MainStreet Financial Planning Document Security System

1. We ask for the minimum amount of information needed to complete our assigned task of providing reliable recommendations about all areas of financial planning including saving, debt, investments, estate planning, taxes and future projections/recommendations for each.
2. We protect client information using several systems that do not interact (or talk) with each other except for email acquisition by our customer relationship management (CRM) system from our email system, with attachments.
3. Documents supplied by clients and reports produced and provided to clients are held in a secure cloud system operated by Citrix for more than 100 million users and 99% of the Fortune 500. These documents are encrypted up and down meaning once they leave either end of the system, they are secure from user to storage and return. It is not connected to any of our other systems.
4. Our CRM system is powered by WealthBox. It is a stand-alone system containing client information for each contact we have with clients either by email, or phone. It has extensive notes from meetings and conversations to inform team members of actions experienced and taken. Data is entered separately except for email reception. It too does not interact with our other systems except it receives client emails with attachments for storage in a duplicate system with our email system when WealthBox recognizes the client's email address.
5. Our email system is operated by Google in the Gmail system. It supplies WealthBox with emails that are received by the known addresses in the contact management system. All emails are archived by Google for future retrieval, if needed.
6. Our financial planning software MoneyGuidePro is another stand-alone system. It does not interact with our other systems and data must be entered separately. Clients are given access to their financial plans as long as they are ongoing clients.
7. All of our data systems use 256 bit-encrypted SSL passwords with two-factor authentication, meaning, in most cases, we must enter numbers texted to us if we sign on from a new computer or passwords have changed.
8. All user employee computers feature encrypted hard drives and the passwords for each of our systems both online and on computer are changed every 90 or 180 days depending on individual system protocols.

Updated: April 12,2020