Maher Duessel
Client Data Protection Protocols

- Employee security training is performed during onboarding, and through multiple yearly updates
- All systems have anti-malware 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' anti-malware software and firewalls are reviewed on a nightly basis
- All laptops have encrypted hard drives
- All firm 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 file transfers not done via *Suralink*, by policy must be done only by firm 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 firm systems can only connect to the Maher Duessel network by secure means, either by onsite authentication, or via a VPN connection

Suralink PBC Request List Management Software

- All file transfers with sensitive PHI/PII are done only via *Suralink,* which uses encrypted communication and is stored in an encrypted format
  - Client folders have restricted access and firm 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.
  - A firm employee should send you a link for your *Suralink* site. This link is specific to your engagement, please upload all information to the *Suralink* site through this link.
  - A link can be sent to multiple individuals at one time if requested from your engagement team contact, please include an email address and an employee will send a link