Q4 WINTER 2022

VOLUME 2

Coding Chronicle

Coding Concepts' Company Newsletter

OCR Settles Potential HIPAA Violation After Dental Practice Discloses PHI on Yelp

By Jill McKeon

The HHS Office for Civil Rights (OCR) reached a settlement with California-based New Vision Dental (NVD), over a potential HIPAA violation. The practice paid OCR $23,000 and agreed to implement a corrective action plan.

New Vision Dental allegedly disclosed protected health information (PHI) online in response to negative social media reviews, a 2017 complaint to OCR stated. The comments included patient names, insurance information, and treatment information.

“Specifically, Complainant alleged that NVD habitually disclosed PHI when it responded to patient posts sometimes providing full names where only Yelp monikers were used by the patients and including detailed information about patient visits and insurance that may not have been previously mentioned in their initial reviews,” OCR noted.

OCR launched an investigation and determined that New Vision Dental impermissibly disclosed PHI, failed to implement certain policies and procedures with respect to PHI, and failed to have the minimum content required in its Notice of Privacy Practices. The settlement agreement is not an admission of liability by NVD.

Coding Concepts
Innovative Coding Solutions

As part of its corrective action plan, NVD agreed to develop, revise, and maintain written policies and procedures to comply with federal privacy and security standards. All workforce members will also receive training on those policies and procedures, and NVD is required to remove all social media postings that include PHI.

“This latest enforcement action demonstrates the importance of following the law even when you are using social media. Providers cannot disclose protected health information of their patients when responding to negative online reviews. This is a clear NO,” OCR Director Melanie Fontes Rainer explained in a press release. “OCR is sending a clear message to regulated entities that they must appropriately safeguard patients’ protected health information. We take complaints about potential HIPAA violations seriously, no matter how large or small the organization.”

Breathing Techniques to Reduce Stress and Improve Focus:

4-3-8 Breathing

The 4-3-8 exercise forces the body to regulate breathing. This will reduce stress, enhance focus, and replenish your body’s oxygen levels. Practice this technique at least 2 times per day to see results. Below are 6 steps to get you started on 4-3-8 breathing:

- Sit-back or lay down in a comfortable space
- Close your eyes and place your hand on your belly
- Take a deep breath through the nose for 4 seconds and expand the belly
- Hold your breath for 3 seconds
- Exhale for 8 seconds while relaxing the belly
- Repeat 3 to 7 times

WINTER 2022

December 18th- First Day of Hanukkah
December 21st- First Day Of Winter
December 21st- 2nd Issue of Coding Chronicle
December 21st- Monthly Staff Meeting
December 25th- Christmas Day
December 26th- Observed Holiday/Office Closed

December 26th- Last Day of Hanukkah
December 26th- Kwanzaa
December 31st- New Year's Eve
January 1st- New Year's Day
January 2nd- Observed Holiday/ Office Closed
January 16th- Martin Luther King Jr. Day

February 14th- Valentine's Day
February 20th- President's Day
March 8th- International Women's Day
March 12th- Daylight Savings Begins
March 17th- St. Patrick's Day
March 20th- First Day of Spring

REDUCE THE RISK OF EMAIL PHISHING RANSOMWARE ATTACKS

EMAIL PHISHING ATTACKS ARE THE LEADING CAUSE OF MALWARE INFECTIONS. IN 2020, 54% OF MANAGED SERVICE PROVIDERS (MSP) REPORTED PHISHING AS THE TOP RANSOMWARE DELIVERY METHOD. ANOTHER REPORT RELEASED BY THE FEDERAL BUREAU OF INVESTIGATION (FBI) LISTED PHISHING SCAMS AS THE TOP CYBERCRIME IN 2020, RESULTING IN OVER $4.2 BILLION IN LOSS OR THEFT. IN ADDITION TO ANTIVIRUS SOFTWARE, YOU CAN TAKE ADDITIONAL PRECAUTIONS BY USING PRACTICES OR TECHNOLOGIES LIKE:

- DON'T OPEN EMAILS FROM UNKNOWN SENDERS - AVOID CLICKING ON ATTACHMENTS, FILES, OR LINKS FROM UNKNOWN ADDRESSES OR UNAUTHORIZED SOURCES.
- KEEP EMAIL CLIENT APPS UPDATED - DON'T ALLOW CYBERCRIMINALS TO TAKE ADVANTAGE OF SECURITY VULNERABILITIES FROM OUT-OF-DATE TECHNOLOGY.
- SENDER POLICY FRAMEWORK (SPF) - EMAIL AUTHENTICATION TECHNIQUE TO DESIGNATE SPECIFIC EMAIL SERVERS FROM WHICH OUTGOING MESSAGES CAN BE SENT.
- DOMAINKEYS IDENTIFIED MAIL (DKIM) - PROVIDES ENCRYPTION KEY AND DIGITAL SIGNATURE TO VERIFY THE EMAIL WAS NOT SPOOFED, FORGED, OR ALTERED.
- DOMAIN MESSAGE AUTHENTICATION REPORTING & CONFORMANCE (DMARC) - FURTHER AUTHENTICATES EMAILS BY MATCHING SPF AND DKIM PROTOCOLS.

HEALTHCARE INDUSTRY REMAINS A TOP VICTIM OF RANSOMWARE ATTACKS

By Sarai Rodriguez

Ransomware attacks continue to be the most prolific threat that organizations face across all infrastructure verticals, with the healthcare sector as a top target, according to the GuidePoint Security Q3 GRIT Ransomware report.

Behind the manufacturing sector, the healthcare industry was the second targeted by ransomware attacks in Q3. Ransomware groups such as Everest, BianLain, and LockBit were responsible for most of the attacks on the healthcare sector.

“Everest is a Russian-speaking ransomware group with potential connections to Blackbyte (who were observed in November 2021 targeting organizations with unpatched Microsoft Proxyshell vulnerabilities), and they maintain a presence on dark web marketplaces and forums such as Breached.to–a supposed RAID forums replacement–and XSS,” the report said.

The report noted a minor downtrend in ransomware attacks during Q3 as the biggest ransomware actors, including LockBit and Hive, saw a combined 53 percent decrease in reported victims.
Despite this slight decrease, the report found that eight groups published increases of five or more victims in October compared to September. According to the report, these groups had 62 more victims than the month prior.

Even though LockBit declined in activity, the ransomware groups remain one of the most active across all sectors.

"While two of the biggest ransomware actors saw a combined 53 percent decrease in reported victims, the total victims published across GRIT’s dataset only decreased by 7.3 percent, indicating a major increase among the remaining ransomware organizations,” the report stated. “If this shift continues, we may see a major increase in targeting from groups toward organizations impacting potential loss of life, such as Healthcare, Utilities, and Energy.”

In February 2022, the Federal Bureau of Investigation (FBI) released a flash alert to warn victims of LockBit 2.0 ransomware indicators of compromise.

“LockBit 2.0 ransomware compromises victim networks through a variety of techniques, including, but not limited to, purchased access, unpatched vulnerabilities, insider access, and zero-day exploits,” the FBI flash alert stated.

“After compromising a victim network, LockBit 2.0 actors use publicly available tools such as Mimikatz to escalate privileges. The threat actors then use both publicly available and custom tools to exfiltrate data, followed by encryption using the LockBit malware. The actors always leave a ransom note in each affected directory within victim systems, which provides instructions on how to obtain the decryption software.”
As the group evolves rapidly, healthcare organizations should remain aware of potential threats, officials stated in brief. The cybercriminal group released LockBit 2.0 in June 2021 after launching the original version in September 2019.

HHS recommended that healthcare organizations follow standard ransomware prevention best practices, such as using multi-factor authentication, enforcing strong passwords, and establishing a comprehensive data backup program.

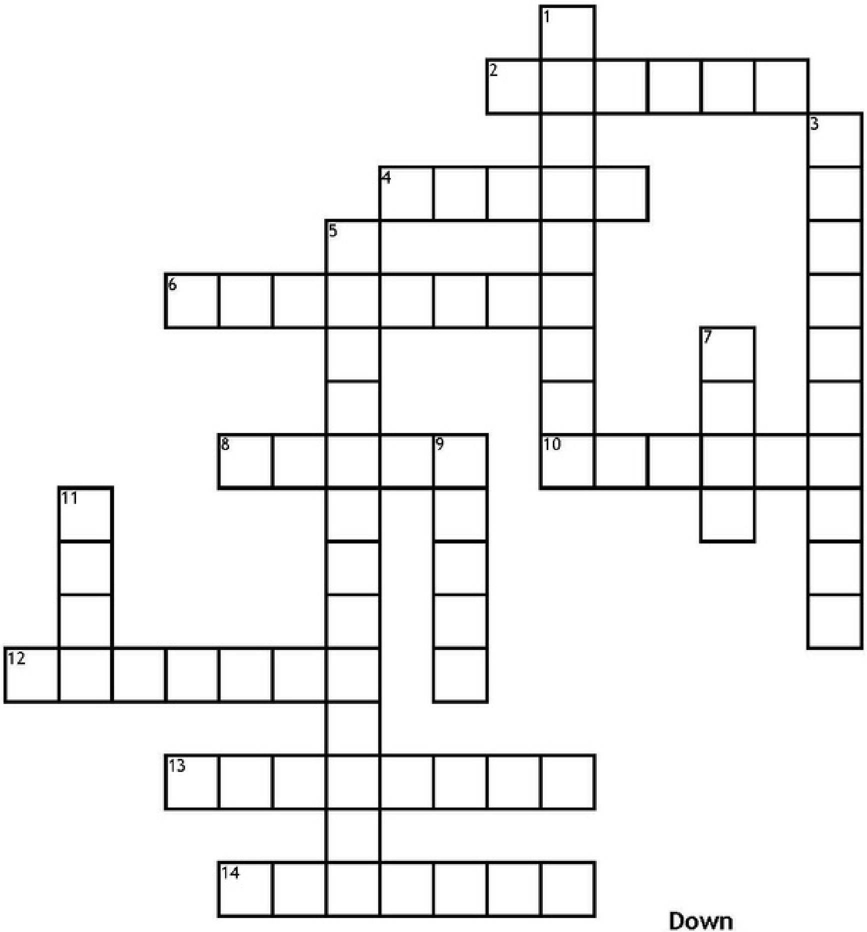
Resources:

- https://healthitsecurity.com/news/ocr-settles-potential-hipaa-violation-after-dental-practice-discloses-phi-on-yelp
- https://memoryspring.com/articles/breathing-techniques-for-improved-focus-and-memory/
- https://healthitsecurity.com/news/healthcare-industry-remains-a-top-victim-of-ransomware-attacks
- https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks

PUZZLE ACTIVITY

EMAIL YOUR COMPLETED CROSSWORD TO ADMIN TO BE ENTERED IN A DRAWING FOR A PRIZE

Phishing



Across

2. Ransomware attacks continue to be the most prolific threat that organizations face across all infrastructure verticals, with the healthcare sector as a top _____.

4. Phishing uses email files, attachments or links to _____ people into providing personal data

6. At Coding Concepts _________ is responsible for security & compliance

8. phishing emails may contain _____ to websites

10. Phishinig is an example of ______ engineering

12. Unprotected systems and uneducated employees leave us at risk of a breach and a potential ________.

13. Phishing is typically carried out by email _________

14. ________ sometimes uses fake caller-ID data to mask where calls are coming from

Down

1. Phishing scams can infiltrate payroll, risking employee ________

3. ___________ URL's or the use of sub domains are common tricks by phishers.

5. Phising is the number 1 cybercrime, costing __________ over $4.2 Billion in loss or theft

7. Phishing is a homophone of fishing because both use ____

9. ______ phishinig are attempts directed at specific individuals or companies.

11. Phishing is an attempt to obtain sensitive ____

Word Bank

data
spear
target
bait
misspelled
organizations
spoofing
vishing
paychecks
social
trick
everyone
links
lawsuit