Security Risk Analysis Prepayment Checklist

Name of Professional(s)/Group/Facility_____ **NPI#**_____

Date Security Assessment Performed:_____

Security Components	Examples	Examples of Security Measures	Check if completed: (*See below for Uncompleted Tasks)
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers	
Asset Inventory	• Inventory of physical systems, devices, and media in your office space that are used to store or contain ePHI	• Workstations • Portable devices • * Information systems	
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement	
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption	

Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention	
Organizational Requirements	• Breach notification and associated policies • Business associate agreements	• Agreement review and updates	

***If any of the above boxes are left un-checked, please provide a proposed completion date and attach a summary of your plan to complete each section**

Signature and Title of Eligible Professional or Designee Date

_____ _____

Please be advised that the above are only examples and should not be used as a comprehensive guide for mitigating security risks. You should put into place reasonable and appropriate administrative, physical and technical safeguards that are tailored to the size and complexity of your practice. For more information, including a ten-step plan for health information privacy and security, review ONC's Guide to Privacy and Security of Health Information, or visit The U.S. Department of Health and Human Services (HHS) Office of Civil Rights' (OCR) webpage. Please be aware that, if chosen for a post payment audit, a copy of the conducted or reviewed security risk analysis and corrective action plan (if negative findings are identified) should be dated prior to the end of the reporting period and include evidence to support that it was generated for that provider's system (e.g., identified by National Provider Identifier (NPI), CMS Certification Number (CCN), provider name, practice name, etc.). A single report submitted for a group of applying providers can be used; however, the report needs to be broken down by provider and NPI. Uploading this documentation at the time of application is optional but this documentation should always be in addition to this prepayment checklist.

Things to Consider to Help Answer the Questions:

Identify the areas where your practice has information systems and equipment that create, transmit, or store ePHI. Include all buildings and rooms within it that have data centers, areas where equipment is stored, IT administrative offices, workstation locations, and other sites. Information systems normally include hardware, software, information, data, applications, and communications.