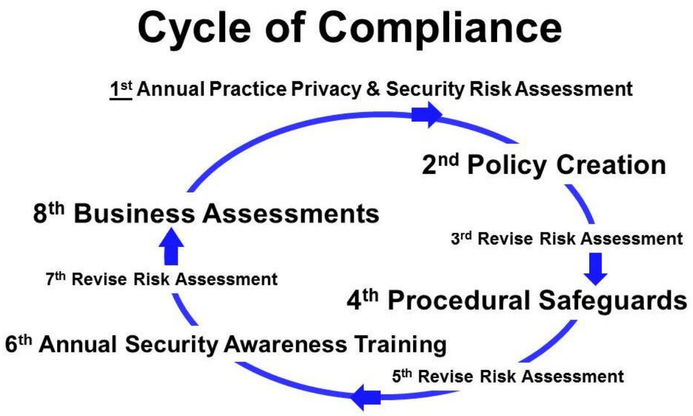
Automated HIPAA Compliance from ACR 2 Solutions

The Health Insurance Portability and Accountability Act (HIPAA) is complex. This is unavoidable, given that the American medical industry is complex. In a typical hospital visit, more than 100 people will see portions of a patient's records, which the HIPAA Privacy and Security rules protect. The ACR 2 Solutions comprehensive HIPAA privacy and security program consists of several modules to assist in achieving HIPAA compliance. The modules can be acquired individually and implemented progressively as outlined below or as cost effective bundles, depending on your organization's needs.

The HIPAA cycle of compliance is shown below. Essentially it is an ongoing process of performing a risk assessment, implementing or improving upon the safeguards for physical, administrative and technical controls, training your organization personnel and repeat. And now, with the recent changes in the law, you must assess the status of those whom you a share protected information. This is why having ACR2's automated tools that track your progress and generate reports to provide easy to use and meaningful guidance are invaluable.

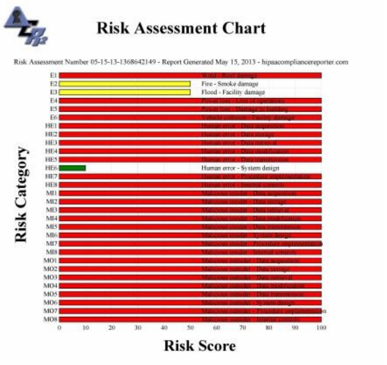

Cycle of Compliance
1st Annual Practice Privacy & Security Risk Assessment
2nd Policy Creation
3rd Revise Risk Assessment
4th Procedural Safeguards
5th Revise Risk Assessment
6th Annual Security Awareness Training
7th Revise Risk Assessment
8th Business Assessments

It is important to understand that it is NOT physically possible to have a perfectly secure system nor is it required. It IS possible to meet the Federal standard of care, in this case HIPAA, by using the methodologies defined by the National Institutes of Standards and Technology (NIST). The Office of Civil Rights (OCR), which performs the HIPAA privacy and security audits for the Federal government, in their risk assessment guidance document calls the NIST risk assessment the "industry standard" for protecting information.

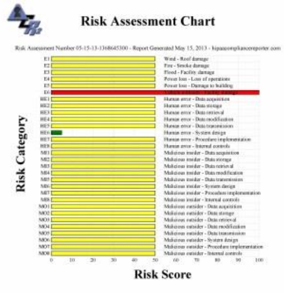
The key NIST document for risk assessment is NIST 800-66 the "Introductory Guide" to HIPAA security. The protocol begins with an automated vulnerability assessment and continues with consideration of policy and procedural safeguards.

1. Initial Risk Assessment – The initial risk assessment consists of two steps.

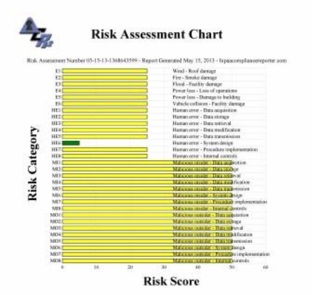
   a. SCAP validated workstation scan – The Security Content Automation Program is sponsored by the Department of Defense and other Federal security agencies. The scanner reviews up to 600 workstation settings in a few minutes. Federal standards are strict. A typical initial workstation scan report is shown at right.

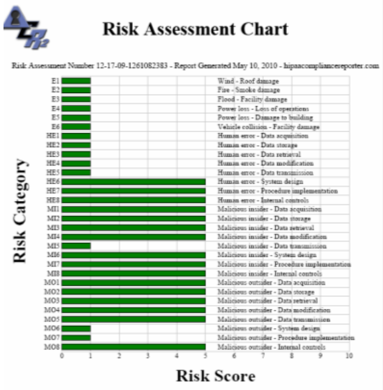


   b. Input of key policy data does a great deal to improve the initial SCAP assessment. Many required policies are easily implemented, and typically are already in place, requiring only writing them down to document. A typical SCAP report modified by adoption of 23 simple policies and procedures is shown at left. A specific site might require few more or a few less.



Following the initial policy inputs, a series of more rigorous policies needs to be developed. ACR 2 Solutions has policy creation solutions for small, medium and large organizations. The extensive program provided by ACR 2 partner Compliance Helper can meet the needs of most organizations. Implementation of the policy package can reduce the risk scores significantly as shown at right. In the example to the right many of the medium risk scores of 50 dropped by half, down to 25 with the implementation of the developed policies.





Over time, the more difficult and demanding safeguards may be implemented. An example is CP-2, the operations contingency plan. This can take months or longer to produce if the facility intends to operate after a fire or other disaster. The risk assessment can be updated at any time, and with diligence eventually will resemble the summary chart shown at left. At which point, new requirements will undoubtedly be published by the Federal government.

While a compliant risk assessment is key to HIPAA security and privacy compliance, there are additional requirements. These include;

2. Annual security awareness training for all staff, as per NIST 800-50 and 800-16. Security Awareness Training is available for small, medium and large organizations.

3. Privacy assessment – NIST 800-53, rev 4 is now in effect with new guidance on privacy objectives and requirements. There is significant (50%) overlap between the privacy assessment and the risk assessment. ACR 2 Solutions offers an option for the HIPAA risk assessment software tool that incorporates privacy assessment as an addendum to the security with separate privacy reporting.

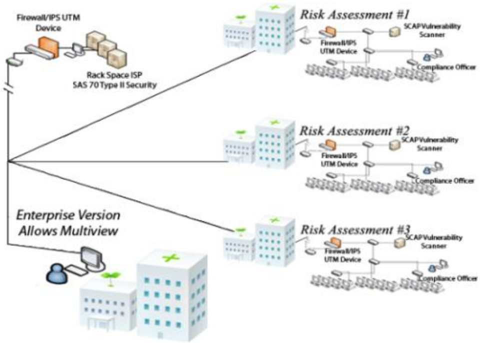
4. Additional options such as business associate agreements and breach risk assessment consulting and reporting. The new requirements for breach reporting are complex. While any breach is an inadvertent release of protected information, not all releases of protected information qualify as breaches. ACR 2 Solutions can provide consulting services to help clients deal with potential breaches of protected information. The difference between a breach and an inadvertent release can be hundreds of thousands of dollars.

5. Business Associate Enterprise Edition and local assessments. - Covered entities are now generally responsible for business associate performance despite contracts. This is a reversal of previous policy.

The practical implication of this change in liability is extreme. If practices are going to consider providing protected information to a business associate they have four choices;

a. Require the business associate to conduct a risk assessment and provide the results to the covered entity, proving satisfactory compliance with the HIPAA Security Rule.
b. Require the business associate to provide HIPAA insurance sufficient to cover the new liability.
c. Accept a major new liability for the practice, potentially up to $1.5 million in fines.
d. Cancel the business associate contract.

As shown at right, ACR 2 Solutions can make it possible for practices to monitor multiple business associates in real time giving you the assurance that you are now charged with obtaining.


Firewall/IPS UTM Device
Rack Space ISP SAS 70 Type II Security
Risk Assessment #1
SCAP Vulnerability Scanner
Firewall/IPS UTM Device
Compliance Officer
Risk Assessment #2
SCAP Vulnerability Scanner
Firewall/IPS UTM Device
Compliance Officer
Enterprise Version Allows Multiview
Risk Assessment #3
SCAP Vulnerability Scanner
Firewall/IPS UTM Device
Compliance Officer