Good Cyber Hygiene
Checklist

GOOD CYBER HYGIENE

- ❑ Start with a risk assessment
- ❑ Written policies and procedures focused on cybersecurity and tailored to company
  - Expectations for protection of data
  - Monitoring and expectations of privacy
  - Confidentiality of data
  - Limits of permissible access and use
  - Social engineering
  - Passwords policy & security questions
  - BYOD
- ❑ Training of all workforce on your policies and procedures, first, then security training
- ❑ Phish all workforce (incl. upper management)
- ❑ Multi-factor authentication
- ❑ Signature based antivirus and malware detection
- ❑ Internal controls / access controls
- ❑ No default passwords
- ❑ No outdated or unsupported software
- ❑ Security patch updates management policy
- ❑ Backups: segmented offline, cloud, redundant
- ❑ Use reputable cloud services
- ❑ Encrypt sensitive data and air-gap hypersensitive data
- ❑ Adequate logging and retention
- ❑ Incident response plan
- ❑ Third-party security risk management program
- ❑ Firewall, intrusion detection, and intrusion prevention systems
- ❑ Managed services provider (MSP) or managed

"GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a **comprehensive information security program** that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondents' or the business entity's size and complexity, the nature and scope of respondents' or the business entity's activities, and the sensitivity of the personal information collected from or about consumers." *In re GMR Transcription Svcs, Inc., Consent*

"[T]he relevant inquiry here is a cost-benefit analysis, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." *FTC v. Wyndham*, (3rd Cir. Aug. 24, 2015)

For more information, please contact:
Shawn E. Tuma
Cybersecurity & Data Privacy Attorney
Office: 972.324.0300 | Mobile: 214.726.2808
shawnetuma@gmail.com
Blog: www.shawnetuma.com