PRMS®
the psychiatrists' program®

CYBERSECURITY RESOURCES

INTRODUCTION

If you engage in online activity – whether it's emailing, perusing social media, surfing the web, or downloading an app – you are susceptible to a cyberattack. While such an event would be a problem for anyone, an attack on a physician's practice can be devastating, causing the loss of data, affecting patient care, and possibly subjecting the physician to actions under state and federal law. To assist you in protecting you and your practice from a cyberattack, we've put together this compendium of resources compiled from our previous writings, tips from governmental sources, and links to additional information from professional and governmental organizations. We hope you find it useful.

CYBERATTACK PREVENTION AND RECOVERY

Prevention Tips:

- Backup your data and keep the backups offline.
- Practice good cyber hygiene; whitelist apps (have network administrators determine what applications may be run on a computer or network rather than individual users), limit privilege, and use multifactor authentication.
- Update and patch systems.
- Make sure your security solutions are up to date. Do not use unsupported software.
- Change passwords every 60-90 days.
- Pay attention to cyberattack events and apply lessons learned.
- Be wary of emails containing unsolicited attachments, even from people you know. Cyber actors can “spoof” an email address, making it look like the message came from a trusted associate.
- Turn off the email option to automatically download attachments. To simplify the process of reading email, many programs offer the feature to automatically download attachments.
- Consider creating separate accounts on your computer. Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need “administrator” privileges to infect a computer.
- During the COVID-19 Pandemic:
    - » Be wary of emails with coronavirus in the subject line, unless it is from a known sender
    - » Consider ignoring coronavirus emails from unknown senders and seeking information directly from the CDC website or WHO website.
    - » Be aware that there is a large amount of “internet click bait” on websites offering information or fake articles about the coronavirus.
    - » Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
    - » Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
    - » Verify a charity’s authenticity before making donations. Review the Federal Trade Commission’s page on Charity Scams for more information.

Recovery Tips:

- Contact your malpractice carrier if protected health information may have been breached.
- Work with an experienced advisor to help recover from a cyberattack.
- Isolate the infected systems and phase your return to operations
- Review the connections of any business relationships that touch your network.
- Review and exercise your incident response plan.

Sources (and for additional information):

- AMA - Working From Home During the COVID-19 Pandemic - What Physicians Need to Know
- CISA – Avoiding Social Engineering and Phishing Attacks
- CISA - Defending Against COVID-19 Cyber Scams
- CISA – Using Caution with Email Attachments
- CISA Insights – Ransomware Outbreak
- FBI Flash Alert - COVID-19 Email Phishing Against US Healthcare Providers

HHS RESOLUTION AGREEMENTS – CYBERSECURITY

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcement of HIPAA Privacy, Security, and Breach Notification Rules. Following notice of investigation by OCR for a suspected violation, covered entities may elect to enter into a resolution agreement with OCR which then halts further investigation. These agreements generally consist of a corrective action plan and ongoing reporting to HHS, generally for a period of three years. A resolution agreement may also include a monetary payment.

The following are a selection of Resolution Agreements stemming from violations of the HIPAA Security Rule.

Noncompliance with HIPAA Rules Results in Business Associate Breach (September 2020):
A clinic agreed to a $1,500,000 settlement amount and corrective action plan after a hacker used a vendor's credentials to steal and post a database of the clinic's patient records online for sale. The hacker demanded money from the clinic in return for a complete copy of the database. OCR's investigation found longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.
Read the Press Release and Resolution Agreement.

Small Health Care Provider Fails to Implement Multiple HIPAA Security Rule Requirements (July 2020):
A small health center agreed to a $25,000 settlement and corrective action plan after impermissibly disclosing the ePHI of 1,263 patients to an unknown email account. OCR's investigation found that the hospital failed to conduct any risk analyses, failed to implement any HIPAA Security Rule policies and procedures, and neglected to provide workforce members with security awareness training until 2016.
Read the Press Release and Resolution Agreement.

Importance of BAA as a Cybersecurity Tool (March 2020):
A physician practice agreed to a $100,000 settlement and corrective action plan after the practice reported that its electronic health record vendor was blocking access to patients' ePHI until the practice paid $50,000. OCR's found that the practice had permitted this vendor to receive ePHI at least since 2013 without obtaining satisfactory assurances (a business associate agreement) that the EHR company would appropriately safeguard and return ePHI.
Read the Press Release and Resolution Agreement.

Failing to terminate former employee's access to electronic protected health information (December 2018):
A hospital agreed to a $111,400 settlement amount and a corrective action plan after OCR's investigation found that a former employee continued to have remote access to the hospital's web-based scheduling calendar, which contained patients' electronic protected health information (ePHI), after separation of employment.
Read the Press Release and Resolution Agreement.

Importance of Safeguards When Using Internet Applications (June 2015):
A physician practice agreed to a $100,000 settlement and corrective action plan after OCR's investigation found that the physician practice was posting clinical and surgical appointments for their patients on an Internet-based calendar that was publicly accessible.
Read the Press Release and Resolution Agreement.

Settlement Underscores the Vulnerability of Unpatched and Unsupported Software (December 2014):
A mental health facility agreed to a $150,000 settlement and corrective action plan after reporting a breach of unsecured electronic protected health information (ePHI) affecting 2,743 patients due to malware. OCR found the security incident was the direct result of the facility failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.
Read the Press Release and Resolution Agreement.

CYBERSECURITY POSTS – LINKEDIN

The following is a selection of LinkedIn posts by PRMS staff alerting physicians to cybersecurity risks and sharing suggestions and resources for avoiding those risks.

Another Ransomware Attack – Lessons Learned

LinkedIn Post 3/28/16
Donna Vanderpool, MBA, JD
Director of Risk Management, PRMS

Earlier this month I commented on a Los Angeles hospital's computer system that was taken over by hackers, and the criminals demanded a ransom payment in bitcoin to release the electronic medical records. The hospital ended up paying the ransom in 40 bitcoins (approximately $17,000), as demanded by the criminals. In that post I shared some technical advice from the Office of Civil Rights and the FBI to combat

the risk of having your electronic records held for ransom.

There has been another news story about a ransomware attack, this time involving a hospital in Kentucky. At least two things are noteworthy about this recent attack:

1. The hospital regained control of its records – without paying the bitcoin ransom
2. The virus was sent in a malicious email to an employee

The second point triggered what my IT team always says: viruses cannot get in themselves – **they have to be let in by employees.** So I wanted to remind folks of the simpler, less technical advice that may get forgotten:

- Never open an attachment unless you know what it is, and you trust the sender.
- Never click on a link in an email message unless you know where it points, and you trust the sender.
- Never install software without confirming with IT that it's OK to do so.

Unsecured Email and HIPAA

LinkedIn Post 6/14/16
Justin Pope, JD
Risk Manager, PRMS

Technically, HIPAA's Security Rule does not require encryption. Under the Security Rule, encryption is an "addressable" implementation specification. However, "addressable" does not mean optional; it means a covered entity must first make an assessment and document whether encryption would be appropriate, and then encrypt, implement an alternative security measure accomplishing the same purpose, or refrain from encrypting only if it would be unreasonable or inappropriate to encrypt. Keep in mind, when HIPAA was written over a decade ago, encryption software wasn't as affordable and readily available as it is now.

In commentary prior to the Omnibus Rule, OCR published the following:

"We clarify that covered entities are permitted to send individuals' unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the ''duty to warn'' individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual." 78 Fed. Reg. 5634 (January 25, 2013)

As it currently stands, unencrypted email may currently be used if the patient agrees to its use and is notified in advance. Given today's plethora of encryption options, OCR has been fairly vocal about the importance of encryption, especially in the context of laptops and portable devices containing protected health information. OCR continues to reach multimillion-dollar settlements with covered entities for improper disclosure of patient information by way of unencrypted portable devices.

For your use, we have made our "Sample Email Consent and Guide to Email Use" available at https://www.prms.com/services/risk-management/email-consent-and-guide-to-use/.

Medical Records Held for Ransom: It Could Happen to You

LinkedIn Post 7/13/16
Donna Vanderpool, MBA, JD
Director of Risk Management, PRMS

In prior posts earlier this year, I had a preliminary discussion on medical records being held for ransom and lessons learned. Recently the Office for Civil Rights (OCR) provided guidance on this topic. As the enforcement agency for HIPAA's Privacy and Security Rules, OCR provides very specific advice that covered entities are required to follow.

Here's what I want everyone to be aware of:

1. **Ransomware attacks are happening all the time.** OCR's guidance states "on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015)." While these statistics are not limited to the healthcare industry, it has been noted that electronic healthcare information is particularly vulnerable, as well as valuable.

2. **Don't think it can't happen to your small practice.** A few years back, a small surgical practice in Illinois was quite surprised to learn that its server with EHRs had been encrypted, and a ransom was demanded for the password

3. **Backing up your data is crucial.** Your ability to recover data from backups is key to recovering from a ransomware attack. The advice is to consider maintaining backups offline and unavailable from networks, as ransomware can have the ability to lock cloud-based backups.

4. **You need a contingency plan**, including disaster recovery planning, emergency operations planning, etc.

5. **Ransomware attacks usually result in a breach of protected information**, which then triggers breach notification requirements. The exception may be a device that is encrypted and off at the time of the attack. Remember that HIPAA's breach notification requirements only apply to "unsecured PHI." If the information is encrypted pursuant to HIPAA's standards (see prior post), then it is not "unsecured" so there is no breach and no reporting required. OCR gives these two examples:

   If a laptop encrypted with a full disk encryption solution in a manner consistent with HHS guidance is properly shut down and powered off and then lost or stolen, the data on the laptop would be unreadable, unusable, and indecipherable…Because the PHI on the laptop is not 'unsecured PHI", there is no breach notification required.

   However, if the laptop is powered on and in use by a user who performs an action (clicks on a link to a malicious website, opens an attachment from a phishing email, etc.) that infects the laptop with ransomware, there could be a breach of PHI. If full disk encryption is the only encryption solution in use to protect the PHI and if the ransomware accesses the file containing the PHI, the file containing the PHI will be transparently decrypted by the full disk encryption solution and access permitted with the same access levels granted to the user. Because the file with PHI was decrypted and thus 'unsecured PHI,' breach is presumed and the breach notification requirements must be complied with.

6. **Staff training is essential.** Staff should be educated on how to detect ransomware. In addition to points more relevant for IT personnel, the guidance gives a few suggestions for employees to detect ransomware, including

- A user's realization that a link was clicked on, an attachment was opened, or a website was visited that may have been malicious. and
- An inability to access certain files as the ransomware encrypts, deletes and re-names and/or re-locates data.

Staff training is something within all of our control. Don't forget this simple, yet effective advice from my earlier post - since malicious software has to be let in to your system:

- Never open an email attachment unless you know what it is, and you trust the sender
- Never click on a link in an email message unless you know where it points, and you trust the sender
- Never install software without confirming with IT that it is OK to do so

The guidance provides much more information, including specific technical requirements. The guidance is short, but packed with good advice, and should be read by all with electronic patient information.
Finally, if you are insured through PRMS, don't forget that you have access to eRiskHub with various online resources to assist you in keeping your patients' information secure, including the ability to submit questions to the experts.

More HIPAA Updates

LinkedIn Post 7/25/16
Donna Vanderpool, MBA, JD
Director of Risk Management, PRMS

There has been a flurry of enforcement activity that everyone should be aware of. During the past month, the following three resolution agreements have been made public:

1. The University of Mississippi Medical Center entered into a resolution agreement, agreeing to pay a $2.75 million. OCR found that the medical center was aware of risks and vulnerabilities to its systems as far back as 2005, yet no significant risk management activity occurred until after the breach. The breach involved a password-protected laptop that was stolen from the ICU. OCR's investigation revealed that ePHI stored on a network drive was vulnerable to unauthorized access via a wireless network because users could access an active directory containing the ePHI of an estimated 10,000 patients. According to OCR, the medical center failed to:

- Implement policies and procedures to prevent, detect, contain, and correct security violations;
- Implement physical safeguards to restrict access to authorized users;
- Assign a unique user name and/or number to identify and track user identity in systems with ePHI; and
- Notify individuals whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

2. Oregon Health & Science University entered into a resolution agreement, agreeing to pay $2.7 million. OCR began its investigation after OHSU submitted multiple breach reports, including reports of unencrypted laptops and a thumb drive being stolen. OCR found many violations, including:

- Vulnerabilities identified in risk analyses that were not addressed – specifically lack of encryption;
- No policies and procedures to prevent, detect, contain, and correct security violations; and
- Lack of a business associate agreement with entity providing cloud storage of ePHI of more than 3,000 individuals.

3. Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), a business associate, entered into a resolution agreement, agreeing to pay $650,000. At issue was the theft of an unencrypted cell phone with ePHI of hundreds of nursing home residents. Violations found by OCR included:

- No policies covering the removal of mobile devices with ePHI from the facility;
- No policies covering what to do in the event of a breach;
- No risk analysis had been performed; and
- There was no risk management plan

For those of you insured with PRMS, we hope you have heard about the enhancements to our policy. HIPAA-related enhancements include:

- HIPAA Defense Coverage – New Separate Limit: Up to $50,000 for defense, fines and penalties (where allowed by law) arising out of any investigations or civil proceedings concerning actual or potential HIPAA violations.
- Date Breach Expenses Coverage – New Higher Limit: Up to $30,000 to manage the crisis of a breach, including credit monitoring and professional services needed to notify patients.
- The enhanced policy is being rolled out state-by-state, as it is approved by the state insurance departments. For more information on other policy enhancements and a listing of states where the enhancements have been approved, click here.

Get Clarification about Encryption

LinkedIn Post 2/1/16
Donna Vanderpool, MBA, JD
Director of Risk Management, PRMS

Background:
Under HIPAA's Breach Notification Rule, individuals must be notified if their protected health information (PHI), which includes demographic and medical information, has been improperly accessed or disclosed. However, if the information is encrypted consistent the National Institute of Standards and Technology (NIST) guidance, using the Advanced Encryption Standard (AES), the Rule has a "safe harbor" under which no notification is required.

The FTC Case:
A dental practice management software vendor recently paid $250,000 to settle a FTC investigation alleging it misled customers about its encryption of patient data. According to the FTC complaint, the company marketed its software to dentists nationwide with deceptive claims that the software provided industry-standard encryption of sensitive patient information and, in doing so, claimed that patient data would be protected as required by HIPAA. The FTC cited numerous statements from the vendor's promotional materials, including the following:

"The database also provides new encryption capabilities that can help keep patient records safe and secure. And of course, encryption plays a key role in your efforts to stay compliant with HIPAA security standards."

In fact, the vendor's encryption did not meet the AES, and was described as less secure and more vulnerable than other widely used encryption algorithms. The FTC alleged that the vendor was aware of the NIST guidance recommending AES encryption to help providers meet their regulatory obligation to protect data, and the requirement of patient notification of breaches unless the data was encrypted consistent with the

NIST guidance. The vendor was charged with two counts of deceptive claims of encryption, related to the industry standard and regulatory obligations.

What This Means for Healthcare Professionals:
Providers need to check with vendors providing encryption to confirm that the encryption technology is consistent with the NIST standards. This should be addressed in contracts with vendors.

Cyberattacks on Healthcare Organizations

LinkedIn Post 5/13/17
Donna Vanderpool, MBA, JD
Director of Risk Management, PRMS

From OCR's Privacy and Security Listservs –

From HHS (5/12/17):
HHS is aware of a significant cyber security issue in the UK and other international locations affecting hospitals and healthcare information systems. We are also aware that there is evidence of this attack occurring inside the United States. We are working with our partners across government and in the private sector to develop a better understanding of the threat and to provide additional information on measures to protect your systems. We advise that you continue to exercise cyber security best practices – particularly with respect to email.

From Homeland Security (5/13/17):
US-CERT has received multiple reports of WannaCry ransomware infections in several countries around the world. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Individuals and organizations are discouraged from paying the ransom, as this does not guarantee access will be restored.

Ransomware spreads easily when it encounters unpatched or outdated software. The WannaCry ransomware may be exploiting a vulnerability in Server Message Block 1.0 (SMBv1). For information on how to mitigate this vulnerability, review the US-CERT article on Microsoft SMBv1 Vulnerability and the Microsoft Security Bulletin MS17-010. Users and administrators are encouraged to review the US-CERT Alert TA16-091A to learn how to best protect against ransomware. Please report any ransomware incidents to the Internet Crime Complaint Center (IC3).

More from HHS (5/13/17):
How can I help protect myself from email-based ransomware attacks?

Ransomware can be delivered via email by attachments or links within the email. Attachments in emails can include documents, zip files, and executable applications. Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system. To help protect yourself, be aware of the following:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.
- Don't click on links in emails if you weren't expecting them – the attacker could camouflage a malicious link to make it look like it is for your bank, for example.
- Keep your computer and antivirus up to date – this adds another layer of defense that could stop the malware.

How can I help protect myself from open RDP ransomware attacks?

Recently, attackers have been scanning the Internet for Remote Desktop Protocol (RDP) servers open to the Internet. Once connected, an attacker can try to guess passwords for users on the system, or look for backdoors giving them access. Once in, it is just like they are logged onto the system from a monitor and keyboard. To help protect yourself, be aware of the following:

- If you do not need RDP, disable the service on the computer. There are several ways of doing this based on which version of Microsoft Windows you are using.
- If RDP is needed, only allow network access where needed. Block other network connections using Access Control Lists or firewalls, and especially from any address on the Internet.
- To find which version of Microsoft you are using: https://support.microsoft.com/en-us/help/13443/windows-which-operating-system

PRMS CYBERSECURITY ALERTS

Special alerts have also been provided to PRMS clients via email.

May 2014:

An Important Alert from PRMS Regarding Windows XP Users

Dear Doctor:

Please be advised that Microsoft will no longer maintain Windows XP as of April 8, 2014.* Microsoft will no longer provide security updates, fix bugs, or offer call center support for Windows XP users. What does this mean for you? If you are still using Windows XP in your practice – 28% of all computer users continue to do so – the security of your Protected Health Information (PHI) may be in danger, potentially resulting in liability. In order to secure your PHI, minimize your risk, remain HIPAA-compliant, and meet your professional obligation to keep patient information secure, we suggest you to do the following:

- Review HIPAA! It is important to understand what capabilities are required of your operating system by law. For more information on HIPAA's requirements, contact your risk managers.
- Do the research. Before utilizing any new program that will manage PHI, assess its strengths, weaknesses, and whether it will be the right fit for your practice.
- Upgrade your operating systems to ensure that they are up to date and compliant with HIPAA. Windows XP is now being phased out. If you continue to use this operating system, you will open yourself up to elevated risk and exposure over the coming months.
- For those devices that have yet to be updated, create an implementation schedule and stick to it! It has been reported that Microsoft will continue to maintain the XP malware engine for another year until July 14, 2015. However, they have already had their final public release of security patches.

January 2018:

We wanted to share this set of easy-to-implement tips and reminders for keeping electronic information secure from the HHS Office for Civil Rights.

December 2017 OCR Cybersecurity Newsletter: Cybersecurity While on Holiday

Cybersecurity threats don't take a holiday when you do. If you're headed out of the office for an extended absence, be aware that cyber threats continue. In fact, some threats may be at an increased risk if you're outside of the familiar, protected environment of the office or home.

When traveling, you must take extra precautions to safeguard personal and sensitive information you carry inside your phone, laptop, and tablet. You can protect yourself and others by leaving any equipment that you won't need behind (just make sure it's secure where you leave it). If you do need to take your work-issued computer and personal internet-connected devices, be sure to add these to-dos to your travel preparedness list.

Bring and Use Your Own Power Adapters and Cords

It's never safe to charge your devices using anything other than your own power adapters. Cyber thieves may install malware onto hotel lamps, airport kiosks and other public USB charging stations. If you absolutely must charge your device on the road, and you don't have access to your charger/adapter, power down your device before you connect it into any airport chair or public USB charging station.

Back Up Your Electronic Files

Before you leave, back up your contacts, photos, videos and other mobile device data with another device or cloud service. And make sure your back-ups are encrypted and secure!

Install Security Updates and Patches

Be sure to patch and update operating systems and software (including mobile device apps). This should be a regular practice, but it is particularly important if you will be unable to update while traveling. Updates and patches can fix security flaws and enable security software to detect and prevent new threats.

Create New Passwords and Change Passwords

Change passwords you will use while traveling, and add multi-factor authentication, if possible. Don't skimp on password creation either—a numerical sequence is not ideal. Passwords should be at least 10 characters or longer with a combination of letters, numbers, and symbols. Consider using a passphrase – a combination of words that are easy to remember, such as "Mydogatemyhomeworkandgotindigestion". Once you're home, change your passwords again!

Lock Devices Down

Most smartphones, laptops, and tablets come equipped with security settings that will enable you to lock the device using a PIN or fingerprint ID. Do this on every available device. In the event you misplace or lose a device, this will be the first line of defense against a security breach.

Remove or Encrypt Sensitive Information on Mobile Devices If you do not need to access sensitive information while traveling, don't bring it. But if you need the information while you are traveling, make sure sensitive information is encrypted. For example, laptops should have full-disk encryption.

Turn Off WiFi Auto-Connect and Bluetooth

Go into your device's Settings feature, and disable the WiFi auto-connect option so that you manually connect when it is safe to do so. Similarly, disable Bluetooth connectivity. If left on, cyber thieves can connect to your device in a number of different and easy ways.

Avoid Public WiFi

Avoid connecting to any public WiFi network. You didn't connect to the free, open WiFi on the airplane, so continue that mindset on the ground. Using your mobile network (like 4G or LTE) is generally more secure than using a public wireless network.

Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Always log into your work networks through VPN, and only use sites that begin with "https://" when online shopping or banking.

Ensure Physical Security of Your Devices

NEVER let your devices leave your sight. If you cannot physically lock devices in your hotel room safe or other secure place, take them with you. There are no good hiding spots in your hotel room! Many breaches occur because a device was left unattended when an opportunistic thief struck. When traveling with laptops and tablets, the best protection is to carry them with you. It's never safe to pack your devices in your checked luggage.

Create Unique PINs

Don't use the same PIN for the hotel safe and a mobile device, especially one that you're storing in the hotel safe! Do you really want to make it that easy for a thief?

Use Geo-Location Cautiously

Most social media sites are happy to automatically share your location as you post photos and messages. This also tells thieves back home that you are away, which is a great time to break in. So, limit the information you post regarding your location at any point in time.

For HIPAA Covered Entities and Business Associates

The HIPAA Security Rule requires that covered entities and business associates conduct a risk analysis to identify risks and vulnerabilities and to mitigate identified threats and vulnerabilities. Risks to ePHI created, received, maintained, or transmitted on workplace owned equipment, and personal equipment if permitted, when workforce members travel must be included as part of a covered entity's or business associate's risk analysis and risk management process.

The HHS Office for Civil Rights (OCR) web site provides guidance on the HIPAA Security Rule as well as guidance on specific cybersecurity topics. We recommend you bookmark these pages so you can refer to them easily whenever you have a question or need some guidance.

Bon voyage! And safe cyber travels.

January 2019:
New Cybersecurity Resources

The Department of Health and Human Services (HHS) recently issued new cybersecurity resources to manage threats and protect patients, including resources for small healthcare organizations. The resources include:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients - Reviews five current threats (phishing attacks, ransomware attacks, loss/theft of equipment/data, insider, accidental or intentional data loss, and attacks against medical devices) and presents practices to mitigate those threats.
- Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
- Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations
- Resources and Templates

CYBERSECURITY RESOURCES

American Medical Association:

- Medical Cybersecurity - A Patient Safety Issue
- Working from Home During the COVID-19 Pandemic – What Physicians Need to Know

Cybersecurity & Infrastructure Security Agency:

- Avoiding Social Engineering and Phishing Attacks
- Defending Against COVID-19 Cyber Scams
- Ransomware Outbreak
- Using Caution with Email Attachments

Federal Bureau of Investigation:

- Flash Alert - COVID-19 Email Phishing Against US Healthcare Providers
- High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations

Health IT Security:

- 4 Sophisticated Phishing Campaigns Impacting the Healthcare Sector
- Healthcare Workers Uninformed About Cybersecurity Best Practices
- Payment Notification is Top Healthcare Phishing Attack Subject
- Ransomware Attack Impacts EHR of Rhode Island Provider

Office of the National Coordinator for Health Information Technology:

- HIPAA Security Training Games
- Security Risk Assessment Tool

Proofpoint:

- Healthcare Email Fraud Attack Attempts Jump 473% Over Two Years

U.S. Dept. of Health and Human Services:

- Cybersecurity Guidance Material
    - » Cybersecurity Checklist and Infographic
    - » Ransomware Guidance
    - » NIST Cybersecurity Framework
    - » OCR Cyber Awareness Newsletters
- Guidance on Cloud Computing
- Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- Guide to Storage Encryption for End User Devices
- Risk Assessment Guidance

PRMS®
the psychiatrists' program®

CONTACT

(800) 245-3333
PRMS.com
TheProgram@prms.com

MORE THAN AN **INSURANCE POLICY**