BROWNEDWARDS

Medical Practice Newsletter

August 1, 2016

CYBER INCIDENT RESPONSE

On July 7, 2016 the Office for Civil Rights (OCR), the enforcement agency over HIPAA Security, reminded us of the importance of a computer security incident* response plan when it issued an e-mail alert focusing on preparedness for cybersecurity incidents.

Attacks related to cyber security continue to increase, and while employee negligence and lost/stolen devices continue to be leading causes of data breaches, reports from both the Ponemon Institute's *Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data* and Health IT Security (HealthITSecurity.com) indicate that outside attacks are now the cause of half the data breaches reported in healthcare. From large insurers, to the Obama Care Website, to major hospital systems, to private physician offices, no healthcare entity is exempt from attempted cyberattack.

The HIPAA Security Rule requires Covered Entities (CE) and Business Associates (BA) to develop a security incident response plan, and the expansion of cyberattack related security breaches should make this planning a priority. A security incident response plan helps CEs and BAs detect breaches, identify weaknesses that were exploited, and decrease losses, while protecting the confidentiality, integrity, and accessibility of data, and restoring normal IT services.

When considering the development of a security incident response plan, CEs and BAs should consider the specific policies and procedures the plan for their entity would require in the event of a security incident.

- Policies help the CE & BA develop a coordinated approach to incident response. The policies should provide a "roadmap" for implementing incident response protocols.
- The plan should be specific to the CE's and BA's structure, size, and function and should be approved by management. It should also allocate necessary resources to incident response preparation.
- Procedures are the specific processes, tools, forms, etc. to be used in the event of a security incident and should be based on the incident response policies and plan. Procedures should include the entity's methods for preparing for incidents, detecting and analyzing incidents, recovering from incidents, and conducting post-incident reviews.

Additional information can be found at:

http://csrc.nist.gov/publications/PubsSPs.html - (Special Publication 800-61, Computer Security Incident Handling Guide)

http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html - *(HIPAA Breach Notification guidance)*

* *HIPAA defines security incidents as attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 CFR 164.304). HIPAA identifies breaches as, generally, an impermissible acquisition, access, use, or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. (45 CFR 164.402).*

Disclaimer: This information is offered for informational purposes only and should not be taken as legal advice.