both face-to-face interactions on-site at their facilities, and remotely via telephone, email, fax, text and other electronic means of communication. Not knowing the personnel with whom staff is interacting and who is coming in contact with patients, or patient information, presents significant risks—to accreditation status, patient and staff safety and revenues.

Threats to Accreditation Status

The Joint Commission and other accreditation agencies require that healthcare organisations have in place policies and procedures to track suppliers that enter their facilities and know where they are at all times. In its guidelines issued in April 2012, and updated in July 2012, the Joint Commission outlined its 'expectations regarding anyone entering a health care organization,' stating[1]:

- *In order to maintain patient safety, accredited health care organizations need to be aware of who is entering the organization and their purpose at the organization (EC.02.01.01, EP 7).*
- *Accredited health care organization leaders need to also make sure they oversee operations and that responsibilities are assigned for administrative and clinical direction of programs, services, sites, and departments (LD.04.01.05, EPs 1 and 3); this includes processes for knowing who is entering the organization and their purpose.*

The Joint Commission has additional expectations for non-licensed,

non-employees who have a direct impact on patient care. These include healthcare industry representatives (HCIRs) in procedure rooms/operating rooms providing guidance to the surgeon, HCIRs providing training to staff on equipment use and surgical assistants brought in by surgeons. Additional requirements related to these individuals include[1]:

- *Taking steps to ensure that patient rights are respected, including communication, dignity, personal privacy (RI.01.01.01, EPs 4, 5, and 7), and privacy of health information (IM.02.01.01, EPs 1 and 2)*
- *Obtaining informed consent in accordance with organization policy (RI.01.03.01, EPs 1, 2, and 13)*
- *Implementation of infection control precautions (IC.01.01.01, EP 1)*
- *Implementation of the patient safety program (LD.04.04.05, EP 1)*

If a healthcare organisation is audited, it must have a way to show that an acceptable percentage of its suppliers are in compliance with its policies. Furthermore, the auditing agency may require that it demonstrate how it is managing suppliers. If the organisation cannot comply, its accreditation status could be hampered.

Threats to Patient and Staff Safety

Supplier representatives can pose risks to healthcare organisations in terms of patient and staff safety. Those with the most access to patient care areas, such as HCIRs, present the greatest risk because they come in close proximately with patients and their caregivers. A supplier representative who has not been immunised has the potential to unintentionally expose patients and staff to infectious diseases. A representative who fails to wear proper attire or follow procedures prior to entering the operating room (OR) or other patient care areas can present health and safety risks as well.

Threats to Revenues

Lack of visibility into the supplier population also presents risks to the financial health of healthcare organisations. For example, if a provider transacts business with a supplier who has been subject to a government sanction, such as those resulting from monthly Office of Inspector General (OIG) checks, and applies for government reimbursement for that supplier's products, it will be denied payment. The provider is also at risk for being fined up to US$10,000 for each service rendered by a federally excluded party.[2]

Another issue is Medicare fraud. An estimated 10 per cent of U.S. healthcare dollars are fraudulent, stemming from false medical claims, fake suppliers and other illegal business practices.[3] Other risks facing providers are supplier representative conflicts of interest, violation of the Centers for Medicare and Medicaid (CMS) Stark Law, and non-compliance with gift laws.

A WORLD GONE DIGITAL

Enacted in 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act has been a major catalyst in driving the transition from paper to digital medical records. With the promise of incentives from the CMS, a growing number of healthcare organisations are taking steps to achieve meaningful use of interoperable electronic health records (EHRs).

The switch from paper to EHRs has the potential to improve both patient care and healthcare business operations:

- *Improve quality, safety, efficiency and reduce health disparities*
- *Engage patients and family*
- *Improve care coordination, and population and public health*
- *Maintain privacy and security of patient health information*

The ultimate goal of meaningful use is to achieve:

- *Better clinical outcomes*
- *Improved population health outcomes*
- *Increased transparency and efficiency*
- *Empowered individuals*
- *More robust research data on health systems*[4]

Along with these advancements comes a new set of challenges which could be disastrous for the supply chain if left ignored. Data gone digital requires a new level of safeguards to protect patient information and keep it out of the hands of those who should not have access to it. Although theft of patient information occurs with paper records, the breaches are typically smaller in scope. With digital health information, thousands or even millions of patient records can be stolen in one attempt.

In its 2015 Data Breach Industry Forecast, Experian states that it expects 'healthcare breaches will increase—both due to potential economic gain and digitization of records.' The company recommends that healthcare organisations 'step up their security posture and data breach preparedness or face the potential for scrutiny from federal regulators.'[5]

Consider these statistics:

- More than 40 million Americans suffered a breach of their PHI from 2009 through the end of 2014. In 2014 alone, 164 PHI breaches were reported to the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR), impacting nearly 9 million patient records, a 25 per cent increase over 2013.[6]
- Research from the Ponemon Institute shows that the cost of data breaches has risen 23 per cent since 2013, and the average cost of a data breach weighs in at US$3.8m.[7] Covered entities and business associates could also be infamously listed on the U.S. Department of Health and Human Services Office for Civil Rights 'Wall of Shame'.[8]
- Medical files and billing and insurance records contain the most valuable patient data and are most often successfully targeted.[9]

Although hackers are commonly associated with data breaches, they are not the only culprits. Business associates have also grown as a significant security threat. The OCR defines a business associate as 'a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity'. Some business associates hold millions of patient records. If a business associate does not have the necessary safeguards in place to protect that data, both itself and healthcare providers for which it provides services, are at considerable risk—not to mention the patients themselves.

Business Associate–Related Data Breaches

- Eighty-seven per cent of business associates report that their organisations experienced electronic information–based security incidents over the past two years.[9]
- Of those surveyed, 95 per cent business associates say they had a security incident involving lost or stolen devices.[9]
- With regard to PHI breaches, 39 per cent of business associates surveyed said a criminal attacker caused the breach and 10 per cent say it was due to a malicious insider.[9]
- Only 41 per cent of business associates feel they have sufficient resources to prevent or quickly detect a data breach.[9]
- When asked what type of security incident concerns them most, more than half of business associates surveyed (51 per cent) said it is the negligent or careless employee. This was followed by use of cloud services (48 per cent) and mobile device insecurity (40 per cent).[9]

- Forty per cent of healthcare professionals surveyed are 'not confident' and 33 per cent are only 'somewhat confident' in their business partners' capacity to manage patients' sensitive data.[10]
- In 2015, a business associate exposed 3.9 million records.[11]

The total cost of managing a data breach can be very significant—including potentially large fines, class-action lawsuits, wasted staff and executive time, as well as long-term damage to the hospital's reputation with patients, bondholders, self-insured companies and the general public. It is the hospital that suffers the damage to its reputation, even if a business associate or one of the business associate's subcontractors was entirely responsible for the data breach.

Further compounding the problem, hospitals and business associates are increasingly targets of criminal cyber attacks because of the high-value information that health records contain, which can include everything from Social Security numbers and birthdates to personal payment information to health insurance identification numbers.

It is hard to pick up a newspaper or read online articles and not come across news on data breaches. The headlines are full of them. Data breaches are on the upward swing worldwide. *Healthcare IT News* reported the top seven data breaches of 2015, three of which were in the healthcare industry[12]:

1. **Excellus BlueCross BlueShield**: The third-largest healthcare breach of 2015, which impacted 10 million of the company's members.
2. **Premera Blue Cross**: Impacted more than 11 million members, including employees of Microsoft, Starbucks and Amazon.
3. **Anthem**: The 'largest healthcare breach ever recorded'—exposing 78.8 million 'highly-sensitive' patient records, and between 8.8 and 18.8 million non-patient records.

The FBI Cyber Division reports, 'Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to EHR, lax cybersecurity standards, and a higher financial payout for medical records in the black market.'[13]

Regulations Aimed at Protecting Electronic Protected Health Information (ePHI)

Business associates, under the HITECH Act, must implement administrative, physical and technical safeguards to protect the patient healthcare data of their customers. In 2013, the Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Rule expanded the definition and security responsibility for business associates so that more suppliers fall under this category.

Under the HIPAA rule, hospitals must identify which of their suppliers are classified as business associates, and have a signed and executed business associate agreement (BAA) for each of these suppliers. For those business associates that fail to sign BAAs, hospitals must have a way to prove that they have attempted to secure agreements.

The OCR has announced that it will audit U.S. healthcare organisations to ensure they are complying with the HIPAA rule, including its provisions around business associates. When conducting an audit of a healthcare organisation, the OCR will:

> "Inquire of management as to whether a process exists to ensure contracts or agreements include security requirements to address confidentiality, integrity, and availability of ePHI. Obtain and review the documentation of the process used to ensure contracts or arrangements include security requirements to address confidentiality, integrity, and availability of ePHI and evaluate the content in relation to the specified criteria. Determine if the

> contracts or arrangements are reviewed to ensure applicable requirements are addressed."[14]

The stakes are high for hospitals that are found in non-compliance with the rule. Each fine for willful neglect without correction costs US$50,000. The fines are limited by category to a maximum of US$1.5m, but a hospital with multiple violations in each of the four violation categories within a calendar year could face up to US$6m in fines.[15]

The Challenges of Compliance

One of the major challenges hospitals face is simply identifying which of their suppliers are business associates. Because the HIPAA Omnibus Rule greatly expands the definition of companies that qualify as business associates, it is easy for a medium-to-large-sized hospital to miss a large number of suppliers that should be classified as business associates and have the required BAAs in place. Advancements in product and service technology that change a supplier's electronic ePHI relationship can also cause a shift to business associate status, with hospitals overlooking suppliers that were not previously in the business associate category.

Another challenge is that many healthcare organisations lack a unified approach to business associate management. Supplier information is contained within spreadsheets or stored within separate unique files across the organisation. Because of this, they do not have an effective or efficient way to manage business associate requirements and demonstrate compliance with the HIPAA Omnibus Rule. In the event of an audit, a hospital taking a disjointed approach would find it a tremendous challenge to report on its business associates and the BAAs it has in place, not to mention proving that it has attempted to secure a BAA from a supplier that has failed to sign one.

Also commonly overlooked are physician practices and other providers owned by the hospital. They typically have a separate supplier list that must also be assessed for business associate risk. Without some automated way of identifying, querying and tracking a hospital's entire supplier list—and conducting automated follow up—a typical hospital system might overlook a percentage of suppliers that are actually business associates. The consequences of not identifying all business associates can be adverse for a hospital if one of those suppliers is ultimately found to be responsible for a HIPAA violation.

COMPLIANCE IS SUPPLY CHAIN'S BUSINESS

Because the task of onboarding, contracting, managing and paying suppliers most often falls to supply chain, the task of managing supplier compliance is a natural fit for this department. Forward-looking healthcare organisations have recognised that by closely linking supply chain and compliance functions, they can more efficiently and effectively comply with increasing regulatory demands, while enhancing patient safety, safeguarding patient privacy and protecting revenues.

How to Integrate Compliance into Supply Chain Processes

With a hospital's supply chain team working closely with its suppliers throughout the procure-to-pay cycle and beyond, there are various ways it can weave compliance activities into its processes. Below are compliance best practices supply chain teams can put into place to mitigate risk for their organisations. Leveraging technology to centralise supplier data for easy, comprehensive access is foundational to improving supplier management and compliance.

Centralise the Supplier Master and Gain Visibility

What supply chain leaders need is the ability to access in-depth and timely information on

suppliers and their individual representatives. A hospital should establish a common supplier master across all parts of the organisation, especially if the organisation recently acquired or merged with another entity. By centralising all supplier data in one place, an organisation can quickly and easily access the information it needs in the event of an audit, including the percentage of suppliers in compliance with its policies.

In most cases, providers have supplier data that is distributed in several different systems and even some data stored in manual spreadsheets. Without full visibility into the entire supplier population, compliance could be compromised and important tasks could be missed, including the protection of value analysis decisions.

Providers could potentially spend more than half of their supplier management time just tracking down information, such as contact details. Furthermore, this takes time away from value-added tasks that drive down supply chain costs, including contract negotiations. Burdened with a high volume of suppliers and their related data, providers need technology and automation to holistically and centrally manage the supplier population.

Case in Point: Mississippi hospital gets DNV audit ready with 100 per cent vendor oversight

Hospitals accredited by DNV Healthcare are required to conduct vendor scorecarding for patient safety and outcomes. A 512-bed hospital based in Mississippi was confronted with this task but without visibility into its entire vendor population, the materials management team found it challenging to identify which vendors needed to be scorecarded.[16] The team also spent significant time conducting various vendor management tasks to meet regulatory and other requirements.

The hospital implemented solutions from a third-party vendor credentialling provider that allowed materials management to effectively collect, centralise and monitor data for 100 per cent of its vendor population at the organisation level. By inventorying and managing their entire vendor population, it is simpler for the team to assure all vendors are compliant with policies and to conduct scorecarding. With quick and easy access to comprehensive vendor reports, the team can ensure the hospital's policies are acknowledged and vendor scorecarding is in effect so that it is better prepared for DNV audits.

Simplify and Capture Information Upfront

Simplifying and standardising the process for suppliers to submit required company data, documents and correct contacts by topic and responsibility expedites the process and improves supplier oversight and management. Establishing the supply chain team as the main point of contact for all supplier information and issues can help facilitate this.

The supplier onboarding process presents the perfect opportunity to capture compliance-critical information, including sign off on hospital policies, confirmation of immunisations, business associate designation and completed BAAs.

Know Who Is in Your Facilities and When

To comply with the Joint Commission accreditation requirements, a healthcare organisation must have in place a way to track which supplier representatives are in their facilities, where they are and when they arrive/depart. A comprehensive supplier credentialling programme with badging capabilities can help facilitate this requirement.

Have a Well-Defined Vetting Process

As part of the credentialling programme, implement a well-defined and thorough

process for vetting suppliers. Best practices in supplier management include having a system to register and authenticate suppliers for tax ID and OIG sanction checks. The OIG has a downloadable List of Excluded Individuals and Entities (LEIE) that can be accessed on its website.[17] This aspect of supplier management not only adds appropriate controls but also impacts many other activities downstream.

Although many hospitals work to credential supplier representatives who come on-site to their facilities, they often neglect to credential those representatives who remain off-site, but still have access to PHI. Hospitals must be sure to vet the entire supplier population—at the company level for both off- and on-site suppliers and additionally at the rep level for on-site representatives.

'If you are a Medicare or Medicaid provider, the first step you should take to protect yourself against these sanctions is to check *all* individuals and entities with which you do business to make sure they are not excluded,' state Ari J. Markenson, JD, MPH and Kelly Skeat, Esq. in a *Compliance Today* paper they authored on the topic.[18] 'This should be done at the time of hire for new employees and as part of the standard vendor enrollment process for all entities with which your organization does business.'

Special Considerations for Vetting Business Associates

On average, 30 to 40 per cent of a healthcare organisation's suppliers typically qualify as business associates. Business associate identification has been cited as a significant challenge for providers, and the larger the supplier master, the greater the challenge. For example, a hospital with 2,375 suppliers identified at least 730 as having business associate characteristics.[19] Identifying and managing hundreds of business associates is no simple task.

As part of the vetting process, all suppliers should be assessed for business associate qualification to make business associate identification more manageable. The new definition of business associate now includes more categories of suppliers. After determining which suppliers are business associates, hospitals should have a BAA in place with each business associate that clearly defines how the supplier will report and respond to a data breach, including data breaches caused by the business associate's subcontractors.

Case in Point: Indianapolis healthcare system reduces risk through better BA management

An Indianapolis-based healthcare system has always taken the privacy of its patients' PHI seriously with processes to safeguard it, but the organisation's method for managing BAAs was largely manual.[20]

'When the HIPAA rule was enacted, we scurried around to assess every vendor relationship for a BAA or the possibility that we needed one in place, checking all past, present and pending vendors,' said the healthcare system's privacy director. 'I was constantly juggling emails. Every once in a while I would go through my BAA database to see what I didn't have and try to reconnect with those vendors. It was a reactive situation because I had no way to actively look at our vendor population and say with certainty that we needed or had a BAA.'

Recognising the need for a more efficient way to manage, track and document BAAs, the organisation implemented an electronic, standardised and centralised platform for business associate management. Users can review their organisation's vendor population through the solution's dashboard, mark which vendors are business associates, and then manage and track BAAs, as well as other compliance documents. This solution also allows users to exchange documents with

their business associates and automatically generates a full audit trail of activities.

According to the healthcare system's privacy director, the greatest benefit she has derived from the solution is the ability to help safeguard patients' health data and prepare for an OCR audit.

'We have a much better handle on what's going on in our vendor world to protect our patients' confidentiality—that's the most important thing,' she said. 'We want to protect our patients and make sure we are doing everything we can to keep their information from being breached, whether there are regulations or not. But now that there are regulations, we're making every effort to comply with them.'

HIPAA Business Associate Compliance Requires Vigilance

Business associate management involves gaining 'satisfactory assurances' from business associates regarding oversight and compliance for themselves and their subcontractors. Business associates should be monitored on a regular basis to ensure they have safeguards in place to protect PHI. A healthcare organisation should perform a risk assessment of its business associates and if any gaps are found in a business associate's processes, it should present to the healthcare organisation a plan that details what it will do to close those gaps. The healthcare organisation should then follow up with the business associate to make sure those steps have been taken. Some hospitals send out surveys to suppliers to determine if they are implementing the safeguards outlined in their BAAs.

In the event of an OCR HIPAA business associate audit, a healthcare organisation typically has just weeks to respond. To be audit-ready, an organisation should have a mechanism in place to quickly and accurately generate reports of all identified business associates, updated contact information and status of the BAAs.

Providers could eliminate at least a quarter of their time 'chasing' business associates by electronically centralising BAAs and related compliance documents in one system tied with the supplier master so that business associate management is part of overall supplier management. This eases ongoing management of business associates to drive a stronger culture of privacy and compliance for providers, and extends that culture to supplier organisations.[19]

Engage in Data Sharing, Not Silos

Although the supply chain team is in an excellent position to drive supplier compliance, they cannot operate in a void. Many different departments and individuals interact with suppliers and their representatives; therefore, a healthcare organisation must have in place a system for making supplier information available to cross-functional staff for a holistic approach to supplier management.

CONCLUSION

Suppliers and their representatives play a critical role in healthcare, supplying products and services without which providers could not properly care for patients. But when healthcare organisations do not have in place policies and procedures to effectively manage their supplier relationships, they place patients, staff and operations at considerable risk.

Because supplier issues can significantly disrupt the delivery of products for patient care, compliance is supply chain's business, too. As a main point of contact for a healthcare organisation's suppliers, and a department directly involved with supplier interactions and transactions, supply chain is perfectly positioned to build supplier compliance into its processes. Effective supplier management significantly minimises risk, protecting healthcare organisations, their staff and their patients.

References

1. The Joint Commission, 'Standards FAQ', available at: Details, http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFAQId=621&StandardsFAQChapterId=66 (accessed 4th April, 2017)
2. Office of Inspector General (1999) 'The effect of exclusion from participation in federal health care programs', available at: https://oig.hhs.gov/exclusions/effects_of_exclusion.asp (accessed 4th April, 2017)
3. The Economist (2014) 'The $272 billion swindle', available at: http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle (accessed 4th April, 2017)
4. HealthIT.gov 'Meaningful use definition & objectives', available at: https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives (accessed 4th April, 2017)
5. Experian '2015 Data Breach Industry Forecast', available at: http://www.experian.com/data-breach/2015-data-breach-industry-forecast.html (accessed 4th April, 2017)
6. PRNewswire (2015) 'Redspin 2014 Breach Report: Protected Health Information (PHI)', available at: https://www.redspin.com/resources/download/breach-report-2014-protected-health-information-phi/ (accessed 4th April, 2017)
7. Wike, K. (2015) 'Breaches more costly than ever, health IT outcomes', available at: http://www.healthitoutcomes.com/doc/breaches-more-costly-than-ever-0001 (accessed 4th April, 2017)
8. U.S. Department of Health and Human Services Office for Civil Rights 'Breach portal: Notice to the secretary of HHS Breach of unsecured protected health information', available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed 4th April, 2017)
9. Ponemon Institute (2015) 'Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data', available at: https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data (accessed 4th April, 2017)
10. Ponemon Institute (2014) 'Fourth Annual Benchmark Study on Patient Privacy and Data Security', available at: http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security (accessed 4th April, 2017)
11. McGee, M. K. (2015) 'Business associate breaches: Key issues', *Data Breach Today*, available at: http://www.databreachtoday.com/business-associate-breaches-key-issues-a-8314; See also http://www.nbcnews.com/tech/security/medical-informatics-engineering-hack-exposed-data-3-9-million-people-n403351 (accessed 4th April, 2017)
12. Davis, J. (2015) '7 largest data breaches of 2015', *Healthcare IT News*, available at: http://www.healthcareitnews.com/news/7-largest-data-breaches-2015 (accessed 4th April, 2017)
13. FBI Cyber Division, Private Industry Notification (2014) 'Health care systems and medical devices at risk for increased cyber intrusions for financial gain', available at: http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf (accessed 4th April, 2017)
14. U.S. Department of Health & Human Services (2016) 'Audit protocol – Current', available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html (accessed 4th April, 2017)
15. U.S. Department of Health & Human Services 'HITECH Act Enforcement Interim Final Rule', available at: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf (accessed 4th April, 2017)
16. 'Forrest General utilized vendor manager to meet accreditation standards', available at: http://ghx.com/industry-resources/case-studies/forrest-general-credential-manager/ (accessed 4th April, 2017)
17. Office of Inspector General 'LEIE downloadable databases', available at: http://oig.hhs.gov/exclusions/exclusions_list.asp (accessed 4th April, 2017)
18. Markenson, A. J., and Skeat, K. (2013) 'Protecting your organization from exclusion sanctions', *Compliance Today*, available at: http://www.beneschlaw.com/Files/Publication/d2474c5d-8da4-473b-9309-7441092c97a3/Presentation/PublicationAttachment/776c802f-26ae-4a0b-ab81-84e779f280e4/Markenson_Skeat_article.pdf (accessed 4th April, 2017)
19. 'Torrance Memorial Medical Center grows procurement cycle solutions with vendor oversight and business associate management', available at: http://www.ghx.com/industry-resources/case-studies/torrance-memorial-medical-center/(accessed 4th April, 2017)
20. GHX 'Eskenazi health improves HIPAA business associate management and HIPAA compliance with GHX compliance document manager solution.'