Don’t Fall Victim To A Data Breach:

Strategies To Protect And Safeguard Personal Health Information

September 2015

NATIONAL ASSOCIATION OF
Community Health Centers
7501 Wisconsin Avenue
Suite 1100W
Bethesda, MD 20814
Phone 301.347.0400
Fax 301.347.0459
www.nachc.com

ACKNOWLEDGEMENT

The National Association of Community Health Centers promotes the provision of high quality, comprehensive healthcare that is accessible, coordinated, and culturally and linguistically competent, and community directed for all underserved populations.

We wish to acknowledge the following for their contributions to this guide:

Jason Phelps
Phelps Technology Consulting

If you have any questions, feel free to contact:

National Association of Community Health Centers
7501 Wisconsin Ave., Suite 1100W
Bethesda, MD 20814
(301) 347-0400

DISCLAIMER

This project was supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) under grant U30CS16089, “Technical Assistance to Community and Migrant Health Centers and Homeless.” (Total grant award is $6,375,000.00. Zero percent of this project was financed with nongovernmental resources.) This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by HRSA, HHS or the U.S. Government.

Table of Contents

Introduction

Health Center IT leaders are regularly reminded of the importance of the security of their network, patient data and staff's role in preventing breaches. The purpose of this information brief is to provide actionable steps for your health center to increase security awareness and provide an overview of how you can avoid your health center becoming a victim of a data breach.

The Health Information Technology for Economic and Clinical Health Act (HITECH) brought some much-needed change to the Health Insurance Portability and Accountability Act (HIPAA). Along with providing incentives for adopting electronic health records (EHR) in the form of Meaningful Use, it also added teeth to the enforcement of HIPAA – specifically, the Privacy and Security Rules. HITECH also forced Business Associates to be covered by the same regulations, which is a great move in the right direction for protecting PHI and preventing breaches.

Health records have become much more valuable in recent years, as evidenced by multiple breaches of large third-party payers in 2014-15. The FBI recently released a warning to the healthcare community that their systems are less secure than other sectors (financial, energy, etc.).[1]

> In the Health Care Cyberthreat Report published by SANS Institute in February 2014, Wilkins stated the following:
>
> These deep fines aren't the only costs health care providers need to be concerned with. According to the 2013 Ponemon Cost of a Data Breach report, expenses related to a breach, such as incident handling, victim notification, credit monitoring and projected lost opportunities, cost health care organizations globally in the range of $233 per compromised record. Additional recovery actions, such as legal actions, recovery, new security control investments, extended credit protection services for victims and other related costs, actually push the cost much higher—amounting to an astronomical $142,689,666 in the case of the WellPoint incident.[2] (p. 5)

There's more to securing PHI than just having a firewall and using strong passwords. While it's true that electronic breaches have become more sophisticated, in many cases, a data breach can happen through human error, both inadvertent and intentional.

1 http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423

2 http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

What is a Breach?

It's important to have a distinct definition of a breach before diving into how to prevent one. The International Organization for Standardization (ISO), defines a data breach (3.7) as follows: "compromise of security that leads to the accidental or unlawful destruction (3.13), loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored (3.50), or otherwise processed." [3]

Remember that, by definition, a data breach can be accidental and doesn't necessarily mean theft. We regularly hear of a company that has had data stolen or compromised by sophisticated hackers, but a data breach can be unsophisticated and even unintentional. Both types of breaches happen to organizations of all sizes. For example, AT&T had multiple breaches in 2013-14 that occurred internally where employees were inappropriately accessing customer information and selling it to third parties. This resulted in the compromise of 280,000 social security numbers and other personal data.[4] Anthem, victim of one of the highest-profile data breaches in 2014-15, had up to 80,000,000 social security numbers and other data stolen in a breach that went undetected for months.[5] The Target breach of 2013 appears to have been started through a SPAM email sent to a third-party vendor of Target.[6] This breach, while obviously sophisticated and malicious, was certainly not intentional on the part of the third-party employee.

What can a health center learn from these very high-profile breaches? Your network security and internal processes are vital to protecting your patients' data.

3 ISO/IEC 27040 - https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-1:v1:en

4 http://www.reuters.com/article/2015/04/08/us-at-t-settlement-dataprotection-idUSKBN0MZ1XX20150408

5 http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

6 http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

Safeguarding PHI

HIPAA regulations defined three types of safeguards for the security of PHI[7,8]:

- Physical safeguards (datacenter security, facility access control, workstation security)
- Technical safeguards (unique logins, staff have access only to information required to perform duties, encryption, etc.)
- Administrative safeguards (risk analysis, training, audits, etc.)

Physical Safeguards

HIPAA guidance from the Department of Health and Human Services (HHS) discusses a wide range of items around physical security. For the purposes of this issue brief, however, we'll focus on a few major items.

Facility Access and Control

The first is your datacenter, or server room. In some health centers, this room takes up several hundred square feet and has dedicated cooling units. Other health centers may have their server located in the closet with the mops and medical supplies.

If your EHR data is stored on a server in a shared closet space or even in an open office area, this is a quick change you can, and should make to significantly secure your data. EHR data should never be stored on a server that is physically accessible to anyone other than those responsible for maintaining that server. It is recommended that a designated person (CEO, COO, etc.) have access to the server room during an emergency if IT staff is unavailable. Having custodial staff or third-party vendors with access to that server is inappropriate. Preferably, key card access would be used for that room that logs all entries/exits and only authorized persons would have access. However, in some cases this isn't practical, so a key that is unique to that room is certainly acceptable. For security inside the room, having video monitoring is an excellent way to monitor and fully verify who has accessed the room. There are many inexpensive webcam options at big-box retailers and online retail websites. Most of these would only record when motion is detected, which helps reduce the amount of storage needed to store the video recorded. This will help when your organization audits access to the room, as all access would be recorded by video.

7 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

8 http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Workstation and Device Security

Workstations should also be physically secure. Laptops that are taken outside the health center should not be left in automobiles or unsecured while traveling.[9] Desktops, which are not practical to lock in a cabinet, can be secured to a desk to prevent theft. Staff should check for unauthorized or unrecognized devices plugged into desktop computers and report them to the appropriate IT staff. This can result in loss or theft of data, and is often unnoticed by staff [see section on data encryption].

Technical Safeguards

When approaching security for your health center's network and data, it's important to think about security in layers. A good analogy would be bulletproof glass. Bulletproof glass is not just a thick layer of a single material, but instead multiple layers of the right materials to build an impenetrable glass. Network security requires the same approach. There was a time when firewalls and antivirus were sufficient for securing a network, but that is no longer the case.

Firewalls, antivirus, SPAM filtering, threat protection, backup and disaster recovery (BDR), and policy management and training are all critical components of a layered security model. This approach provides a failsafe in the event that one layer fails, much like the bulletproof glass analogy.

There is wisdom in having a trusted IT partner with whom you can discuss your security needs (even if your health center has dedicated IT staff). That partnership can help save time and money by bringing expertise to the table that your staff do not have. When selecting an IT partner, find one with people who focus on security and preferably a partner with healthcare information technology (HIT) experience. That experience helps with navigating through legal requirements and translating them into technical terms that you can understand. A trusted IT partner can provide guidance and recommendations with all of the areas listed below.

Firewalls

Your network should be protected by a business-class firewall that includes Intrusion Prevention System (IPS) and/or Intrusion Detection System (IDS) modules (or software). If your firewall, router or wireless access points can be purchased at a big-box retail store, you should consider replacing them with something that is designed for an enterprise environment.

IPS/IDS systems provide monitoring and alerting for intrusions or malicious activity. As with most technology, however, any IPS/IDS system is rendered useless unless it is properly *installed, configured and monitored* by someone who is qualified to do so. This could be done by internal IT staff if they are properly trained or certified, but there is a strategic advantage to having those systems monitored by a third-party who has contractual obligations to monitor your network. This decreases the burden on your in-house staff and allows them to focus on daily operational tasks. It also relieves your health center of the cost of maintaining proper ongoing training for IT staff.

9 http://www.modernhealthcare.com/article/20141220/NEWS/312199922

Antivirus

Antivirus software is something that is required, but is not solely sufficient to protect your network. Always be sure your antivirus software is up-to-date, configured to scan USB devices that are plugged in (or, better, prevent them from working when plugged in) and regularly running thorough scans of all your systems. Generally speaking, this is not something you should purchase from a big-box retailer, but through your IT vendor.

SPAM Filtering

SPAM filtering is an important part of a layered security model. Unwanted emails are not only frustrating because they fill our inbox, they also deliver malicious content and phishing scams designed to steal money and information[10]. You'll recall that Target's massive breach was likely started through a SPAM email sent to a third-party vendor.

There are many different SPAM filtering approaches and vendors, so choosing one can seem daunting. As with antivirus tools, there is no perfect SPAM filtering tool. When working with your IT vendor for a solution, focus on finding the best fit for your health center in terms of features and cost, including ongoing maintenance.

Threat Protection

For the most part, the topics discussed in this paper up to this point have been focused on keeping unwanted entities *out* of your health center network. But what happens if someone is on the inside, or something is already siphoning data out of your network?

There have been changes in the information security industry where security companies are now able to provide insight into connections going out of your network and prevent connections to known bad actors. This approach is growing more popular, and can be delivered in different ways. When evaluating vendors, look for those who can work within your existing network without causing latency (slow connections) and without requiring significant changes to your network layout.

Backup and Disaster Recovery (BDR)

Backup and disaster recovery planning is required by HIPAA regulations for all covered entities.[11] Federal regulations not only require that data is backed up, but that covered entities test their backups to confirm they are working and make revisions as needed after testing.[12]

As with other technical safeguards, there are many ways to build your BDR strategy. Find the right balance of cost, ease of implementation and ease of testing for your health center. Compliance with HIPAA and HITECH are not optional, so work with your trusted IT vendor to find a solution that meets your needs and your budget. It is important to look at several different solutions to build a proper budget for a BDR system, especially if you do not have one in place.

10 http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

11 (CFR 164.308(7)(ii) (A)) and (CFR 164.308(7)(ii) (B))

12 (CFR 164.308(7)(ii) (D))

Data Encryption

The HITECH Act added additional language and recommendations for encrypting data "in motion" (i.e., while moving between server and workstation) and "at rest" (e.g., while stored on a server, laptop, backup media).[13] There are two steps that can be taken to address these changes. The first is to always use a VPN (virtual private network) when connecting to your EHR from outside your health center network. The second is to encrypt workstations, especially laptops that contain PHI. If a laptop were stolen that contains PHI, but that laptop's hard drive was encrypted,[14] no breach report is required since the data was not breached.[15]

Education

For all health centers, especially those without in-house IT staff, a cross-functional team of staff focused on security is a great step toward building your security plan. A great way to help educate that team is reading about current information security (infosec) trends and changes in the security landscape. The infosec community is receiving a lot of media attention because of the high profile breaches in recent months, so information is readily available for those who want to learn. Some great places to start are listed below:

- Brian Krebs – **http://www.krebsonsecurity.com**
- Security Week - **http://www.securityweek.com**
- Dark Reading – **http://www.darkreading.com**
- NH-ISAC - **http://www.nhisac.org**
- Security Bloggers Network (list of blogs, podcasts and newsletters) - **http://www.securitybloggersnetwork.com**

When your security team meets, have someone bring an article or blog post discussing security and teach the other members of the team. Combined with having a more technical person (perhaps from your IT vendor) being part of your team discussion, this can provide valuable insight to staff and give them actionable information to take to their respective teams. This is a great way to build awareness and compliance throughout your organization by grass roots teaching of staff.

13 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

14 http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

15 http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/html/2013-01073.htm

Security Audits

Writing policies and building secure networks takes a lot of time and effort. It requires changes to workflows that can sometimes be painful to staff. This can lead to non-compliance and result in a data breach. Audits help expose workflows that have not been changed as directed by policy, and also find areas for improvement within the health center's policies and network changes.

One of the requirements of Meaningful Use was a risk assessment that was to be turned in with your attestation. The Department of Health and Human Services (HHS) even released their own assessment tool[16] to help providers properly assess their environment for risk from both technical and non-technical areas. This tool provides a great baseline for areas that need to be improved upon, but the tool itself does not do the improvement. Having a third-party firm audit your health center from a technical, policy, and procedure perspective allows an outside entity to show what areas you improved as well as areas that still need improvement.

Human Layer

The final layer is one that is often overlooked. Staff, patients and outside entities are all interacting with patient data or with the health center network. While health center staff likely have a limited access "key" to the network, their "key" to PHI is likely able to access most, if not all, of patient records. The first "key" is their password. Passwords must be secure and they must be changed regularly. All too often people choose easy passwords that are easy to guess. In fact, the most popular password of 2014 was 123456.[17] Don't let that be a password in your health center.

An additional approach to password security is using multifactor authentication. This essentially means that to log in to your systems, you would have to provide two of the following:

- Something you know (like a password);
- Something you have (e.g., mobile phone, physical token);
- Something you are (e.g., fingerprint)

Many people are accustomed to this with debit card PINs and online banking asking security questions when logging in to their website. This adds a layer of security, but must be carefully implemented. Talk with your trusted IT vendor to see if this is a good fit for your health center to begin implementing.

As mentioned at the beginning of this brief, data breaches are not always intentional security attacks. Social engineering[18,19] is not only becoming more common, but doesn't require much sophistication and has led to some high profile breaches.[20,21]

16 http://www.hhs.gov/news/press/2014pres/03/20140328a.html

17 http://splashdata.com/press/worst-passwords-of-2014.htm

18 http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529

19 https://www.us-cert.gov/ncas/tips/ST04-014

20 http://www.cnet.com/news/social-engineering-cracked-palins-e-mail-account/

21 http://www.forbes.com/sites/thomasbrewster/2015/04/27/tesla-explains-breach-through-att/

While sitting in the waiting room at a local medical office recently, I overheard the receptionist confirm demographic information to a patient over the phone. What caught my attention was that the receptionist was reading aloud the birthdate and confirming the patient's first and last name – all clearly heard throughout the entire waiting room. This alarmed me because not only was this information being overheard in the waiting room, but the receptionist had no way of knowing that the person on the other end of the line was in fact the patient! By reading the "credentials" of the patient to the person on the phone, it wouldn't have taken much more to have a data breach of that patient's data. A few questions like "what phone number/address do you have on file for me?" and "I recently had to change my Social Security number, could you please confirm that you have my new one?" may not set off alarm bells quickly enough to prevent someone's identity from being stolen.

Administrative Safeguards

The HIPAA Security Rule defines administrative safeguards as "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[22] Much of what has been discussed in this information brief certainly is relevant in all three sections of the Security Rule, but a very important component of the Security Rule is the creation of policies and procedures.

Policies and procedures, while not the most adrenaline-inducing topic, provide safeguards by simply defining steps your health center has taken to prevent breaches and secure patient data. They should be updated as technology and processes change at your health center. In other words, they aren't final and unable to be changed once passed by your Board of Directors. When going through an audit, your policies are one of the ways your health center is graded on compliance. While this list is not meant to be exhaustive, from a security perspective, your policies and procedures should cover the following items:

- HIPAA Privacy/Security Officer
- Password policy
- Backup/Disaster Recovery (including testing backups)
- PHI Access policies (need-to-know)
    - Include BYOD and mobile device access policies
    - Include approved applications and cloud services
- Annual Risk Assessment
- Breach notifications in event of breach[23]

22 (45 CFR 164.304)

23 (45 CFR 164.400-414)

According to research conducted by the Journal of Mobile Technology in Medicine, 91% of healthcare professionals owned a mobile phone and 87% of those used it during clinical practice.[24] It's important to note that these devices were personal and not issued by their company. The surge of "bring your own device" (BYOD) has occurred in healthcare as it has other industries. Especially in the health center world where budgets are limited, it's even more likely that a medical provider would be using their personal device for work. The benefits include increased productivity, access to medical records on the go, increased patient engagement through mobile applications (apps) and more. The downside? IT, and even the health center as an organization, has no control over these devices and what data is stored on them. If a device stores PHI, the health center is required to have control over that data. Mobile Device Management (MDM) provides a layer of control to the health center, but many staff would not want their personal devices to be under the control of the health center. Balancing this can be tricky, but having a clear BYOD policy is a step in the right direction. Health centers should weigh the risks and benefits of a BYOD strategy and make the best decision for the health center.

Shadow IT is a way to refer to cloud services and applications that staff use within a network that may not be permitted by policy. Do you know what your employees have installed on their computers or mobile devices? Are they using any cloud services that are not permitted by your health center to store corporate data?

In most cases, these services are not malicious by design. However, data being transferred out of your network that contains PHI must be encrypted and stored in locations that are HIPAA/HITECH compliant. Consumer file sharing services (e.g., Dropbox), note-take services (e.g., Evernote) instant messaging services (e.g., HipChat, Yahoo! Messenger) and even email services (e.g., Gmail, Outlook.com) are all part of Shadow IT and are growing in popularity amongst staff, so they naturally bring it to work. Enforcing health center policy is required to secure data and prevent an accidental breach. It's easy to take for granted that cloud services are secure, but unfortunately breaches can (and do) happen to these services.[25,26,27,28] In the event a breach occurs in a cloud service that is in use by your staff, the only way to respond appropriately is to first know what services are in use and who is using them. More importantly, you should know which services are HIPAA/HITECH compliant and educate staff on appropriate use of cloud services.

24 http://www.journalmtm.com/2013/healthcare-professionals-use-of-mobile-phones-and-the-internet-in-clinical-practice-2/

25 https://blog.hipchat.com/2015/02/01/hipchat-security-notice-and-password-reset/

26 http://thenextweb.com/apps/2014/10/14/dropbox-passwords-leak-online-alleged-hack/

27 http://blog.evernote.com/blog/2013/03/02/security-notice-service-wide-password-reset/

28 http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users

I personally have been in different medical offices in several states along the East Coast and have been given the standard "Privacy Policy" form that states that I received a copy of the Privacy Policy. I always ask for a copy of the Privacy Policy when signing, and so far, each time I have been met with confusion when I request it. Staff didn't know where the policy statement was located, and they often did not even know what they were asking patients to sign. One office worker stated, "that paper you're signing is the privacy policy," when in reality it simply stated I received a copy of the privacy policy. Ironically, not only did the form that I was signing not have the policy statements written out on it, there were no copies to be found. Our health center patients deserve better. Staff should not only know where office forms are located, but also understand what they are asking patients to sign.

Your health center policies should be reviewed annually for compliance and any necessary updates or changes. Once your Board of Directors has approved policies, whether new or updated ones, make sure that all staff are aware of the policy and have easy access to review them. Team meetings or huddles are great places to review policies or discuss changes as they occur.

In addition to training on policies, staff should also be trained on the proper handling of paper records. While most health centers have now adopted and are using EHR systems, paper is still a big part of the medical community. Records faxed in from other offices, and patients sending completed forms back to providers all add up to a tremendous amount of paper. One single thing that can cut paper usage is properly implementing a digital fax server. Once this fax server is built into the daily workflow, one may find a significant decrease in paper usage and less clutter around desks. Digital faxes don't get misplaced and can easily be reviewed by providers. There are several different ways that a digital fax could be implemented, including hosting your own digital server or using a third-party service. It is required that the appropriate Business Associate Agreements are in place for any third-party vendor that moves or stores PHI, and that encryption is used in the transmission and storage of PHI.

There are certainly times, however, that require paper records to be used. In these cases, it's imperative that they are treated with the same level of security as a digital record would be. While it's not practical to have a password to open a physical folder of papers, locking records in cabinets or desks and keeping working areas clear of all medical records is vital. Custodial staff or contractors have no reason to access medical records, so office areas with printers and fax machines should also have locking cabinets or doors to prevent unauthorized access.

Encourage staff to find ways to reduce paper usage. Using laminated demographic forms and a dry-erase marker is a great way to reduce paper on repetitive forms. Using tablets or computers for registration forms is another great way. To encourage your patients, offer an incentive for filling out registration forms online prior to an appointment. This not only increases your efficiency at check-in, it reduces paper usage and prevents paper forms with PHI from being mishandled.

Health Center Response

While this brief has included a lot of information about technology, processes and, ironically, paper, the goal is to help you take actionable steps to help secure PHI in your health center. What is your health center's response to this topic? Are you confident in your security program? How can your health center take action to reduce your risk of being the victim of a data breach?

First, **your health center should have a named privacy/security officer as required by HIPAA**. This person's role is to lead the health center's security program by developing and implementing security policies and procedures. [29]

The Security Officer would be responsible for leading the team-based approach to security at the health center. As mentioned before, using a cross-functional team helps build support, awareness and cooperation with security policies across your organization. This team would assist in reviewing the security policies for improvements and assist in training peers throughout the health center.

Secondly, **your staff should be educated**. Health center staff at all levels play an important role in the security of your patients' data. It's important they not only understand the importance of security, but the repercussions of a data breach. Financial penalties are just one consequence of mishandling data; other costs include reputation damage in the community, and possibly even recreating data that was lost due to inadequate backups. According to the Verizon 2011 Data Breach Investigations Report, nearly 60% of small-to-medium businesses that suffered a data breach closed their doors within 6 months. Data breaches should be taken seriously and all staff educated on their role in preventing your health center from being the victim of one.

Training is a vital component of any security program. Educating staff on security policies, protecting patient data, and proper handling of medical records is essential. Bringing in consultants for training your security team in a "Train the Trainer" session can be valuable to your organization by empowering staff to train others. Training assistance and materials can also be found through your Primary Care Association (PCA), Health Center Controlled Network (HCCN) or national/Federal organizations such as NACHC.

Third, **your technical safeguards should be reviewed and updated** in accordance with industry best practices, some of which have been outlined here in this brief. It's clear that the human component is extremely important, and when combined with a strong technical security posture makes your network and data much more difficult to be compromised.

One of the changes in the HITECH Act is the added responsibility placed on Business Associates for HIPAA compliance. HHS has published a sample Business Associate Agreement (BAA)[30] with updated language, but be sure to consult with your legal counsel to confirm compliance with applicable state laws. This means updates are likely necessary to your existing BAAs. Every BAA must impose ten primary criteria on Business Associates:[31]

29 (45 CFR 164.308(a)(2))

30 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

31 http://healthcare.dmagazine.com/2013/06/24/hipaa-changes-how-to-revise-your-business-associate-agreements/

- What uses and disclosures are permitted;
- No other uses or disclosures unless specifically allowed by law;
- Business Associate must implement appropriate safeguards;
- Business Associate must report breaches and problems;
- Assist Covered Entity with granting individuals' access, amendment, and accounting of disclosures;
- Comply with other requirements applicable to Covered Entity;
- Business Associate must make books and records available to HHS;
- At termination, return or destroy all information;
- Ensure that subcontractors meet the same standards; and
- Authorize termination if the Business Associate breaches the BAA.

These changes are necessary, but fall short of a complete security plan. While BAAs are great documents that provide legal coverage, health centers must have a plan in place for handling data security and appropriately monitor for breaches through business associates. Taking proactive steps for data security, as opposed to simply reacting to a breach, is comparable to primary care for our health instead of waiting until symptoms are out of control.

Finally, combine all of the elements discussed into a strong security plan that is documented in policies and procedures. The security plan can be a part of the risk management plan that your health center likely has in place already. By including the technical aspects of firewalls, BDR, password policies and the procedural aspects for handling paper records, etc., a well-documented security plan helps protect data and meet critical compliance requirements. Your security plan should be reviewed regularly and updated as technology and your health center change.

The appendices contain a resource list of helpful content referenced in this brief as well as checklists that can be used to review your environment and for working with IT vendors to implement necessary technical safeguards for your health center.

APPENDIX

Steps to Preventing Data Breach

1. Name a privacy/security officer. ☐
2. Appoint a security team responsible for executing the health center security program. ☐
3. Select trusted IT partner as an advisor for security program and technical safeguards. ☐
4. Create a documented security program. ☐
5. Ensure health center data is *physically* secure. ☐
6. Name a person responsible for staying *current* with the latest security threats/trends and *advising* health center management accordingly. ☐
7. Ensure health center requires strong passwords. (if possible, with some form of multifactor authentication) ☐
8. Ensure health center has a reliable and tested backup in place. (including corresponding policies in place) ☐
9. Ensure health center has an enterprise-grade firewall with IPS/IDS functionality that is *installed, configured,* and *monitored.* ☐
10. Train staff regularly on how to *protect* PHI and why it's important. ☐
11. Conduct an annual independent *audit* of our *systems, processes* and *policies* that involve PHI. ☐

Questions to Ask your Trusted IT Partner

	Yes	No
Is our health center BDR system adequate? (If not, what provides the best solution given our needs, budget and regulatory requirements?)	☐	☐
Does our firewall include IPS/IDS functionality? If so, is it properly configured and monitored?	☐	☐
Is our SPAM filter providing adequate protection from malicious emails?	☐	☐
Does our health center meet HITECH requirements for encryption of data containing PHI? (What steps can be taken to increase security beyond the baseline requirements?)	☐	☐
Are we using an encrypted VPN for remote access and is it utilizing a trusted SSL (secure socket layer) certificate?		
Is our EHR database encrypted? If not, do we have safeguards in place to render the data unreadable in accordance with 45 CFR 164.304?		
Should our health center consider other security solutions besides AV and firewall?	☐	☐
Are the cloud services in use by our staff (known or unknown) HIPAA/HITECH compliant? (If not, what services should we consider, if any?)	☐	☐
Should our health center implement multi-factor authentication for additional security?	☐	☐
Our health center has a security team whose purpose is to execute our security plan. Could your organization provide an ad hoc member as an advisor to review policies and to provide feedback and training?	☐	☐

Resource List

HealthIT-specific Resources

ONC Guide to Privacy/Security - **http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf**

Guidance for Data Encryption - **http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html**

Sample Business Associate Agreement - **http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html**

Security Risk Assessment Tool - **http://www.healthit.gov/providers-professionals/security-risk-assessment-tool**

ONC Privacy and Security - **http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information**

OCR Health Information Privacy - **http://www.hhs.gov/ocr/privacy/index.html**

NIST Encryption Definitions - **http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf**

Security Reading

Brian Krebs – **www.krebsonsecurity.com**

Security Week – **www.securityweek.com**

DarkReading – **www.darkreading.com**

NH-ISAC – **www.nhisac.org**

Security Bloggers Network – **www.securitybloggersnetwork.com**