Regarding	**HIPAA SRA Question**	**RevolutionEHR details**
CEHRT	Do you have a process to review EHR system login attempts to identify potential brute-force (high number of failed login attempts) login attacks?	RevolutionEHR monitors system for login attacks; RevolutionEHR server is not maintained locally.
CEHRT	Is your EHR configured to allow additional privacy permissions (i.e. for high-profile patients, or if patients pay out-of-pocket for services and do not wish to disclose to their health plan) to patient information? Is your EHR configured emergency access (i.e. break the glass) so they may access restricted patients in the EMR/ePHI/PII without calling an administrator?	RevolutionEHR does not provide patient-level privacy permissions that allow specific patients to keep their data "more safe" than others. RevolutionEHR maintains an emergency access URL so users with restricted access can get in to the application without restriction. RevolutionEHR doesn't have the concept of restricted patients so access to all patients' data would be available.
CEHRT	Certified EHR Technology (CEHRT) for Meaningful Use Stage II configuration check: Is your EHR configured with the following (All features must be ON to answer YES): system logging status, record all ePHI accesses, end-user encryption OR not storing ePHI on end-user devices, audit-log protection (i.e. changed or deleted not allowed), detection if the audit log is altered?	RevolutionEHR is 2014 CEHRT and meets appropriate technical requirements including built-in access logs and audit logs that show when each user signed in, and the actions that each user may have taken within a patient record. RevolutionEHR does not store ePHI on end-use devices. ***Recommendation: run an audit report/access report from admin to become familiar with this functionality if you are not yet using it regularly***
CEHRT	Does this certified Electronic Health Record Technology (CEHRT), or EMR software, enable users to electronically select a patient's record for an accepted or denied amendment?	See RevolutionEHR Amendment Demo for instructions and documentation of this functionality
Technical Safeguards	Do you have a procedure for facility access so IS personnel can access the Data Center / Main Data Facility for the purposes of disaster recovery or emergency mode operations?	RevolutionEHR database is not maintained locally. *Organizations with file and mail servers and should document their policies and procedures appropriately.*

HIPAA Security Officer	Does your Business Associate Agreement contain the required components for your vendors to take responsibility for protecting your ePHI, including the obligation to likewise obligate their sub-contractors to notify you immediately if they have a breach and to take responsibility (legal and practical) by terminating agreement where warranted and/or reporting the problem to the HHS Secretary? This includes the vendor maintaining their own HIPAA/HITECH Act security measures.	*** Retain a copy of your current BAA with RevolutionEHR*** Details on the security measures in place at RevolutionEHR's data center are available here: http://www.atomicdata.com/data-centers/minneapolis-central
Physical Safeguards	Do you have controls in place for ensuring workstations that have access to ePHI systems are physically secure from unauthorized access (i.e. not facing patient/client waiting areas, workstation or access-ports (i.e. USB, power, etc.) not accessible via patient/client waiting areas, behind locked doors, etc.)?	Complete a physical walkthrough for each practice location noting how staff interact with ePHI, how access to hardware is managed, etc.
Network security	Is SHA1 or greater used as a hashing algorithm (i.e. EHR server communication) to ensure ePHI being transmitted is not altered during transmission across public networks?	Customer databases exist in the secure framework of RevolutionEHR, and ePHI is accessed and transmitted via the secure web portal https://revolutionehr.com/pms/ which maintains a SHA1 or greater hashing.
Network security	Is the encryption level for electronic transmissions of ePHI at least: 3DES, AES, or EES, or Asymmetric keys: RSA PKCS #1, employing128-bit ciphers or larger to ensure all ePHI being transmitted is sufficiently encrypted during transmission (i.e. SSL access to EHR.)?	Customer databases exist in the secure framework of RevolutionEHR, and ePHI is accessed and transmitted via the secure web portal https://revolutionehr.com/pms/ which maintains a SHA1 or greater hashing.