Maher Duessel
Client Data Protection Protocols

- Employee security training is performed during onboarding and through multiple yearly updates (current training is due April 22, 2020).
- All systems have antimalware software, with virus definitions updated in real-time. Full scans are performed weekly.
- All systems are running Bitdefender software firewalls.
- The logs from all systems' antimalware software and firewalls are reviewed on a nightly basis.
- All laptops have encrypted hard drives.
- All MD networks are protected by layer 7 firewalls with intrusion detection and prevention systems, gateway malware protection, and gateway file capture threat protection against ransomware.
- Other data transfers not done via our secure file transfer site, by policy, must be done only by MD provided encrypted USB memory sticks.
- Any data residing on Maher Duessel server equipment is encrypted, and if that data is included in any sort of backup, it is also encrypted, both in transit and in storage.
- All MD systems can only connect to the MD network by secure means, either by onsite authentication, or via a VPN connection.

Secure File Transfer Site

- All file transfers with sensitive PHI/PII are done via our secure file transfer site, which uses encrypted communication and is stored in an encrypted format.
  - MD's secure file transfer site requires 2 factor authentication to log into.
  - Client folders have restricted access and MD employees must request access to a specific client, which is then granted by a member of our IT department.
  - Folders cannot be viewed by employees who are not on the engagement team for that specific client.
  - An MD employee should send you a link for your secure file transfer site. This link is specific to your engagement. Please upload all information to the secure file transfer site using this link.
  - A link can be sent to multiple individuals at one time if requested from your MD contact. Please include an email address and an MD employee will send a link.