HIPPA compliance for vendors and suppliers

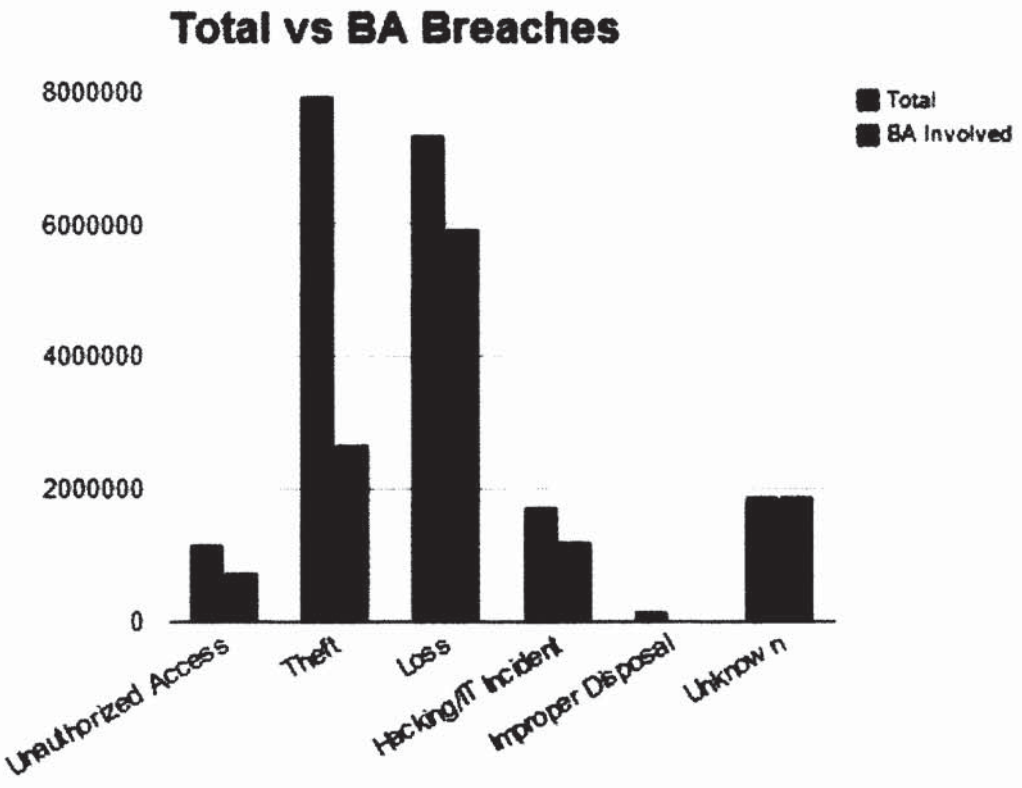
John M. White, CHPA, CPP

Between 30 to 45% of breaches in Protected Health Information (PHI) involve vendors, yet in most cases it is the hospital that is held liable for the breach. In this article, the author explores the practice of relying on vendors to conduct their own background checks of employees they assign to hospitals. He provides guidance on how hospitals can insure that such checks are up to the standards of the hospital's own background procedures without taking over that responsibility from vendors.

(John M. White, CHPA, CPP, is the President/CEO of Protection Management, LLC. Mr. White has over 35 years experience in law enforcement, corporate security, healthcare security management, and security consulting. He is a member of IAHSS, International Association of Professional Security Consultants, International Association of Chiefs of Police, National Association of Chiefs of Police, ASIS International, and serves on the Healthcare Security Council of ASIS International and the Commission on Certification with IAHSS.)

We all know to what extent our employers go to insure compliance with HIPPA, and yet there are almost daily breaches of Protected Health Information (PHI) somewhere in the country. It has been stated that anywhere between 30-45% of the breaches involve staff from third parties, or in the case of hospitals that could include vendors, doctors, and students just to name a few. In fact, if you go back and look at the number of complaints filed with the U.S. Department of Health and Human Services (HHS) since 2003, there has been a steady rise in the number of total complaints going from 3,742 in 2003 to 10,443 in 2012 (Source hhs.gov). Not all of these complaints are due to 3rd parties, but the likelihood is that somewhere between 30-45% are. So what does your organization do to prevent unauthorized access to PHI?

Since 30-40% of the actual


Total vs BA Breaches
8000000
6000000
4000000
2000000
0
Total
BA Involved
Unauthorized Access
Theft
Loss
Hacking/IT Incident
Improper Disposal
Unknown

cases of HIPPA violations are related to third parties, you might think that organizations are carefully screening those resources prior to giving them access to the facility. (See chart which shows the BA--Business Associates--portion of breaches.) Unfortunately, you would be wrong in many cases because hospitals have been known to not conduct background checks on third parties. In fact, they often relegate that duty to the vendor firm to conduct the background checks on their staff. Yet, when there is a HIPPA violation, it is the hospital that is often on the hook for fines and sanctions. Because of that you would think that hospitals would put forth their due diligence efforts to not only screen those that will be in their facility, but also that they take extra precautions to insure that those vendors will not have access to PHI.

THE 'DUAL EMPLOYER' CONCERN

Consider for a moment that hospitals often bring in temp employees for things such as clerical, travelers, Locum Tenens, consultants, construction workers and many others. Hospitals have also been known to have vendors present during surgeries and other medical procedures to demonstrate new medical equipment. In many cases the hospital requires that the company they are getting temporary staff from conduct background checks on the temp staff. However, if you ask the hospital what the extent of the background investigation is on the temps, you often will hear that they are not sure. I know I have been told by hospitals that they want to keep their responsibilities at arm's length because there is a "dual employer" concern and that they are not responsible for the temps.

There are even cases of clergy being allowed within the hospital, and given hospital identification to wear while upon the campus, and those clergy have been convicted of sex crimes and are on the Sex Offender websites. When asked who conducted their background checks prior to being issued a hospital ID badge, there were a lot of those deer in the headlight looks in the room. It is incumbent of the hospital to insure that the PHI of their patients is protected at all times, and in many cases the hospital will be held accountable and need to re-

port breaches of HIPPA even when it involves a third party.

STOLEN LAPTOPS AND UNATTENDED COMPUTERS

Many cases of PHI falling into the wrong hands is a result of electronic PHI being compromised on laptops and removable computer drives. It is almost a weekly occurrence that a laptop is stolen from a healthcare provider and on that laptop are PHI and patient identifiers. In the past when I have been on medical center campuses, I have noticed computers unattended with a user logged on. Many times I have also found patient charts unsecured with no one around, or patient lists lying out. I can report that hospitals have gotten a lot better at removing information from public view. For example; monitors or marker boards in the ER have been changed to eliminate names and medical information, so if you are in view of the information and not a staff person that needs to know, you will not likely know why a patient is there, or what their name is.

Information technology appears to be the leading cause of PHI breaches, so it should be the highest priority for a hospital to control this information. However, if that was the case why is this information still getting out each month? As healthcare providers move to get patient records online and available to the patients there have been some issues with the security of the information. As we see often on the news there are people out there hacking into computer networks. Right now there is a substantial concern with the Healthcare.gov website over this same issue. This means that those that are responsible for online security of PHI have to insure that their systems are secure. In some cases hospitals have 3rd parties that provide this service, meaning their Information Technology department may be partially or wholly contracted staff.

WHY ARE BACKGROUND CHECKS DIFFERENT THAN OTHER VENDOR REQUIREMENTS?

The issue often comes down to who is doing background checks on vendors, contractors, students, and non-hospital employees? Are those backgrounds at the same level as the hospital's backgrounds? What sources are they using for obtaining their informa-

tion, and has that source been vetted? Although hospitals and medical offices may wish to keep an arm's length from any hiring decisions made by vendors, can they afford to do so with little or no oversight?

Hospitals currently require vendors and other non-employees to meet other requirements such as hepatitis vaccinations, Environment of Care training/orientation, and other regulatory or accreditation standards, and they do so onsite so that the hospital can verify compliance, yet why are backgrounds any different?

In my professional career I have seen numerous issues where vendor employees have been the concern when it came to theft of inventory, equipment, or electronic information from healthcare facilities. In a majority of the cases there was information in the employee's background that should have been found and made available to hospitals/medical offices prior to allowing that person to work within the medical center, or have access to confidential information or security sensitive areas. However, the third party that employed that person either did not do a comprehensive enough background prior to hire, or did so and made a decision to assign that person to the medical center anyway.

LIMITATIONS OF BACKGROUND CHECKS

In almost all cases where I have reviewed the background check process for medical centers and offices, I have found that the organizations are doing a decent job of researching an applicant's background. In most cases they are contacting previous employers, references, and in many cases they have a third party online service that scans court records for criminal cases involving the applicant. However, when you call previous employers you often get just the facts; Date of Hire, Job Title, Rate of Pay and that is it. It seems that employers are very hesitant to give anything more for fear of civil action being brought against them if they say more. As for references, what applicant would ever put down someone's name that would say anything bad about them? Really, references listed on every application are more than likely someone that has agreed to be nothing more than a good reference. It begs the question why references

are even asked for. In reality it comes down to an employer who cannot afford to not ask for them, because if there is an issue later down the road they can state that they reviewed and contacted the references provided by the applicant. I have spoken with many Human Resources staff that conducts backgrounds and they all say that they know that references are always going to say good things about an applicant, yet they have to call them anyway. So do we think that a vendor is going to do any better?

VERIFYING A VENDOR'S BACKGROUND CHECK PROCESS

What can a healthcare organization do to ensure that the backgrounds being conducted on a vendor's employees are at least at the level that the hospital is at? First, any employer that is looking to bring in contract employees, vendors, students, contractors, and so on should verify the background check process that that vendor is using. If your organization is bringing in 3rd party staffing for a project, or long-term, and your organization is not conducting the background checks, you should at least be making a site visit to the vendor's hiring office and vetting their background and hiring process. You need to be certain that you are comfortable with their processes by conducting your due diligence. With the national level of HIPPA violations of between 30-45% being related to 3rd party staff, you have to consider risk reduction as much as possible.

IS THEIR LEVEL OF ACCESS APPROPRIATE TO THE JOB?

When it comes to vendors, and if they are going to have access to your network, you must insure that their level of access is appropriate for their job. If the duties that they are hired to perform involve PHI or security sensitive information, the intensity of your due diligence must be at a higher level, and it would be wise to perform audits on their access ongoing.

In addition to that, seeing how there is an ongoing problem of electronic devices and files being compromised almost weekly somewhere in the country, healthcare organizations need to do a better job at controlling access to PHI. Whether the risks are with online medical records accessed

over the internet, or files maintained on intranets, the issues are all the same. Let's not forgot that the old way of compromising PHI in the paper form is still an ongoing concern as well. Almost every site that I have visited this year has been found to have PHI issues where I have found patient records or papers with PHI on them lying out in plain view. I have also found computers on with PHI on the screen, and no one in the room. And I could not even begin to count the number of times when I worked as a security director where I would receive inner-office mail with PHI within an envelope that I should have never been able to view. Yet, with those inner-office multiple use envelopes, all someone has to do is forget to change the "To" on the envelope and a HIPPA/PHI violation is going to happen.

OTHER RISK REDUCTION CONSIDERATIONS

Another risk reduction measure to consider would be the disabling of USB ports on computers so that staff cannot download medical files and information to USB drives or portable devices. If you want to control sensitive information, you need to control access to it as well as the ability to move information from the network to another device. The number of laptops lost or stolen with PHI on them is an ongoing issue and yet there are encryption tools available and the ability to restrict downloading of information available and not being used.

So what it really comes down to is that healthcare organizations can do a better job of vetting their contracted staff, students, temp employees and so on. They can do so without creating a dual employer situation by merely conducting their due diligence on the third party employer's processes and practices. Access to PHI and other sensitive information must be controlled and audited, and organizations should investigate their options to reduce the possibility of anyone downloading files to a portable drive or emailing files. Remember, just like that inappropriate email you thought you addressed to your friend but later found you sent it to your boss, once that electronic message has been sent you cannot recover it, and the person that receives it can use it anyway they like. And if that message had PHI within it you now have a much bigger problem to contend with.