As we bid farewell to late night comedy host David Letterman, I thought it appropriate and timely to give a nod to one of Letterman’s most iconic segments, his “Top 10”, with my own Top 10 list for complying with applicable Security Law:

#10. THE HIPAA SECURITY AUDIT. If you are feeling overwhelmed and anxious with every new Big Data breach announced (hello Anthem!) and don’t know where to start with getting your own Security Compliance program up to snuff, start with the HIPAA Security Audit. Not only is it legally required under HIPAA (see 45 C.F.R. 164.306), the comprehensive checklist of Technical, Administrative and Physical Implementation Specifications that must each be evaluated, if done right, will get your organization well on its way to identifying risks and allowing it to hopefully prevent a breach before it happens. Unfortunately, many organizations either do not complete the Security Audit properly (not thorough enough) or do not do enough to mitigate the gaps that are identified. Concentra recently ended up paying the feds (HHS) $1.7 Million because although they identified 254 of their 597 laptops were NOT encrypted, they did NOTHING until a breach caused ePHI to be compromised when an unencrypted laptop was stolen. So the moral of the story here is complete the HIPAA Security Audit, do it right, and if you identify gaps in security, fix them!

# 9. LEARN FROM RESOLUTION AGREEMENTS. The Federal Department of Health and Human Services (HHS) posts every resolution agreement it enters into with a covered entity for HIPAA non-compliance (and in the near future, we expect to see resolution agreements with Business Associates too!) To date, there are 24 Settlement Agreements posted and one lucky winner (Cignet) that was assessed Civil Monetary Penalties. You can read them all here: www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html. Why are these important for Security Law compliance? Because they highlight areas where others have fallen short, and what issues HHS has focused on and looks for in an effective security compliance program. Resolution Agreements are a GREAT opportunity to learn from others’ mistakes. Failure to complete updates
Another summer is underway. Fiscal Year 2015 has come to a close, and a new fiscal year is upon us.

And many new, yet exciting changes are happening all around us. The New Jersey community providers are gearing up for a “Fee for Service” system, and wondering if reimbursement rates will be adequate to keep them fiscally viable.

To address the issue of fiscal viability, the IT Project knows that we can assist by helping providers save money on some of your information technology infrastructure costs. Consider phones, Internet and cell phone expenses, for example. The IT Project can definitively guarantee, that by working with one of the recommended NJAMHAA vendors, we can save you at least 10% on your overall telecommunications expenses. Now for a small organization, maybe 10% doesn’t seem to be all that much. But over time it does add up. We have some other organizations that pay upwards of $36,000 a year, and saving $3,600 is money that can be put to better use to serve consumers, or offer to employees to boost morale. Why pay more when you don’t have to. It’s like getting free money, just to have your contracts, plans and usage reviewed. There are even painless solutions, where you may not even have to switch carriers. The IT Project is here to help YOU! So give us a call and challenge us to help you save some money on things you need to keep your infrastructure running smoothly, such as phones and Internet services.

The next big change is for healthcare providers is to be interoperable. In healthcare, interoperability is the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.

The IT Project can help you understand what you need to do and assist in getting started if you haven’t already. Of course, if you have an electronic health record, and have attested for Meaningful Use, then of course, you’re more than three-quarters the way there.

One of the biggest changes for all of the contracted providers who offer substance use treatment, is that on July 1, 2015, the Division of Mental Health and Addiction Services (DMHAS) launched an Interim Management Entity (IME) in lieu of the originally proposed Administrative Services Organization (ASO). This new IME will provide the much needed care coordination, authorizations and referrals needed to serve those seeking help with a substance use problem.

On a national level, the new ICD-10 implementation goes into effect October 1, 2015. That’s just a few months away. And with that, a new DSM-V has been created by the American Psychiatric Association (APA) that is causing havoc everywhere from a licensing standpoint. Now that so many provider organizations are using Electronic Health Records, the APA has found a way to monopolize on this, and charge user license fees for incorporation of the DSM into an electronic health record. Even NJ DMHAS has been having an uphill battle in being allowed to use the DSM-V in the NJSAMS platform.

And that means that users of NJSAMS must continue to capture and record the DSM-IV as well as the DSM-V and ICD-10 codes for their own billing and/or internal purposes. I’ve discussed this matter with several different providers expecting to hear cries of help. Instead, time and again, I was told, “Not a big deal for us. We have a crosswalk built into our system.” And I immediately felt a sense of relief, “That’s great. For once, the providers are okay with having to report data to the state in multiple ways and formats.”

As we gear up for the new USTF portal, the data collection effort becomes even more challenging. At this time, providers will be sending the ICD-10 diagnostic codes instead of the DSM-V codes. Of course, the DSM-V is almost identical and is really a sub-set, if you will, of the ICD-10 code set. But, I’ve been told there are some definitional characteristics that may be a little different, but it’s doubtful that there will be a major push to collect the DSM-V codes. So this may be good news for those who have enter data into the portal. Less data entry is always welcomed!

The challenges with the USTF, as I see it, has to do with an initial data load, and how the state is going to get there. With every provider having to send a data set of about 200 fields, for every active client in the organization, without additional supports from the state. It is going to take a lot of resources in time and money for the providers. The IT Project will continue to forge ahead and assist with these issues. We are looking to put together a small group of stakeholders that would like to contribute positive ways to tackle the new USTF requirements, and we hope to meet shortly inAugust or September. Change... It’s inevitable … All we can do is learn to adapt and make the best of it! You can always learn more or provide for a more interactive relationship with the IT Director at DMHAS by attending the IT Project’s quarterly IT PAC meetings. All are welcomed to attend, share and contribute ideas on improving the systems for everyone. The next meeting is scheduled on Monday, September 28, 2015 at 10:30 a.m. at NJAMHAA’s office in Mercerville. For details and to get involved, contact Ron Gordon, Associate Director of the IT Project, at 609-838-5488, ext. 215, or rgordon@njamhaa.org.

Peace to all. Have a wonderful summer.

June Nato, Director, IT Project

P.S.: SAVE THE DATE: MARCH 2, 2016 for the NJAMHAA IT PROJECT annual IT Conference, being held at the Pines Manor, in Edison, NJ.
Anyone who has been involved in any type of conversation about the state of the healthcare industry over the past couple of years, especially on the behavioral health side, comes away with two overarching questions. First, how much money is being lost by our healthcare system because behavioral health hasn’t been properly integrated and leveraged? And second, when will the primary care community begin the process of actually integrating behavioral health services into its workflow?

For the past few years, I’ve had the pleasure of participating in several large events and conferences where techies and healthcare policy leaders from around the world gather to discuss issues of interoperability and connected care. Attendees range from giant Electronic Medical Record (EMR) companies to smaller Electronic Health Record (EHR) companies like Foothold Technology. It seems that very few of the larger EMR presenters at these conferences had thought of, or were working with, behavioral health providers. For many of them, “coordinated care” meant only coordinating the various providers of physical healthcare. Most participants expressed astonishedness at the idea that smaller EHR companies, working exclusively with behavioral health, mental health, intellectual/developmental disabilities and substance abuse providers, were even able to share data through HL7 or C-CDA formats. And yet, all expressed interest in accessing such data and putting it to use to help improve care across the continuum. Primarily, this is because everyone sees the payment models changing. In the near future, the success of a given healthcare organization will increasingly depend on its ability to arrange coordinated care among different providers and create value by offering the right service at the right time at the lowest cost. Increasingly, the healthcare world will begin to realize this means working with behavioral health providers.

Let’s take a look at a fictional scenario to describe the power of connected care and the need for interoperability. Imagine a scenario where a woman with breast cancer and resultant depression is receiving services and treatment from various providers. Let’s say that our fictional character decides to undergo surgery and has follow-ups with her oncologists and psychiatrists. With interoperability, an EHR can receive data files from all service providers involved in her care and can take that data from those services and parse them directly into that EHR database. This would also mean that medications, for example, that are prescribed by an oncologist can be imported into an EHR and put directly into a medication module for this consumer without direct data entry by users of an EHR. EHRs and EMRs track different data, yes, and behavioral health is usually chronic, while medical care is usually episodic. But, the underlying capabilities of the systems are not materially different. In this scenario, with interoperability, the central character is able to not only receive coordinated care, but also, clinicians and providers are able to provide the best possible treatment and services to meet her holistic needs.

The good news is that many of the things we used to just talk about, like data exchanges, the shifting of funding streams to some kind of value-based alternative payment model – those things are beginning to actually happen. In fact, Foothold Technology’s electronic record and human services software, AWARDS, can address all these issues of interoperability today.

If you are interested in speaking with someone at Foothold Technology about AWARDS, contact Nick Scharlatt at nick@footholdtechnology.com.
As most Windows based personal computer users know, Microsoft periodically issues patches and updates for its operating systems. These updates sometimes include new features and important security enhancements designed to improve the users’ Windows experience. Recently, a member of Microsoft’s Windows CXE patch team, Thierry Paquay, expressed some ideas as to how Microsoft would like IT professionals to approach this potentially critical aspect of Windows support for not only the soon to be released Windows 10, but all Microsoft products. To get the desired feedback, Microsoft is encouraging those who manage organizational level support to be more proactive in the installation of the various forms of updates and to turn on telemetry reporting to allow the return of information to Microsoft. Heading the list of update categories in order of importance are: security updates, hotfixes, and optional and convenience updates. For those concerned about any changes in Windows 10 hardware requirements, Michael Beck, Microsoft Partner Director for Windows CXE, assures that no changes are required if you are using Windows Vista and above. That is to say, if your PC is functioning on Vista, Windows 7 & or 8.1, or Windows 10, it will run fine. The option of performing a full wipe and load, as well as an in-place upgrade, will also be available. For more details please see the following: https://redmondmag.com/articles/2015/05/18/marching-orders-for-it-pros.aspx

Microsoft Provides Advice on Windows® 10 Updates

Microsoft Announces New Editions of Windows® 10

In order to capitalize on various operating environments and devices, Microsoft will issue different versions of its new ‘Windows® 10’ operating system. In addition to the anticipated Windows 10 Home, Pro and Education versions, Microsoft will offer the following variations:

Windows 10 Mobile is designed for the smaller, touch screen devices like smartphones and smaller tablets. It will offer security and management options for those using their personal devices in the work environment.

Windows 10 Enterprise is designed for the mid-to large-sized organizations, providing options to address the concerns of today’s threats against company information, devices and identities.

Windows 10 Mobile Enterprise may be seen as a combination of the previously mentioned versions, allowing for businesses to better manage enterprise specific features, as well as mobile devices.

Other versions of Windows 10 for industry environments will be available for devices such as ATM’s, handheld terminals, retail and robotics.
to the Security Analysis, failure to encrypt devices, improper disposal, lack of policies and processes, and failure to implement security measures are among the mistakes HHS has no tolerance for, and that your organization cannot afford to make. We know this because others have made the same mistakes, and the Resolutions Agreements tell us that these failures resulted in hefty settlement amounts, to the tune of millions in some cases, that Covered Entities had to pay to HHS.

# 8. LEARN FROM BIG BREACHES. We all shake our heads when the next big data breach hits the headlines -- “Anthem hacked, 80 Million records compromised”; “Premera breached, 11 Million records compromised”; “TRICARE unencrypted back up tapes stolen, 4.9 Million records compromised” -- and the list goes on, and on. Indeed, these headlines induce uncontrollable head-shaking in shock, in disgust, in exasperation. But, these cases also offer another opportunity to LEARN from others’ mistakes. With each new BIG BREACH case announced, we should be asking “what went wrong?” and “how do I prevent that from happening to my organization?” In Anthem, while the facts are still coming to light, it is known that the access credentials of a System Administrator were somehow obtained and this led to an external hack. The employee realized this when he saw queries running across the database, which he did not initiate (good catch, employee!). This was immediately reported, and notifications were issued to individuals without delay. One take away here is to ask why or how the access credentials were compromised. Employees should be WELL educated and trained regarding not sharing access credentials, not writing them down (and throwing them out), not storing their user name and passwords in unsecured electronic devices, and not responding to “phishing” emails where someone poses as “IT personnel” and asks for the employee’s access credentials. Do your employees all have a heightened sensitivity to phishing for access credentials? Does your organization have policies that prohibit IT personnel or others from requesting access credentials by email or other unsecured or unauthenticated means? If you don’t, you should - or you might end up like Anthem.

# 7. GET CONTROL OVER YOUR BUSINESS ASSOCIATES. I know. Trying to get Business Associate Agreements in place with vendors is as easy as herding cats. But, it must be done. All vendors that require access to PHI to perform a function or service on behalf of a covered entity are business associates (note: if they don’t require access to PHI, then the vendor is not a BA and a BAA is not needed). Once you have identified all your BA vendors, getting contractual language in place is critical; and, I don’t mean just “HIPAA-compliant” BAA language. There is a lot at stake when an organization hands over their PHI to a third party, and although BAs are now directly liable for non-compliance with the HIPAA Security Rule, a basic bare bones HIPAA BAA does not address a LOT OF OTHER STUFF. There are many other important issues to be addressed, such as allocating responsibility as to who secures ePHI and when, allocating risk, allocating costs and liability, and migration of the data post termination of the relationship (and who pays and how much?). The time to address these issues and manage these risks is during the contracting process with your BA vendors, because later it will be too late.

# 6. SOCIAL MEDIA & THE INTERNET. Does your organization have policies specifically regarding social media use and the Internet? If it doesn’t, it should. Use of professional chat groups and other social media may be appropriate, but disclosing PHI on such sites, either inadvertently or negligently, is not. Things I’ve seen: a video is posted on YouTube for what seems like a good cause, but when you zoom in on the video, you can see a whiteboard with patient names and other identifiable information in the background (this is a breach); a doctor posts a case on a professional chat circle to see what other colleagues think about the case, but while she does not disclose her patient’s name, she discloses sufficient other general information that someone on the chat group coincidentally was able to identify the patient (this is a breach); a nurse posts a picture of a patient’s echo cardiogram on her Facebook site that shows a very, very rare disease. Since it’s just a picture, she thinks there is no way that the patient can be identified. However, one of her distant “friends” knows what hospital she works at, and knows that her neighbor has spoken about having a rare cardiac condition that lines up to the picture and so in all likelihood can identify the patient (this is a breach). Social media and the Internet pose a new wild west and challenge for security. Corralling in this relatively new security risk starts with developing good policies on these topics, and then educating employees on what is and what is not allowed when it comes to the Internet and social media use.

# 5. NO SNOOPING! The temptations can be great, but employees must be made aware of the repercussions of snooping. Snooping violates patient privacy and security. In Walgreens v. Hinchy, a jury awarded a patient/customer 1.44 Million dollars because a Walgreen’s pharmacist snooped in a patient record for her own personal purposes (she wanted to know if her husband’s ex-girlfriend had a prescription for a condition that she believed her husband contracted). In the Walgreens case, the corporation was forced to pay up under legal theories of respondeat superior, making an employer essentially liable for the illegal act of its employee. But this case might have been avoided with better training and internal sanctions. Employees should also be made aware that State AGs have CRIMINALLY PROSECUTED individuals, including doctors, nurses and other staff, who have snooped in patient records with NO legitimate purpose. Therefore, the stakes are high (for both the employer and the employee), but the solution is easy. If the reason one wants to access a record is not an “authorized” purpose (i.e. treatment, payment, health care operations etc), then the access is prohibited. Period.

# 4. E-MAIL & TEXTING. Gmail, msn, iCloud, yahoo, hotmail etc. THEY ARE ALL UNSECURE! Patient information should NOT be sent through unsecured email and texting. Unfortunately, employee non-compliance is high as they do not want to give up the efficiency of using these easy means to “quickly” send a file or other patient information. Unfortunately, the speed at which the information travels does NOT directly correlate to the level of security those methods offer. With all the focus HHS is placing on encryption and how breaches could have been avoided with encryption, I would not recommend allowing emailing and texting (there is an exception HHS allows if a patient requests for their PHI to be sent directly to them by email, and is informed of the
Providers Must Prepare to Thwart the Threat of Cyber Attacks

Data breaches have dramatically increased in the past year, but the future may bring even more cause for concern to companies defending themselves against cyber-attacks. A new avenue of opportunity is coming to light from beyond the standard platform of mainstream PC’s, namely people’s personal “connected” devices. These devices can offer malicious hackers alternate entries into corporate systems.

Victims of recent cyber-attacks, thinking they were adequately prepared, now realize that being prepared means more than it did yesterday. Anticipation of the next attack is something corporations are now striving for to protect themselves from intrusion. Gathering information to thwart threats is becoming increasingly desirable through real-time analysis.

Responding to potentially destructive attacks has become an industry in itself. Many corporate executives and decision makers are now taking a more in-depth look at the alternatives at hand. Can success be achieved internally or is an outside entity better suited to the task? Whatever choice is made, minimizing the effects will be the goal to reach.

For more information, see the presentation, Why Providers Need to Rethink Incident Response, http://www.healthdatamanagement.com.

Malware Containment Runs High Costs to Organizations

As recent history has shown us, destructive malware can have a major impact on an organization’s standing on the world stage and its operational costs. Companies such as Sony Entertainment and Target have fallen victim to these attacks, indicating that no matter how big they are, vulnerability is hard to avoid.

Data gathered in various surveys show that a typical organization may encounter as many as 17,000 alerts on a weekly basis. On a larger scale, time wasted responding to erroneous information may average up to $1.27 million per year. Also contained in those surveys is information supporting the belief that the participants feel the severity and volume have increased in the past year.

Knowing the risks involved with malware, how are companies prepared to defend themselves? Based on the survey results, more than 60 percent have organized systems while more than 30 percent prefer an “as needed” approach. However, approximately 40 percent state there is no one person driving the activities, while about 45 percent say a Chief Executive level person is responsible. Going further, close to 70 percent of the participants rely on vendors or peer level sources for their intelligence. Less than 50 percent have automated tools in place and those that do say an average of 60 percent of malware containment can be handled by those tools.

For more in-depth details, please see http://resources.idgenterprise.com/original/AST-0139548_Damballa_Ponemon_Malware_Containment.pdf.

chorus communications
Call Rob Molinaro for all your data and telecommunication needs. Tell him that the IT Project referred you! 215-922-1862 rmolinaro@choruscommunications.com

quali facts
Bob Marasa
robert.marasa@qualifacts.com
615.386.6755

HUNTER TECHNOLOGIES
Gene@huntertechnologies.com
732.542.9292
"Top 10" List for Security Law Compliance

Continued From Page 5

security risk of the provider/covered entity doing so). Luckily, secure alternatives and solutions are continuing to pop up, such as DIRECT messaging, encrypted patient portals, Tiger Text and PingMD. Look into them, and get your employees to stop texting patient information!

# 3. ENCRYPT. This includes data-in-motion and data-at-rest. If you do not encrypt devices that house or facilitate ePHI, you better have a very, very exceptional reason why you do not -- AND you have to document it (per the HIPAA Security Rule), otherwise you will be getting no sympathy from HHS when data is breached. Encryption is also a Safe Harbor under the Breach Notification Rule, so if a device is lost, stolen or hacked but the ePHI is encrypted, you do not have to notify HHS or individuals (at least under HITECH, but check your individual state’s breach laws).

# 2. REPORT BREACHES & SECURITY INCIDENTS. Here, I am talking about the internal kind of reporting. Employees are the “eyes and ears” of an organization. A covered entity must notify HHS and individuals of a breach as soon as it is discovered or “should have been discovered with reasonable diligence” (see 45 C.F.R. 164.404(a)). That means that as soon as an employee is aware of a breach, the 60-day time frame within which an organization has to make its notifications starts ticking. For this reason, it is critical for employees to know who they must report such knowledge to. If they don’t, then the covered entity can be assessed additional penalties for every patient and every day late the notices were made. Delay in notifying individuals about a breach or in discovering a breach may also lead to a larger volume of data being compromised and for a longer period of time ---which is why time is of the essence when getting information from the employee to a person who is able to properly act on it.

# 1. EDUCATE & TRAIN. The human factor is probably one of the weakest links in Security compliance. The only way to begin to try and manage this risk and weakness is to start with establishing a culture at your organization that Security is vitally important. Then, employees must be constantly educated and trained on the organization’s policies and expectations. I’ve found that the most effective method to training employees is through use cases. What should the employee do when he/she discovers a breach? What kinds of phishing emails might you see, and how to respond? A well-educated and trained workforce that is given constant Security Reminders on the latest and greatest hacking schemes and security vulnerabilities will better ensure that your Security program is more effective and your organization is hopefully less vulnerable to breaches.

Save the Date

Wednesday, March 2, 2016

2016 NJAMHAA Annual IT Conference

WIELD THE POWER
OF INFORMATION TECHNOLOGY

Piners Manor, Edison, New Jersey

For more information visit http://www.njamhaa.org/evente
Questions? Contact mbczikova@njamhaa.org
3. Mobile technology is replacing computers as the way people go online. As of May 2013, 63 percent of adult cell owners use their phones to go online. Furthermore, 34 percent of cell Internet users go online mostly using their phones (meaning not with computers).

4. Phones are connecting people to health services. One in five smartphone owners have a health app. One-third of all cell phone owners look up health information on their phones (2012).

5. People are ready to use phones to track their mental health. In a 2012 study on using mobile technology to monitor health funded by the National Center for Biotechnology Information, 79 percent of respondents reported a positive attitude toward the use of free mental health phone apps. Again, blacks were more likely than whites to own smartphones (43.1 vs. 20.6 percent) and held a more positive attitude toward free use of the prototype system than whites.

6. Another 2014 study found that nearly 70 percent of respondents were interested in using their phones to monitor their mental health. Interest was near 80 percent among respondents under 45 years of age.

As you can see, mobile technology is making it very easy for people of all backgrounds to be connected to the tools of a modern society. Health applications are becoming more important to consumers as they look for ways to be more involved with their own health monitoring.