HIPAA Security Risk Assessment Service

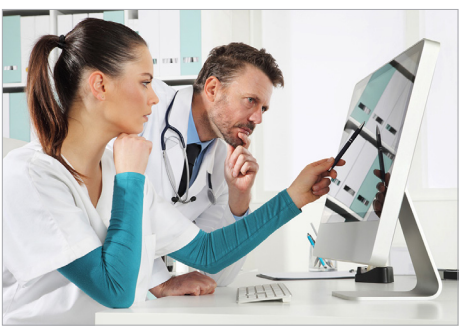
Helping Community Connect® practices comply with Merit-based Incentive Payment System (MIPS) requirements

What it is

The Center for Medicare & Medicaid Services (CMS) requires health care providers utilizing an EHR to conduct Security Risk Assessments (SRA) to safeguard their patient electronic Protected Health Information (ePHI)

Three security safeguards help comply with the HIPAA Security Rule:

1. **Administrative -** policies and procedures to clearly show how the practice will comply and adopt the HIPAA Security measures
2. **Physical -** control physical access to areas of data storage to protect against inappropriate access
3. **Technical -** protect electronic communications containing PHI when transmitted over open networks



JOHN MUIR HEALTH

How John Muir Health Can Help

John Muir Health provides SRA services to help Community Connect practices comply with CMS Merit-based Incentive Payment System (MIPS) requirements

- Security Risk Practice Self-Assessment
- Security Risk Management Plan
- Equipment and Vendor Lists
- Security Risk Policies and Procedures
- Security Officer Job Description
- Disaster Recovery
- Contingency Plan
- Review/update prior year SRA for existing clients

Protect ePHI and your practice by requesting a Security Risk Assessment today

Contact your John Muir Health Regional Physician Services Manager

JOHN MUIR HEALTH