

## SECURITY RISK ANALYSIS COMPLIANCE FORM

This form is intended to be used by a Provider [an Eligible Professional (EP) or Eligible Hospital (EH)] as documentation in support of the Meaningful Use (MU) Measure for "Protect Patient Health Information". Protecting "Patient Health Information (PHI)" includes conducting and/or reviewing a "security risk analysis" of the Provider's or organization's activities, policies and procedures for handling and maintaining the security of PHI. All responses included in this form are subject to verification, ~~pre-payment or~~ post-payment, including on-site post-payment audit and any responses found to be inaccurate, unsupported or false may result in a failure of the MU measure and recoupment of the incentive payment. (This form may be completed by an authorized staff person on behalf of the Provider.)

### 1. Provider Information

Provider's Name & Professional Title: \_\_\_\_\_ NPI: \_\_\_\_\_  
 If EP, Name of Practice or Organization: \_\_\_\_\_ NPI: \_\_\_\_\_

### 2. My Organization

a) Type b) Size (number of staff including Professional, Technical, Clerical & other support, FT, PT & volunteers)

<input type="checkbox"/> FQHC/RHC <input type="checkbox"/> Group Practice <input type="checkbox"/> Individual or Shared Office <input type="checkbox"/> Outpatient Clinic <input type="checkbox"/> Hospital	<input type="checkbox"/> 5 or less <input type="checkbox"/> 6 - 10 <input type="checkbox"/> 11 - 25 <input type="checkbox"/> 26 - 50 <input type="checkbox"/> 51-100 <input type="checkbox"/> 100+
---	---

### 3. Written Policies and Procedures

a) My organization has at least one formal written policy on the handling and security of PHI.  Yes  No  
 b) We have the following written policies and procedures (check all that apply):  
 HIPAA Compliance  
 IT Security  
 Maintaining and Protecting PHI  
 Business Associate's Agreement (BAA)  
 Other (describe): \_\_\_\_\_  
 c) We have required staff training on security and protecting PHI on at least an annual basis.  Yes  No  
 If "Yes", then (check all that apply):  
 (i)  Training is conducted on a group/seminar basis  
 (ii)  Individual, self-study basis  
 (iii)  Other (explain) \_\_\_\_\_

### 4. CEHRT

a) Date my organization's CEHRT was installed\*: \_\_\_\_\_ (mm/yyyy)  
 b) Date of the most recent upgrade of my organization's CEHRT: \_\_\_\_\_ (mm/yyyy)

\*If you have not changed your CEHRT product/vendor since your very first EHR Incentive Program attestation, this will be the original implementation date. If you changed product/vendor since your very first attestation, indicate the implementation date of the current CEHRT.

### 5. Risk Analysis

The Security Risk Analysis must include the following:

- Auditing, reviewing and/or evaluating the organization's written and informal practices
- Review of the policies and procedures regarding the handling, maintenance and protection of PHI
- Review and identify an analysis of CEHRT addressing encryption/security of data & implement updates as necessary
- Making a critical evaluation of the results identifying risks and developing a risk mitigation plan to include appropriate actions to address deficiencies noted included, but not limited to, updated policies and procedures, employee training and system changes.

**The SRA must be completed within the calendar year (Jan 1-Dec 31) of the Program Year.**

**A SRA must be done on an annual basis and include the entire reporting period; the same SRA cannot be used for two different Program Years**

a) Risk Analyses for my organization are conducted by (check all that apply):  
 Staff within the organization\*  Contractors  
 Other (describe): \_\_\_\_\_  
 b) When was the Security Risk Analysis performed? Please provide a date: \_\_\_\_\_  
 c) What is the provider's MU reporting period? Please provide date range used: \_\_\_\_\_  
 d) What period in 2019 did the Security Risk Analysis cover? Please select one of the following:  
 January 1-December 31, 2019  July 1-September 30, 2019  
 January 1-March 31, 2019  October 1-December 31, 2019  
 April 1-June 30, 2019  Other (provide date range): \_\_\_\_\_

\*This may include staff within the Provider's immediate office. If the organization has different divisions, sections, offices, etc., or dedicated staff for internal audits or compliance reviews, and staff from such areas of the organization perform the risk analyses, they should be viewed as "staff within the organization".

This form is being submitted in support of the attestation of the above named Provider for Program Year \_\_\_\_\_.

If applicable, initial here: \_\_\_\_\_ "I am authorized to complete and sign this form on the Provider's behalf".

Printed Name & Title: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_