MARSH & McLENNAN AGENCY

SPECIAL ALERT

Volume Fourteen, Issue Nine

August 2018

OFFICE OF CIVIL RIGHTS (OCR) CYBER SECURITY NEWSLETTER

A recent Office of Civil Rights cybersecurity newsletter discusses software vulnerabilities and patches. Because organizations need to comply with HIPAA security requirements, the government continues to provide information on protecting electronic health information. More details on the HIPAA Security rule can be found in our 2014 March *Benefit Advisor* at http://www.mcgrawwentworth.com/Benefit_Advisor/2014/BA_Issue_2.pdf.

The newsletter discusses a common vulnerability in computer processors sold over the last decade. This security flaw allows malware (for example, Spectre and Meltdown) to bypass controls and possibly access sensitive data. Once this problem was discovered, vendors developed patches to block such bypasses. However, some of the patches affected the performance of certain programs.

Many entities and business associates often use software when they work with EPHI. The Security Rules require these entities to protect EPHI and identify any potentially vulnerable situations. They must analyze risks, take steps to eliminate them, and establish a process for patching software. Technology and potential security issues change and develop rapidly. Organizations need to be vigilant to keep up on potential threats. One useful resource is the United States Computer Emergency Readiness Team (US-CERT). This organization collects and publishes information on threats that arise. Its website is https://www.us-cert.gov/.

Organizations can also identify potential security issues using certain tools. Scanners, for example, are software tools that can test systems and networks for known vulnerabilities, including outdated or unsupported software. Part of any security plan should be finding potential security issues and correcting them. Patches can often keep systems secure.

Continued on Page 2

We welcome your comments and suggestions regarding this issue of our Special Alert. For more information, please contact your Account Manager or visit our website at www.mma-mi.com.

Patches do not apply only to software on computer systems. You may need to install them on phones, computers, servers, routers and so on. Applying patches can be a routine process. However, sometimes patches can affect the function or output of other programs. As a result, organizations need to evaluate them and understand how they affect their interdependent systems. The newsletter suggests organizations add a patch management process to their security management program. It should include these critical steps:

- **Evaluation** – Evaluate patches to determine whether they apply to any software or systems.
- **Patch testing** – Test patches on isolated systems, if possible, to find any unwanted side effects, such as improperly functioning applications or unstable systems.
- **Approval** – Once patches are tested and evaluated, you can approve them.
- **Deployment** - Your organization can schedule patches to be installed live or with production systems.
- **Verification and testing** – once the patches are in place, your organization should continue to test and monitor systems to make sure there are no unforeseen side effects.

Making sure systems that use or house EPHI are secure is a critical step to complying with HIPAA Security Rules. HIPAA covered entities need to explain how they will handle vulnerabilities in their Security Plan. MMA

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affective if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change.

Marsh & McLennan Agency LLC

Health & Benefits
3331 West Big Beaver Road, Suite 200
Troy, MI 48084
Telephone: 248-822-8000 Fax: 248-822-4131
www.mma-mi.com

Property & Casualty
15415 Middlebelt Road
Livonia, MI 48154
Telephone: 734-525-0927 Fax: 734-525-0612
www.mma-mi.com