

## Detailed Analysis – Achieving HIPAA Compliance with SkyView Partners' Products

As part of health insurance reform, the U.S. Dept of Health and Human Services introduced a set of security standards for electronic protected health information (EPHI). These requirements are better known as HIPAA – the Health Insurance Portability and Accountability Act. While the HIPAA Security Standards have been in effect for several years, it is not until recently that enforcement of the Security Standards has occurred. Between increased scrutiny from the Federal Trade Commission (FTC – the arm of the U.S. Government that fights Identity Theft) and the Obama administration's investment in healthcare reform more organizations are getting serious about HIPAA compliance.

This document shows how SkyView products can help your organization comply with various requirements of the HIPAA Security Standards.

SkyView product descriptions:

**[Risk Assessor for IBM i and i5/OS](#)** is an IBM i and i5/OS security diagnostic tool that compares your security configuration against security best practices. Risk Assessor examines more than IBM i and i5/OS 100 "risk points" including system values, user profile settings, object level authorities, TCP/IP configuration, and more. Risk Assessor provides easy-to-read reports that allow you to easily determine where your systems' security configuration deviates from security best practices. In addition, Risk Assessor provides a comprehensive analysis guide which includes an explanation of the best practices settings and recommendations for IBM i

**[Policy Minder for IBM i and i5/OS](#)** is an IBM i and i5/OS security compliance tool that compares your systems' current settings against your organization's security policy requirements. Your policy implementation is documented and non-compliant items are identified. Using the FixIt function, non-compliant items can be set back to match policy settings. Policy Minder automates the process of keeping your IBM i and i5/OS security configuration in compliance with your security policy.

### HIPAA Requirement – Section 164.306 – Security standards: General rules:

- Ensure the confidentiality, integrity and availability of all electronic protected health information the covered entity creates, receives maintains or transmits.

**Solution:** Use **Risk Assessor's** recommendations to understand what it means to have confidentiality, integrity and availability on IBM i and i5/OS. Risk Assessor describes the settings required to ensure integrity of the data and operating system as well as confidentiality and availability of data.

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

**Solution:** Once you've determined the settings that are required to implement your security policy, use **Policy Minder** to implement the settings. Then, to ensure your data stays protected use Policy Minder to ensure your systems stay configured according to your security policies.

---

**HIPAA Requirement – Section 164.308 – Administrative safeguards**

Ensure the confidentiality, integrity and availability of all electronic protected health information

*Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

- *Risk analysis* (Required).  
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.

**Solution:** **Risk Assessor** provides a comprehensive, expert and unbiased assessment of over 100 risk points across IBM i and i5/OS.

- *Risk management* (Required).  
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

**Solution:** The key to ensuring that vulnerabilities are kept at bay is to ensure systems remain in compliance with policy requirements. **Policy Minder** automates these compliance checks and provides a method to document, implement and maintain your systems' configuration settings.

- *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends

**Solution:** **Policy Minder's** FixIt function can be used to remove (delete) user profiles from the system. FixIt produces a report which can be used as proof to your auditor that terminated users' profiles are being removed from the system on a timely basis. If large numbers of profiles need to be removed, this can be easily accommodated through the user profile upload function which uploads a list of profiles into Policy Minder from a spreadsheet.

- *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

**Solution:** Use the system value category of **Policy Minder** to check the password system values to ensure they continue to meet your password composition requirements. In addition, the user profile category of Policy Minder can be configured to examine user profile settings to ensure the password expiration interval has not been overridden and that no profiles have a default password.

---

## HIPAA Requirement – Section 164.312 – Technical safeguards

- *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights

**Solution:** Use the library and directory categories in **Policy Minder** to maintain compliance for the privileges each role is to be given to EPHI. Compliance checks will identify when new access has been assigned to files containing EPHI. Policy Minder's FixIt function can be used by administrators to change the settings to match the roles' requirements and provide a documented record of the change.

- *Automatic logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- *Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

**Solution:** Use the system value category of **Policy Minder** to check the time-out and audit control system values to ensure they continue to meet your security policy requirements.

---

## HIPAA Requirements – 164.316 – Policies and procedures and documentation requirements:

- *Standard: Policies and procedures.* Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications ...
- *Standard: Documentation.* Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form
- *Availability.* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

**Solution:** Use Policy Minder to implement your security policy requirements. Use the compliance check feature to maintain the policy implementation. Both policy and compliance check reports can be sent as PDF attachments to appropriate personnel. Or administrators and non-administrators (e.g., auditors) can view the reports through Policy Minder's browser interface.

---

These are just some of the ways SkyView Partners' products can reduce the cost and complexities of maintaining your compliance requirements. For more information on SkyView Partners' solutions, please visit the SkyView Partners website at [www.skyviewpartners.com](http://www.skyviewpartners.com). To find out more about the HIPAA Security Standards, [click here](#).

**Who is SkyView Partners?** SkyView Partners Inc. is a firm specializing in policy-based security compliance management and assessment software as well as security services for IBM i (AS/400 and iSeries) customers.