UB|MD
PHYSICIANS' GROUP

Compliance Alliance

U.B. Associates, Inc. First Quarter - 2016 Volume 10, Number 1

IN THIS ISSUE:

Cybersecurity & Ransomware

By: Lawrence C. DiGiulio, Chief Compliance Officer

Protecting our patients' personal health information from cyber-attacks is an important part of your job. Healthcare has the dubious distinction as the industry that has been most successfully cyber-attacked since 2010. The plethora of successful ransomware attacks against hospitals and their EHR systems has been in the news since the first reported attack against Hollywood Presbyterian Medical Center in February. Since then, hospitals in Texas, Tennessee, Kentucky, Ontario, and now MedStar in Maryland and DC, which includes Georgetown Medical Center, have all been successfully attacked.

A ransomware attack is a type of malware where a hacker gains access to an EHR or other computer system. The attack usually comes through a phishing scheme, gaining access to your computer via an email attachment or a web site you open, by masquerading as a trustworthy electronic communication to you. Once the attack is successful, the malware encrypts all the data on your computer and also attempts to compromise any other computers on the network that trust your computer, such as those running the EHR, and encrypts their data as well. After the hospital or healthcare provider's data is encrypted, it cannot be accessed by anybody but the extortionist until they send the malware an encryption key over the network to decrypt the data. This key is sent after a ransom has been paid, usually in untraceable Bitcoin. Hospitals attacked in the last month have been forced to initially divert patients to unaffected hospitals and then convert to paper back-up systems until the ransom is paid and the data is freed (if at all) by the extortionist or data is loaded from backup media.

Cybersecurity professionals are not the only or even the primary line of defense for these attacks. The extortionists use easy to deploy phishing emails. These emails contain attachments that contain the ransomware software that is only launched if one of our users clicks on the attachment. Another method is the extortionist will ask you to visit a web site for some seemingly work related reason. An example of this kind of email follows:

From: *Franklin, Serena*
Sent: *Wednesday, March 30, 2016 10:32 AM*
Subject: *Outlook Web*

Today Wednesday 30th March, 2016. we are upgrading our email system to Microsoft Outlook Web Access 2016. This service creates more space and easy access to email. Please update your account by clicking on the link below and fill information for activation.

Click for activation [I have deactivated this link]

Inability to complete the information will render your account inactive.

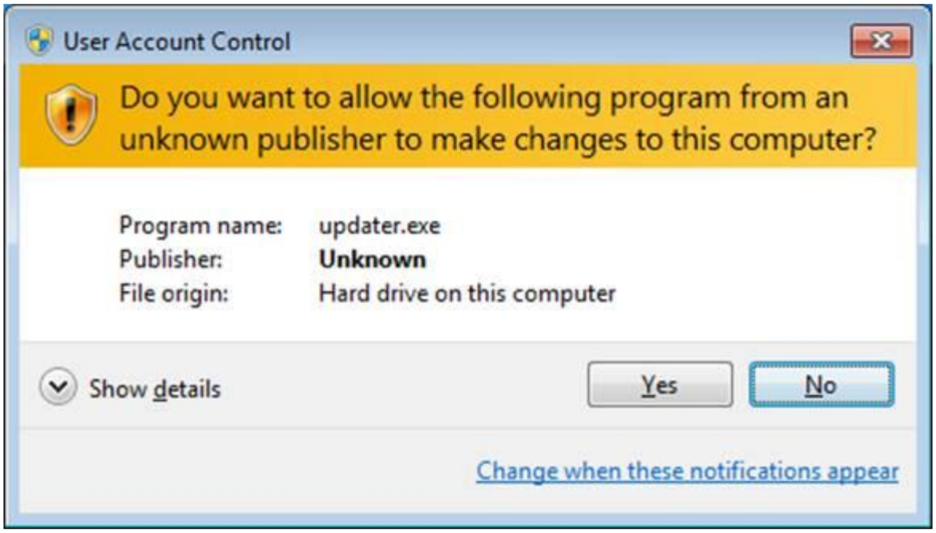
Thank you.

IT Admin Desk

This email was sent Wednesday from a UB email address that was compromised by a hacker outside of our organization. It highlights a clear threat to our patient's PHI.

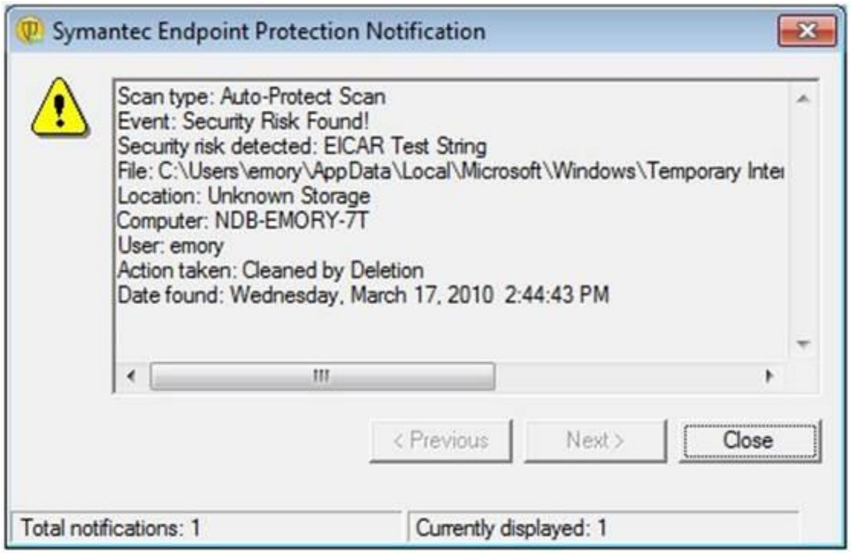
Attack methods are constantly changing which is one of the reasons antivirus protection is not foolproof. Recently, malware was found in Microsoft Word documents for the first time. It is very important that you do not click on attachments or follow a link unless you know the sender and you are expecting the attachment or link. If not, confirm with the sender that the sender has not been hacked and the attachment or link is valid. When possible, use shared network drives to exchange documents instead of Email.

To assist you in preventing ransomware and other malware attacks, there is active antivirus protection in place that is updated regularly. It is important that we pay attention to any warnings that our antivirus defenses provide us. Examples of warnings that we should not ignore follow:


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: updater.exe
Publisher: **Unknown**
File origin: Hard drive on this computer


Symantec Endpoint Protection Notification

```
Scan type: Auto-Protect Scan
Event: Security Risk Found!
Security risk detected: EICAR Test String
File: C:\Users\emory\AppData\Local\Microsoft\Windows\Temporary Inte
Location: Unknown Storage
Computer: NDB-EMORY-7T
User: emory
Action taken: Cleaned by Deletion
Date found: Wednesday, March 17, 2010  2:44:43 PM
```

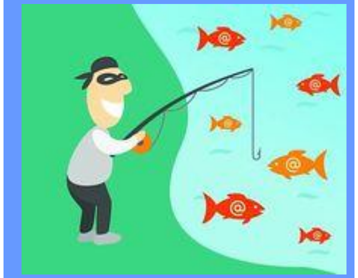
Total notifications: 1   Currently displayed: 1

If you receive one of these notices, do not continue to open the attachment and contact your practice plan IT Professional or the Office of Medical Computing.

It is your responsibility to keep our patients' protected health information safe -- in the physical world as well as the cyber world.

Since writing this article, the Office of Civil Rights, the agency charged with enforcing HIPAA, promulgated the following warning relevant to this topic:

- **Ransomware Attacks** – Hackers and ransomware tools are becoming more sophisticated. The main objective in using ransomware is to destroy backups of files and databases that contain electronic patient health information and to encrypt and lock up files and databases that contain ePHI in order to charge covered entities and business associates hundreds to thousands of dollars to unlock the data.



US-CERT and CCIRC recommend healthcare entities and business associates to take the following preventive measures to protect their computer networks from ransomware infections:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Data should be kept on a separate device, and backups should be stored offline.
- Maintain up-to-date anti-virus software.
- Keep operating system and software up-to-date with the latest patches.
- Do not follow unsolicited web links in emails.
- Use caution when opening email attachments.
- Follow safe practices when browsing the web.

The Federal Bureau of Investigation encourages healthcare entities and business associates not to pay the ransom, as this does not guarantee files will be released. Any instances of cyber fraud should be reported to the FBI.

Resources:
United States Computer Emergency Readiness Team (US-CERT): https://www.us-cert.gov/ - *(Ransomware remediation)*

Federal Bureau of Investigation (FBI): https://www.fbi.gov/scams-safety/fraud/internet_fraud - *(Report internet fraud)*

The United States Computer Emergency Readiness Team also put out a ransomware alert on March 31, 2016 with a listing of effective preventative measures:

https://www.us-cert.gov/ncas/alerts/TA16-091A

UB just issued this article to help protect against phishing attempts:

http://www.buffalo.edu/ubit/news/topics/safe-computing.host.html/content/shared/www/ubit/news/2016/top-five-phishing-signs.detail.html

As always, if you know of any compliance issues, have any compliance related questions, or suspect any fraud or abuse, please call our anonymous compliance hotline at (716) 888-4752, call us directly or email us. We have a strict non-retaliation policy that will be adhered to in all instances to protect any person who reports to the compliance department or their supervisor.

Coding Corner: Advanced Care Planning

By: Beverly Welshans, CHC, CPMA, CPC, CPCI, COC, CCSP, UBMD Director of Audit & Education

On October 30, 2015, the Centers for Medicare and Medicaid Services (CMS) released the final payment rules for Medicare reimbursement of physicians who consult with their patients on advance care planning. This separate payment system under the 2016 Physician Fee Schedule will impact the almost 55 million Medicare beneficiaries and their healthcare providers.

End-of-life care, also known as Advance Care Planning (ACP), enables patients to formulate advanced directives: a living will, the designation of a healthcare proxy, Medical Orders for Life-Sustaining Treatment (MOLST), and the preparation for hospice care, among others. Patients should start thinking about their healthcare options, and share such important decisions with their physicians and family before the need for hospitalization.

CMS has not specified any required documentation; however, these codes will be subject to audit. At a minimum, providers should document:

- *The necessity for the ACP services, such as: patient has an end stage chronic illness; will be undergoing an emergent or high risk procedure; has had a condition change that prompts the need for ACP, etc.*
- *The specific amount of time spent on the ACP service, with whom the conversation was held (patient and/or surrogate).*
- *That the patient was informed that the ACP service is voluntary.*

The CPT codes for these services are:

- 99497 – Advance care planning including the explanation and discussion of advance directives such as standard forms (with completion of such forms, when performed), by physician or other qualified health care professional; first 30 minutes, face-to-face with the patient, family member(s), and/or surrogate.
- 99498 + each additional 30 minutes.

Effective January 1, 2016, Medicare pays $86 for 30 minutes of ACP in a physician's office and will pay $80 for the same service in a hospital (CPT billing code 99497). In both settings, Medicare will pay up to $75 for 30 additional minutes of consultation (add-on CPT billing code 99498). Such counseling can take place during a senior's annual wellness visit or during a routine office visit and at various stages of health, always "at the discretion of the beneficiary."

In order to have the deductible and coinsurance waived for ACP when performed with an AWV, the ACP code(s) must be billed with modifier 33 (Preventive services). Both the ACP and AWV must be billed together on the same claim. Since payment for an AWV is limited to only once a year, the deductible and coinsurance for ACP billed with an AWV can only be waived once a year. There are no frequency limits for ACP billing, just for waiving of deductible and coinsurance. A deductible and coinsurance do apply when ACP is provided during other encounters. The service may not be performed during a global period or in the same month as TCM (Transitional Care Management) or CCM (Chronic Care Management).

CMS states that the services can be performed by a physician or "non-physician practitioner" within their scope of practice. This means physician, NP or PA. This differs slightly from the CPT description of being performed by a physician or "other qualified health professional". Reimbursement may vary by payer. Since ACP is a time-based service, it cannot billed when be performed by a resident.

Follow the link below to view the official CMS notification.

https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/MM9271.pdf

> *"Relativity applies to physics, not ethics."*
> *~ Albert Einstein*

Final 60-Day Rule

By: Sue Marasi, CHC, CPC-A, Compliance Administrator

Since the inception of the Affordable Care Act that requires Medicare Pats A & B health care providers to report and return overpayments to the appropriate party (i) "by the later of" 60 days after the overpayment was "identified", or (ii) the date the corresponding cost report is due, if applicable, there has been a lot of confusion among providers, lawyers, regulators and others regarding the definition of "identified", and the look-back period.

In response, in 2012, the Centers for Medicare & Medicaid Services (CMS) issued a Proposed Rule. Four years later, on February 12, 2016, CMS published a Final 60-Day Rule which clarifies the meaning of overpayment identification, the required look-back period for overpayment identification, and the methods for reporting and returning identified overpayments to CMS as follows:

__Meaning of "Identification":__ What it means to "identify" an overpayment was not defined in the original 60-Day Rule, so we were left to wonder if it meant when an allegation was made, when the allegation was verified as a billing error, or when the overpayment was quantified.

The final rule states that a person (ie: provider or staff) has identified an overpayment when the person has or should have, through the exercise of reasonable diligence, and through timely good faith investigation of credible information, determined that the person has received an overpayment, and quantified the amount of overpayment. Therefore, the 60-day clock does not start running until after the reasonable diligence period has concluded, which may take 6 months, at most, from the receipt of credible information, unless extraordinary circumstances exist such as a Stark Law violation. In total, then, it can be an 8 month period: a 6 month timely investigation, and 60 days to report and return the overpayment.

__Look-back Period:__ Overpayments must be reported only if a person identifies the overpayment within six years of the date that the overpayment was received. According to CMS, this is a more practical time frame (than the originally proposed 10 years) because it aligns with the False Claims Act statute of limitations, and providers generally retain records for six to seven years based on state and federal requirements. The six year look-back period will apply to any overpayments reported or repaid on or after March 13, 2016.

__How to Report & Return Overpayments:__ Providers must use an applicable claims adjustment, credit balance, self-reported refund, or other appropriate process established by the applicable Medicare contractor to satisfy the obligation to report and return overpayments.

This Rule is meant to support compliance with existing statutes, promote quality patient care, and protect Medicare from improper and fraudulent payments. Health care providers who fail to report and return an overpayment could face potential penalties including:

- False claims liability
- Civil monetary penalties
- Exclusion from federal health care programs

In conclusion, in order to avoid significant liability, all health care providers and their staff should use reasonable diligence to identify, report and repay any overpayments. Any information of a potential overpayment should be promptly evaluated for credibility, documented and followed up on accordingly.

Have a question or topic regarding compliance or coding that you would like to see covered in *Compliance Alliance*?

We are always looking for suggestions!

Please send them to Sue Marasi in the Compliance Office.
(You may remain anonymous if you wish.)

Training Update

By: Beverly Welshans, CHC, CPMA, CPC, CPCI, COC, CCSP, UBMD Director of Audit & Education

__Lunch 'n Learn__

The monthly 2016 UBMD Lunch 'n Lunch series commenced on April 19, 2016. These sessions are held once per month and cover a variety of topics related to compliance, coding and/or billing. Each session is credited with 1 CEU accepted by AAPC, AHIMA, MAB, PMI and a host of other sanctioning bodies.

They are held in the classroom (room 208) at 77 Goodell Street from 12:30 – 1:30. 2016 Dates are; April 19th, May 17th, June 14th, July 12th, August 16th, September 13th, October 11th, November 15th and December 13th . Please feel free to bring your lunch and join us. These are a great opportunity to learn and earn free CEUs.

UBMD ANONYMOUS COMPLIANCE HOTLINE

888-4752

We have a strict non-retaliation policy.

CONTACT US:

**UB Associates, Inc.
UB Downtown
Gateway Bldg.
77 Goodell St., Suite 320
Buffalo, NY 14203
Fax: 716-849-5620**

**Lawrence C. DiGiulio, Esq.
Chief Compliance Officer
Phone: 716-888-4705
E-mail:
larryd@buffalo.edu**

**Suzanne M. Marasi, Editor,
Compliance Administrator
Phone: 716- 888-4708
E-mail:
smmarasi@buffalo.edu**

**Beverly A. Welshans,
Director of Audit & Education
Phone: 716- 888-4702
E-mail:
welshans@buffalo.edu**

Answers to 2015 Fourth Quarter FWA Quiz:

1. Knowingly billing for services and/or supplies not provided is an example of: **a. fraud**
2. Billing for services that were not medically necessary is an example of: **c. abuse**
3. Being involved in fraud and/or abuse schemes exposes you and your practice to the possibility of penalties including, but not limited to monetary fines, repayment of claims, imprisonment, loss of provider license, and exclusion. **a. True**
4. Which of the following is/are important to preventing fraud and abuse? **d. All of the above**
5. Which statement(s) below is/are correct? **d. All of the above**

CODING ALL-STARS

What happens when our auditors Bev Welshans & Jess Wachowicz show up at the AAPC Coding Conference.....***together*?!**

THIS HAPPENS!!

Way to rock the conference ladies!

First Quarter 2016 Quiz

**** To submit your quiz answers, please go to**
https://smbsweb.med.buffalo.edu/ubmd/training.aspx
and select Training Module "2016 – 1st Quarter Newsletter"

****

1. Which of the following is true regarding ransomware attacks?
   a. The attack usually comes through a phishing scheme via an email attachment or website you open.
   b. Once successful, the malware encrypts all the data on your computer and attempts to compromise any other computers on the network that trust your computer.
   c. Once the data is encrypted, it cannot be accessed until a usually untraceable ransom has been paid to the extortionist.
   d. All of the above are true.
2. It is very important that you do not click on attachments or follow a link unless you know the sender and you are expecting the attachment or link,
   a. True
   b. False
3. CMS has not specified any required documentation for ACP services; therefore, the codes will not be subject to audit, and providers are not required to document the necessity for ACP services, amount of time spent on ACP services and with whom, or that the patient was informed the ACP service is voluntary.
   a. True
   b. False
4. To have the deductible and coinsurance waived for Advanced Care Planning when performed with an Annual Well Visit, the ACP Code(s) must be billed with modifier ______ (Preventive Services).
   a. 26
   b. 32
   c. 33
   d. 53
5. Health care providers who fail to report and return an overpayment could face potential penalties including:
   a. False claims liability
   b. Civil monetary penalities
   c. Exclusion from federal health care programs
   d. All of the above

****

PLEASE DO NOT EMAIL OR FAX YOUR ANSWERS

Answers must be submitted online at:

https://smbsweb.med.buffalo.edu/ubmd/training.aspx

Be sure to click on your correct practice plan to ensure proper credit!