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, recoupment, 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: __________________________
   If EP, Name of Practice or Organization: ________________________
   NPI: __________________________

2. My Organization

   a) Type
      - FQHC/RHC
      - Group Practice
      - Individual or Shared Office
      - Outpatient Clinic
      - Hospital
   b) Size (number of staff including Professional, Technical, Clerical & other support, FT, PT & volunteers)
      - 5 or less
      - 6 - 10
      - 11 - 25
      - 26 - 50
      - 51-100
      - 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):
      - 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

   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
      - October 1-December 31, 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: __________________________

Revised 1/2/2020