The HealthPOINT Security Risk Assessment (SRA) is a qualitative risk analysis providing all of the core requirements to “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity” as required by the HIPAA Security Rule (45 CFR 164.308(a)(1)), and to satisfy the related core Meaningful Use criteria as described in the final CMS Medicaid and Medicare Electronic Health Records Incentive Rule.

The SRA results in many deliverables for an organization:
- Executive Summary for Administration
- Detailed Findings Report for the IT Staff and the Compliance Official
- PHI inventory
- Criticality and Threat matrix

STEP 1: The first step in our risk analysis methodology and our privacy compliance review is to analyze and inventory the protected health information (PHI) that is used and disclosed by a HIPAA covered entity. In generic risk analysis terms, this is your most valuable “asset”. From a HIPAA perspective, PHI is the asset that must be safeguarded for both Privacy and Security Rule purposes.

STEP 2: An essential step in a risk analysis is to determine the PHI that is created, stored, maintained or transmitted by an organization (including PHI that is discarded). This list is then mapped to the relevant software applications used for this purpose. The criticality is an evaluation of the impact loss of use or the loss of PHI data would have if these applications were unavailable (due to either a natural or man-made threat that had been exploited).

STEP 3: A risk analysis compares the criticality of PHI and its applications with the threats that exist. Threats are derived based upon prior experiences at your facility, and a reasonable analysis of general, natural and man-made threats (for example earthquakes may be a greater threat than tornados in your area, and the risk of a disgruntled employee sabotaging systems is always prevalent).

STEP 4: Using the PHI inventory, criticality matrix and threat matrix we then evaluate your existing controls and safeguards to establish the gaps or risks. We use a simple scale of high – medium – low to define risks and provide a narrative for each risk. As a HIPAA covered entity, we recommend a response plan as follows:

- **High Risk**: These gaps and risks require immediate attention and remediation, preferably if the resources are available within the next 30-60 days.
- **Medium Risk**: These gaps and risks require attention and remediation within the next three months. They represent sufficient threat to PHI to be incorporated in your work plans.
- **Low Risk**: These gaps and risks require attention and remediation within the next six months. They do not represent an immediate threat to PHI.

Call HealthPOINT at 605.256.5555 to schedule your Security Risk Analysis and Remediation Process Action Steps.