

M2S PEMS Enhanced Security FAQs

Why does M2S have such strict requirements for PEMS passwords?

Unfortunately, there are hackers that for one reason or another would like to access your information. And for M2S, that information is your very important Protected Health Information (PHI). To ensure institutions are protecting your PHI, the National Institute of Standards and Technology (NIST) has recently drafted recommendations in a Guide to Enterprise Password Management (<http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>) that HIPAA regulations expect M2S to follow. The password requirements for PEMS were designed to meet these requirements.

What happens if M2S does not follow the guidelines?

The PHI in PEMS would be less protected from intrusions, putting risk to the privacy of the patient. Failure to comply with HIPAA can result in both civil and criminal penalties. In February 2009, the American Recovery and Reinvestment Act of 2009 (ARRA) became law. This Act created a tiered civil penalty structure for HIPAA violations. Following the password guidelines adds extra security to the accessibility of the PHI, protecting the privacy of the patient, and financial and reputational harm to M2S, and the covered entity (i.e. Hospital or Physician's Office)..

What happens if my data is breached?

M2S would be required to alert all covered entities involved. The covered entity would be required to notify the United States Department of Health and Human Services and the patients involved, and potentially make an announcement to the public media. We would also be vulnerable to fines and penalties as mentioned above. M2S is making every attempt to protect your data and to avoid an embarrassing and potentially harmful situation that a data breach could bring.

I frequently forget my M2S password. How can I easily obtain it without having to call M2S' customer service?

Re-setting your password is as easy as answering a security question that was created and set by you! Simply log-in to PEMS and set your own question and answer. If you type the wrong password in PEMS, you will be prompted to answer the question you have set. An e-mail will be sent with a new password. Voila! You can log-in to PEMS and re-set your password to one that will be easy for you to remember.

There are many people that require access to my PHI in PEMS. How can I easily and securely share this information with them?

DO NOT SHARE YOUR PASSWORD. M2S provides access to PEMS for free. Please send an e-mail to the M2S customer service department (customer-service@m2s.com) to request access for individuals.