

## ELECTRONIC COMMUNICATION AGREEMENT

Richard R Hill MD PhD  
19910 Malvern Rd., Suite 223  
Shaker Heights, OH 44122

Electronic means of communication such as emails and texting are fast and efficient but if not protected by encryption, can lead to breaches in personally identifiable information (PII) and protected health information (PHI). **Encryption** is an electronic process that scrambles email messages so hackers on the Internet can't read/steal the information, allowing secure communication of valuable health information. For example, I may send you an email that reads, "your thyroid study result was abnormal-we will talk about it at your next appointment". After encryption, a hacker might see, "#\*U&lkj))Dur8\*9)3578@!\$" which is useless information.

To protect against information breaches, I use **protonmail**, which is a very secure **free** email service that allows **end to end encryption**. This means both the emails you send me and the emails I send to you are encrypted.

Please sign up for a free protonmail account at [www.protonmail.com](http://www.protonmail.com) and then use the account to send me emails. Everything you send me and all of my replies will then be secure. The use of other email services will not offer this security.

You can also use **Google Voice** at **216-309-1550** to leave me a voicemail. This is best for conveying brief one-way info such as confirming an appointment or requesting a refill; things that do not require back-and-forth communication. My replies to you will be in the form of a text message-and while Google offers some security, it is less secure than messages sent via protonmail.

I, \_\_\_\_\_, have read and understand the electronic communication agreement-including the risks to myPHI and PII should I not choose to use the encryption format described above.

Date \_\_\_/\_\_\_/\_\_\_\_\_