UC San Diego Health

Promoting Interoperability Attestation*

QPP Login Set-up
Base Measures
Security Risk Analysis

Promoting Interoperability:** ***Formerly Meaningful Use (MU) & Advancing Care Information (ACI)

Promoting Interoperability Measure Set (Base)*

- ACI Promoting Interoperability is designed to demonstrate your clinicians' ability to track, record, and share their patients' personal health information accurately and securely

Objective Name	Measure Description
Electronic Prescribing	At least one permissible prescription written by the MIPS eligible clinician is queried for a drug formulary and transmitted electronically using certified EHR technology.
Health Information Exchange	Sending Health Information via EMR and Receiving/Incorporating Health Information via EMR.
Patient Electronic Access	At least one patient seen by the eligible clinician during the performance period is provided timely access to view online, download, and transmit to a third party their health information subject to the eligible clinician's discretion to withhold certain information.
Public Health and Clinical Data Exchange	Report to any two different agencies/registries: • Immunization Registry Reporting • Electronic Case Reporting • Public Health Registry Reporting • Clinical Data Registry Reporting • Syndromic Surveillance Reporting
Security Risk Analysis (Protect Patient Health Information)	Conduct or review a security risk analysis in accordance with the requirements by CMS.

Security Risk Analysis (PI_PPHI_1)

- Attestation only
- The Security Risk Analysis must be completed before December 31st, 2020. In order to truthfully attest to the Security Risk Analysis Statement.
- This is a requirement by CMS, please review the suggested Security Risk Analysis Action Plan to the right.

CMS Suggested SRA Action Plan

Security Areas to Consider		Examples of Potential Security Measures
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
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Security Areas to Consider		**Examples of Potential Security Measures**
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 ensure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Business associate agreements	• Plan for identifying and managing vendors who access, create or store PHI • Agreement review and updates

Security Risk Analysis (PI_PPHI_1) Myths and Facts

FYI: Myths and Facts for SRA

The following table addresses common myths about conducting a risk analysis, and provides facts and tips that can help you structure your risk analysis process.

Security Risk Analysis Myths and Facts	
Myth	**Fact**
The security risk analysis is optional for small providers.	False. All providers who conduct certain electronic transactions, such as billing, are "covered entities" under HIPAA and are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.
My EHR vendor took care of everything I need to do about privacy and security.	False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.
I have to outsource the security risk analysis.	False. It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
A checklist will suffice for the risk analysis requirement.	False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.