EAR Identity theft prevention

All patient information is kept electronically. Any document used for data collection or transmission is scanned into the patient file and then shredded on a daily basis.

E-mail and Fax documents use only a partial identifier and contain a disclaimer that we be notified if the fax or e-mail was received in error.

Computers are password protected at the log-on and for each individual program that is used (Noah, Blueprint, Quickbooks). Only program features required for an employees’ job function are activated. There is an audit control function in Noah that can track activity by user and is used by the business owner.

Data is backed up on a regular basis and kept off site. The back-up device is also password protected.

We have a confidentiality agreement in place with all vendors that have access to patient names.

Patient financial information regarding their bank, credit status or credit charges are not kept on sight but processed through First Data/Merchant Solutions on an individual basis.