WHITEPAPER

UNDERSTANDING

HIPAA COMPLIANCE

5 Most Overlooked Aspects of HIPAA Compliance

by Theresa Sheppard, RDA

INTRODUCTION

HIPAA Compliance

Technological advances have given healthcare professionals the ability to interact efficiently with other providers, insurance companies, and patients. These advances allow patients to receive better care overall. However, along with this progress comes patient concern as to the proper safeguarding of their information. In 1996 The Health Insurance Portability and Accountability Act (HIPAA) was designed to protect the rights of individual's healthcare information, and protect patient safety.

Healthcare professionals know it is important to protect the privacy of their patients, but the issue can become complex when determining how to protect specific types of information, and understanding how to abide by security regulations, including the creation of written policies, and procedures.

Here are five often overlooked areas in which you have direct control over your level of security. Examining these are vital to reaching maximum HIPAA compliance.

Backup

Encryption

Email

File Sync

Access

1 Regular Backups of Patient Data

Backing up data can be a relatively simple task accomplished through a consistent, regularly administered backup schedule. Restoring critical data is something that nobody hopes to face, but everone must prepare for. It is essential to restrict access to backup data, both to protect the patient, and meet HIPAA stipulations.

Many practices backup their data in an unencrypted format, and may move devices between locations. How is that thumb drive or portable disc being safeguarded? Other offices may start their backup process, and then leave before the backup completes. Is the integrity of these backup jobs that are left to complete on their own being verified? Can you confirm that the data has been saved properly? Are you testing the restorability of these backup jobs regularly? If you allow an unencrypted portable drive to stay in the office, unchecked, and untested, your organization is putting itself at a high risk of a security breach. These weaknesses are simple to fix and should be remedied immediately.

2 Encryption

There are 18 unique identifiers that are associated with every patient. If any of these identifiers are accessible, the data must be encrypted or scrambled so that the data is impossible to identify. HIPAA
states that specific security measures must be documented if it is considered reasonable and appropriate to do so.

Even though the question of whether or not a process is “reasonable and appropriate” seems as though it should be self-explanatory, many are confused by this broad statement. Just remember that “reasonable and appropriate “ is determined by the HHS & OCR, not the individual practice. It is your responsibility to implement the law. So stay on the safe side - encrypt everything.

3 Emailing of Patient Information

HIPAA recommends that email communications be safeguarded and tamper-proof. Many people do not realize that typical email engines such as Gmail, Outlook, and Yahoo are not encrypted. The path that email data takes from one office to the next is not a straightforward one. It takes numerous routes, passing through multiple servers before the transmission is completed. Most of the time, these “pass-through” servers are not secure.

Email is extremely useful for distributing information quickly, but we must be careful not to substitute convenience for security. A simple step to protecting emails containing private information is to make sure your outbound email is encrypted. Several companies can work with your existing email provider to offer this ability.

If your office is in the practice of sending digital x-rays to specialty offices, it is imperative that the e-mail is de-identified. This means no personal patient information can be attached with that x-ray image. If something is attached to an x-ray that can identify a patient by means of an ID number, name, date of birth and even initials, then you are in violation.

4 Use of File-Sync Services

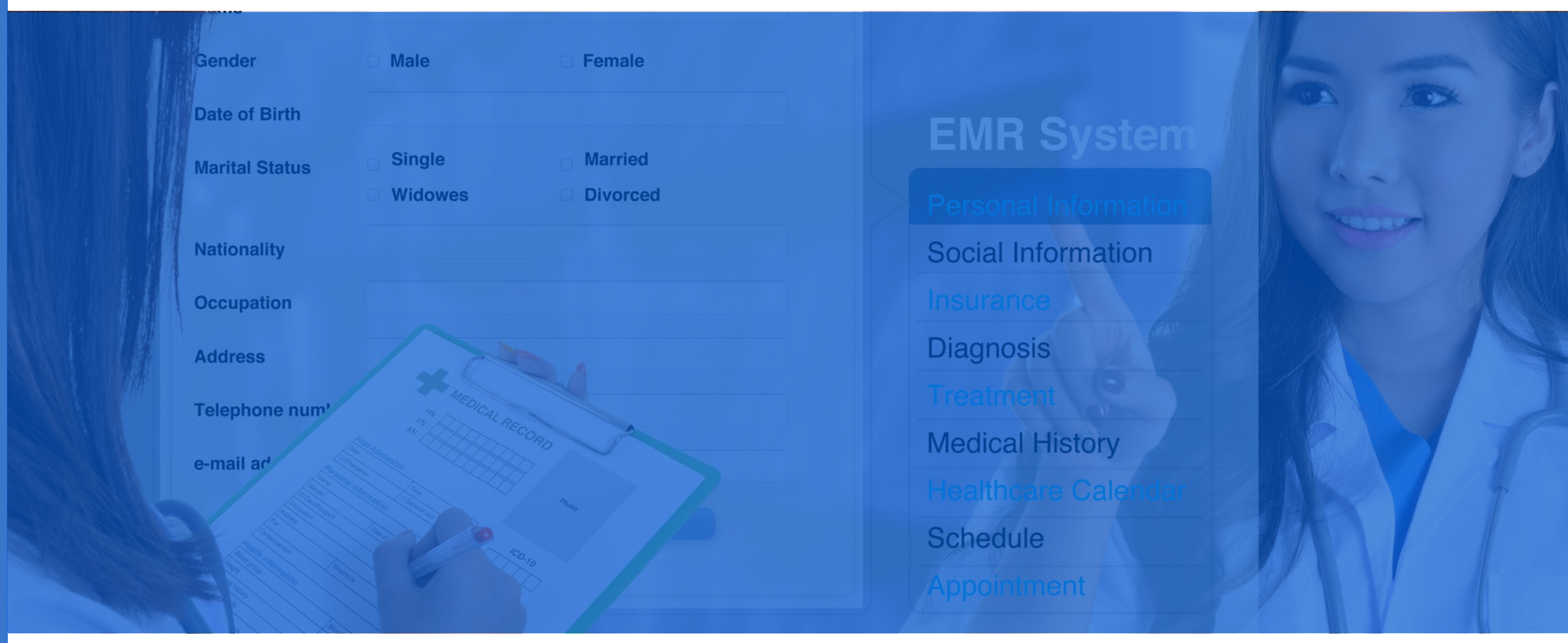
Commonly used file-sync services such as Dropbox offer the ability to access data seamlessly from multiple locations. For those “instantaneous, on-the-go, sleep with my phone in hand” type of people, these tools have become indispensable. While convenient, using these services as an extension of your own storage may not be HIPAA compliant. While some documents may be acceptable, it is not an option for any documents that contain patient information.

5 Information Access

Compliance can be a daunting task, and practices should consider working with a HIPAA professional who can assist them with reaching a maximum level of compliance. While 100% compliance is not typical, healthcare professionals need to strive to reach this goal to the best of their ability.

Auditors will be looking for proof that you have taken extraordinary steps to protect patient privacy, and your office data.

Visible, demonstrable evidence (VDE) is making sure you have written policies and procedures in place, have trained your team, and that you have taken precautions in logging information of the employees that have access to patient information. Example: Securing patient charts at night, and making sure that they are not visible to everyone. If electronic charts are used, it is a good idea to keep them covered while sitting at a desk during the day. If you label charts, be cautious and perceptive of how you are labeling them and with what data. Complete any document shredding before leaving at night.



Conclusion

Not only are breaches devastating to the patient, but they can also be financially disastrous to a practice. It can create a massive amount of work to be done once a security breach has occurred. Patients will need to be notified in writing. It is their right to be informed that the breach has transpired. Next, you will be required to contact the Health and Human Services website, and possibly your local media to report the breach. Once this has happened, you will join over 1,100 practices also listed on that site. This is not the type of publicity that any organization wants!

Learning about the requirements to achieve HIPAA compliance serves to help your organization secure patient healthcare information, develop the policies and procedures surrounding data access, and protect yourself in the event that you should experience loss or a breach of data.

Theresa Sheppard,
RDA specializes in Risk Management, Insurance Solutions, and HIPAA Compliance
www.TheresaSheppard.com

References
U.S. Department of Health and Human Services (2015) Health Information Privacy
http://www.hhs.gov/ocr/privacy/
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

ABOUT NOVABACKUP

NovaBACKUP Corporation specializes in ultimate data protection for Managed Service Providers and professional offices with unmatched support.

For more than a decade, we have been committed to providing all-inclusive and powerful cloud-based data protection to thousands of MSPs and professional offices around the globe.

We are industry leaders in Backup and Disaster Recovery, with vast experience in helping specialized industries reach the strictest data protection goals. Our job is to make data protection as simple and reliable for you as possible. From initial contact to ongoing operations, our backup experts will be there to support you. We take a people-first approach to backup. That means that you can count on us to provide you with the support you need to resolve your data protection concerns. For a complimentary evaluation of your backup environment, speak with one of our data protection experts.

Schedule a call with one of our backup experts today!

Our Service Promise

We promise to treat the protection and safety of your data like we do our own. Our job it to make data protection as simple and reliable as possible. You can count on us to provide professional, knowledgeable support that meets your data protection needs. Feel free to reach out to our team if you need assistance with your backup and recovery needs.

NovaBACKUP
29209 Canwood Street
Agoura Hills, California
91301

Tel.: (805) 579-6700
Fax: (805) 579-6710

M-F 9am-5pm PT

Email: msp@novabackup.com
www.novabackup.com