VIVA HEALTH®

2019

The Vendor Vine

VIVA HEALTH, Inc. provides this newsletter as a resource to its contracted entities that meet the CMS definition of a first tier, downstream or related entity (FDR). This newsletter is published annually and will be available on our website at ***http://www.VivaHealth.com/FDR.***

We hope you find this newsletter helpful. We value your feedback and suggestions! If there are topics you would like for us to address in a future newsletter, please let us know. You can reach out to one of the contacts listed in the "Your VIVA HEALTH Contacts" box on the last page of this newsletter.

VIVA MEDICARE Earns High Marks From CMS

For 2020, VIVA MEDICARE earned **4½ out of 5 stars** from CMS on its Medicare quality performance. The score is based on 48 different quality measures that illustrate everything from customer service to how well the plan helps its members stay healthy. In addition, VIVA MEDICARE is one of the most highly rated plans in Alabama for a decade.

4½ STARS

Highest Star Rating for a plan in Alabama[1]

BEST INSURANCE COMPANIES U.S.News & WORLD REPORT MEDICARE ADVANTAGE ALABAMA 2020[2]

10 YEARS

One of the most highly rated plans in Alabama ***for a decade***[3]

We appreciate our FDRs' support in helping us achieve these excellent ratings!

[1] Every year, Medicare evaluates plans based on a 5-star rating system. The Star Rating referenced is for contract year 2020.
[2] https://health.usnews.com/medicare/viva-medicare-medicare-plans-in-alabama [3] Based on the 2011-2020 Medicare & You Handbooks for Alabama.

Viva Health's Annual Compliance And Offshore Attestation

FDRs are required to complete Viva Health's Annual Compliance and Offshore Attestation. This form is available on our website at ***https://www.VivaHealth.com/FDR.***

If you have not done so already, please go to our website to obtain the form, complete it, and return it to Viva Health by December 31, 2019. Please remember, the attestation must be completed by an authorized representative of your organization.

Impermissible Disclosure in Mailings

HIPAA covered entities and business associates have to constantly be on guard and take steps to reasonably help prevent and/or detect security incidents that can compromise personally identifiable information (PII) or protected health information (PHI). However, paper records can also pose a great threat when PII or PHI is disclosed to an impermissible individual or entity.

For example, imagine if a mass mailing goes wrong – where someone inadvertently mismatches information causing the entire mailing to disclose PHI to unintended recipients. Or, maybe the placement of an address is too close to PHI which causes PHI to become inadvertently exposed in a window envelope during mailing. These specific examples have required covered entities and business associates to report large breaches to the U.S. Department of Health and Human Services (HHS) – resulting in these entities finding themselves on the HHS "wall of shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Please remember that it is Viva Health's expectation that our vendors require the same level of commitment to privacy and diligence when handling paper PII and PHI as is required with the most sensitive electronic records. This is especially true when paper records leave your organization.

Thank you for your commitment to protecting member information!

Being Audit Ready

The CMS Program Audit remains one of the primary mechanisms CMS uses to evaluate Medicare Advantage plans on how they take care of their members while meeting the CMS requirements. Therefore, CMS tries to audit all plans on a regular basis. Viva Health was last audited in 2014 and with each passing year the chances of being selected for a CMS Program Audit increase.

The good news for 2020 CMS Program Audits is that the audit protocols and methodologies have changed very little from the 2018 audit protocols. This means the data collection and review methodologies established in 2018 still work for 2020. However, the downside to using the same audit protocols is that CMS has honed its abilities to review the data and find potential issues. With the increased likelihood of an audit and CMS's audit capabilities, being audit ready is crucial. As a Viva Health delegate, you are considered to be Viva Health in the eyes of CMS. This means CMS as well as Viva Health expect all delegates to be audit ready.

Being audit ready is more than just pulling and producing data. Being audit ready is ensuring you are up to date with the constantly evolving CMS rules and expectations. Being audit ready means proactively reviewing your processes and data to identify potential faults and correcting them as soon as possible. Being audit ready is communicating regularly with your Viva Health contact to facilitate the flow of information in both directions. Being audit ready does not mean that mistakes will not happen, but it means mistakes are identified and corrected before they become a systemic issue.

We value your participation with Viva Health and your effort to do things right. If you have any questions or concerns about being audit ready, please contact us:

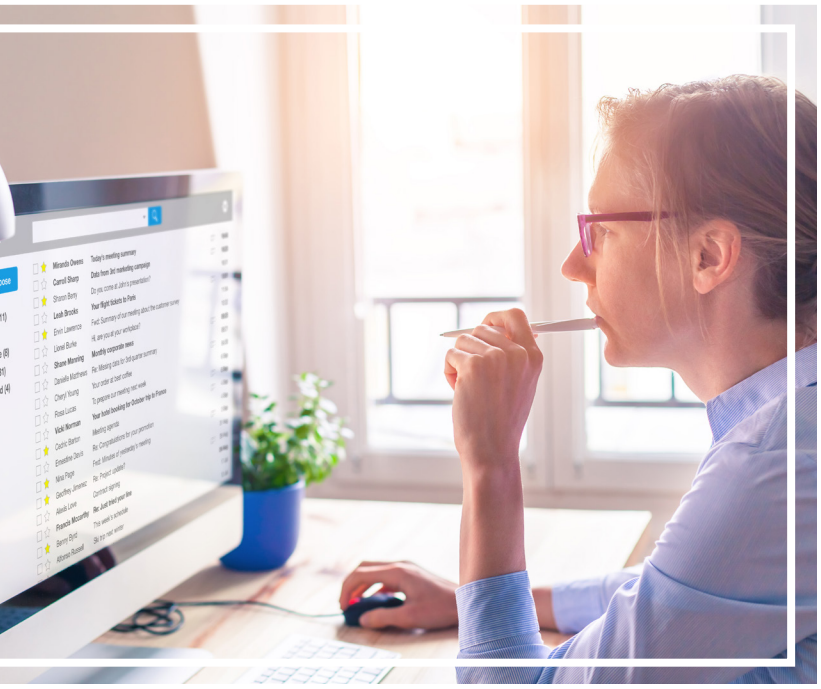
Tanya Maddox, *Viva Health Vendor Oversight Manager* – 205-558-3283 – tanyamaddox@uabmc.edu

Charlie Cutcliffe, *Viva Health Compliance Officer* – 205-558-7606 – ccutcliffe@uabmc.edu

CMS Program Audit: https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/ProgramAudits.html

Vendor Email Compromise (VEC)

In its annual report, the FBI Internet Crime Complaint Center (IC3) reported receiving 351,937 complaints in 2018 – an average of more than 900 every day. The most financially costly complaints involved BEC (Business Email Compromise). Reports to the FBI came in from every state and involved victims of every age.



Vendor Email Compromise (VEC) attacks, a form of BEC, are on the rise! VEC involves highly realistic emails requesting payment of invoices. The victims of VEC attacks are not only the company whose email accounts have been compromised, but also those who have received an email from the company!

VEC attacks start with a spear phishing email targeting to a high level employee such as the CEO or CFO. Once credentials have been obtained from an employee through the spear phishing attempt, the account is accessed, and email forwarding rules are added. A copy of every received and sent email in the compromised email account is then forwarded to the attacker, unbeknown to the employee.

Over a period of weeks or months, the emails are studied and the attackers learn about customer billing cycles and typical invoice amounts. The attackers also study the format of the emails, obtain the relevant logos, and use this information to create highly realistic fake invoices for the right amount at the right time.

The invoice requests are sent just a few days before an organization would usually receive an invoice or make a payment for an invoice. The attacker then requests a bank account change so that the payment is made to the attacker's account as opposed to the legitimate organization.

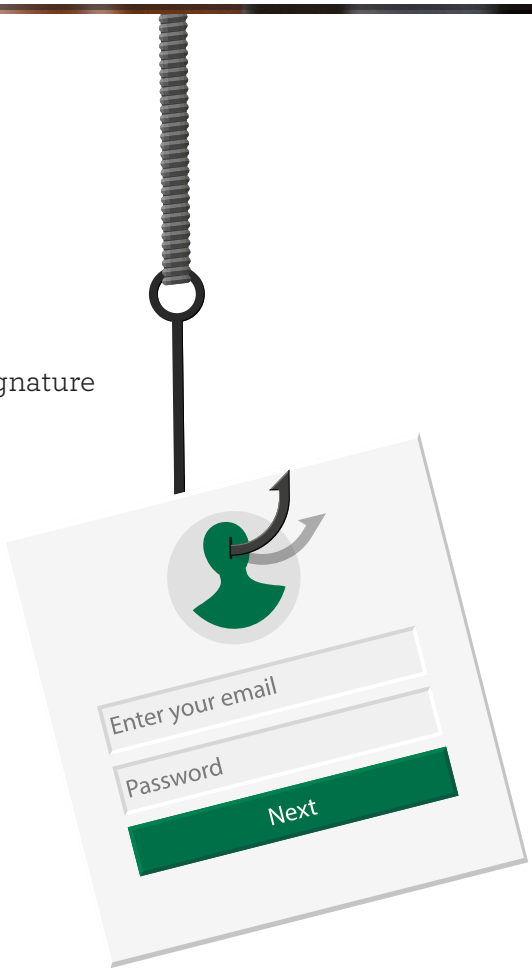
These types of attacks are difficult for employees to identify as all the typical signs of fraudulent emails are lacking. There may not be spelling mistakes, grammar issues, and the emails come from a genuine – not spoofed – email account.

A few ways to protect yourself from these type of attacks:

- Employee training – staff should be able to identify "suspicious emails" but continual cybersecurity training will reinforce updated types of threats
- Implementing multi-factor authentication – this can assist in preventing unauthorized access if an attacker obtains an employee's credentials
- A robust cybersecurity policy, which should be updated at least annually

What to watch for in phishing emails?

- Known sender name, but "mailto" doesn't match – example below:
  From: Lynn Murphree
  [mailto:admin@company-execs.com]
- Unknown sender
- Unexpected attachment
- Sender name in the address does not match the name in the email signature
- Poor grammar
- Sense of urgency
- Asking for sensitive information
  (banking information, passwords, etc.)



For additional information regarding cybersecurity education, please visit the Department of Health and Human Services' website at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

Your Viva Health Contacts

Tanya Maddox
Vendor Oversight Program Manager
Phone: 205-558-3283
Email: tanyamaddox@uabmc.edu

Teresa Evans
Director of Privacy and Vendor Oversight
Phone: 205-558-7544
Email: temevans@uabmc.edu