Medical Courier Connection

In this Issue…

As members of "the Connection," each quarter you will receive our electronic newsletter that will have regular columns written by Industry professionals and members of our Advisory Board, links to other valuable resources, and other industry news. If you prefer to obtain the newsletter from the website rather than in your email, please email ken.arnold@integritydelivers.com and we will remove you from the list.

A note from the Editor

Welcome to 2017

Just curious – if you're a client of Integrity Medical Courier Training, when is the last time you read through the Administrative manual that we produce, and what ideas did you consider for a future date that you have yet to implement?

I've always believed that once things settle down after the first of a new year, it's a good time to reflect on the previous year, the highlights and lowlights of your overall journey in this business, and to allow yourself to dream a little about where you would like to be in another year, both personally and professionally. A great place to start is a quiet late-February or early-March day where you dedicate an entire day (or long relaxing weekend) to yourself and your business – with no interruptions!

Start by taking a look at your procedures, policies, and the details of your operations. How's your network security? What about accounting? Consider asking for vendor discounts and "shopping" for better prices if you haven't done that lately. Make a list of what areas you need to improve on based on issues that came up in 2016, and what warrants giving more attention, time, and/or resources based on good or bad experiences?

In the end you will walk away with a list, yes, but guaranteed you will feel refreshed and ready to tackle the new year with some fresh vision and excitement.

P.S. Don't forget ~ We offer affordable site assessments that include route ride-along's with our training! ☺

HR/Admin To-Do's

- Obtain 2017 W4's from employees and W9s from Ics (W9s are required to be updated every three years per IRS regulations)
- Review new I-9 requirements for 2017 new-hire employees so you're prepared
- Update ICE sheets (in case of emergencies – do you have contact information for your workforce, and do they have yours!?)
- Obtain copies of driver's licenses from all employee and IC drivers
- Obtain updated MVRs (if you have IC's you can and should be requiring these annually as part of your contract and at their expense)
- Obtain updated Insurance documentation from all IC's
- Inventory drivers supplies – do they have gloves, ABRs, spill kits?
- Perform a "surprise" inspection! Do drivers lock their doors when they go in and out of buildings? Shut the car off every time? Park in handicap spots without a sticker? (that's your company's reputation at stake!) Use a carrying case? Disclose PHI? Tires have tread? Lights all work? (you get the idea!)

HIPAA – Assess Your Risk

First Quarter, 2017

Part of the training we provide at Integrity Medical Courier Training is “HIPAA” training, also known as patient confidentiality. It can include a myriad of private information relating to any patient of any healthcare service or facility.

For instance most, if not all, diagnostic laboratories include paperwork with specimens sent to the lab and in return, diagnostic reports. Included on this paperwork, at the least, will be a patient’s name and address and the type of test(s) being ordered along with a diagnosis code or codes. That information can quickly cause a breach if the paperwork is stolen; which alone is reason enough to take time to assess your exposure risk on a regular basis. Now consider that many patient sheets can also include billing information such as insurance provider, social security numbers, dates of birth, insurance policy and group numbers. If your drivers are not paying attention to the risks around them, your company could be held responsible financially by one means or another, including but not limited to the loss of a contract or client, and/or civil penalties.

In a 09/27/2015 article posted by HIPAA JOURNAL, they reported that in September 2015 Insurance Data Services (IDS), a Wyoming-based medical billing company, who had contracted a West Michigan based Delivery Service to deliver client mailings, experienced a breach when a vehicle used by the courier company was stolen. The vehicle theft was reported to law enforcement officers and an investigation into the theft commenced. Fortunately, the theft was captured by closed-circuit television cameras; however, the recordings revealed a masked and gloved individual entering the vehicle and driving away. Consequently, it was not possible to identify a suspect. The vehicle was found and recovered, but the contents had been taken by the thief.

No electronic PHI was exposed; but patient mailings were taken from the vehicle. The information contained in the mailings did not include any Social Security numbers, financial information, dates of birth or medical insurance numbers; however patient names, phone numbers, addresses, treatment codes, diagnosis codes, account balances and health insurer names were potentially compromised. Approximately 2,900 individuals are understood to have been affected by the security breach.

It was not clear whether the vehicle driver was to blame in any way for the vehicle theft, but IDS did make the decision not to use the company for any future deliveries. IDS also revised its policies to prevent similar incidents from occurring in the future. (source: http://www.hipaajournal.com/car-theft-results-in-exposure-of-phi-of-2900-individuals-8117/)

(continued on next page)

According to the US Department of Health & Human Services Office of Civil Rights Division , "The BA provided breach notification to HHS, affected individuals, and the media. The BA also updated its procedures to utilize a secure client portal to transmit PHI with clients. As a result of OCR's investigation the BA created policies and procedures relating to safeguarding PHI, using and disclosing PHI, and Breach Rule Notification and trained its staff on its policies. The OCR obtained written assurances that the CE completed the corrective actions listed."
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (10/08/2015)

Is this something you want to handle after a crisis, or would you prefer to prevent one? We've heard companies say that they believe they are exempt from the rules because of a reference in the regulation that states, "…organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all." (See 45 CFR 164.502(e). As you can see above though, that exemption did not apply for the courier who was servicing IDS.

"HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected." What caused such a stern statement? In 2016 Raleigh Orthopaedic Clinic, P.A. of North Carolina "potentially violated" the HIPAA Privacy Rule by handing over protected health information (PHI) for approximately 17,300 patients to a potential business partner without first executing a business associate agreement. The group agreed to pay $750,000.00 in settled charges for that violation!

Our suggestion is that now is a great time to review your policies, procedures, safety protocols, and what your client's expectations are in the event there is (1) an exposure, and (2) a breach. Do you have Business Associate Agreements in place? Have you asked your drivers to assess their risk? If they're in a rougher neighborhood or section of the city, what protections have you put in place – or what requirements have you made clear? Locking vehicles, never leaving them running, never abandoning client products (specimens, charts, files, interoffice mail, supplies, etc.) even for a moment!, never discussing patient information with anyone outside of the company and only discussing patient information with coworkers when it is necessary, are all good rules to have in place. If you don't have a contract with your IC's – get one! If you don't have clear policies and standard operating procedures for employees – start writing down what you need and get that in place! If you get training from us, do you have those signature pages on file for every employee and IC that we provide at the back of the manuals?

If you need a Business Associate Agreement, HHS offers model business associate agreement language at: http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Websites, Social Media & Networks

Networks

How many of you follow the "Digital Goddess" (aka Kim Komando)? I usually don't buy a tech product without consulting her website, PC Magazine, or some other reputable source first.

Recently Kim Komando included in her newsletter for small businesses a warning about Ransomware. The statistics she provided were startling with respect to how many businesses actually pay the ransom to get their files back! She stated that "in 2016 alone, cybercriminals were able to earn $1B by spreading ransomware." She then stated that it's not a matter of if your small business will be hit, it's a matter of when.

The top three suggestions you can do today to safeguard your company against cyber threats included: (1) Patch your system! You know those pesky little updates that software providers send out. DO THEM! (2) Train your employees! You're only as strong as your weakest link. Don't allow cybersurfing, opening personal emails, opening attachments unless they are expecting a file, use of private/personal applications like Dropbox, Spotify, or Slack, or accessing personal social media accounts. Make it a serious offense in your company. (3) Have a backup plan! Carbonite is a great backup service that we have used for years. We also use Quickbooks Online accounting software because it is regularly maintained, updated, backed up, and far more secure than we could provide on our own.

Your Website

While you're at it, when is the last time you looked at every page of your own website? What's outdated? Sick of those old images? Spend a dollar per image and update them by going to 123rf.com! Once you have your site spit-shined and your information up to date, make sure you have maximized your search engine optimization by checking what keywords your pages are hitting on.

Social Media

I won't talk long on this because social media seems to have taken over the business world but honestly, if you're spending too much time, consider saving some by looking into Hootsuite. It's a Social Media Marketing and Management tool that lets you write one post that will hit multiple sites and be formatted to work well with each one. You'll still have to read each one to get updated but now you won't need to spend a lot of time posting in multiple places just to "stay out there."

Don't forget to update your profiles! Even just a new photo is enough to generate hits!

Emergency Preparedness

Preparing for an emergency can be anything from a significant amount of your workforce coming down with the flu, to an accident that puts you out of commission for a period of time, to a major weather or natural-disaster event, to a single gunman involved in a robbery, or a full-on terrorist event. We've had plenty of events in various parts of the U.S. over the past several years so any of these scenarios shouldn't be hard to imagine how they could effect you and your business. But what about a financial crime? How would you deal with that? What about a lawsuit? Or a personal family crisis? These are all things we hear about from time to time but rarely consider ourselves to be at risk of experiencing these events that interrupt life as we know it.

There are a multitude of resources that you can and should check out so you don't miss a step in this all-too-important piece of risk assessing and emergency planning!

- If you're a client of Integrity Medical Courier Training, take a look at the Admin section of our manuals where we've included some short quick tips.

For a much broader perspective of considerations,

- Check out the SBA's site at https://www.sba.gov/managing-business/running-business/emergency-preparedness/emergency-preparedness
- Check out Ready.gov's website at https://www.ready.gov/business
- Check out the CDC at https://www.cdc.gov/niosh/topics/emres/business.html
- Check out FEMA resources at https://www.fema.gov/media-library/collections/357
- Check out Homeland Security's resources at https://www.dhs.gov/how-do-i/prepare-my-business-emergency
- Then there is the Red Cross at http://www.redcross.org/get-help/prepare-for-emergencies/workplaces-and-organizations
- And the IRS at https://www.irs.gov/businesses/small-businesses-self-employed/preparing-for-a-disaster-taxpayers-and-businesses

You really don't need to read every single thing provided above but a quick glimpse at those pages will certainly help you to think of things you may not have thought about!

It would certainly be beneficial for you to also google search your City and County's Emergency Preparedness and Disaster Plans! Maybe if you're properly equipped and prepared, you can consider putting your company on their vendor list to help out!

Benefits of Membership

- Inclusion in the Business Directory that we make available to Healthcare Professionals seeking medical-specialty courier services.
- Free live webinars with Industry professionals & Advisory Board members
- Free quarterly e-newsletters
- Access to Free publications, past webinars and previous Medical Transportation Summit presentations

If you're not a client of Integrity Medical Courier Training, give Ken a call for a free preview of our training or visit us at www.IntegrityDelivers.com
We offer on site, live webinar, and recorded training options!

How many other training programs offer [on-site classes and service](#) for up to 3-days?
We do!

When we come to your facility, we'll provide you with a risk and site assessment, go with your sales team to meet and see the companies you service, make recommendations for safety, HIPAA, route efficiencies and supplies, train your new-hires and retrain those whose certification has expired including dispatchers, admin, and ops! [Pick 1, 2, or 3 days!](#)

[Prefer live webinars for your company?](#)
We offer live training 6-days per week, morning, afternoon, and evenings to accommodate every time zone and courier schedule!
Sessions include all elements of courier-specific bloodborne pathogen, exposure control, specimen integrity and HIPAA.

[Do you have IC's?](#)
We offer two affordable, pre-recorded, on-demand "Awareness" classes that can be taken at your IC's convenience 24/7/365 from your office or their home!

[Bloodborne Pathogen/Exposure Control](#) $14.95
[HIPAA Compliance](#) $12.50