



## Role-based Access Control Cures Healthcare's IT Security Ill's

*Healthcare IT administrators face the enormous challenge of creating a security system that provides governance over IT systems, minimizes risks of a security breach, and ensures compliance with the law. Healthcare providers and health insurers face more regulations and greater data security risks than ever before. Many are relying on pinSpark's role-based access governance solution to help them overcome this growing challenge of risk reduction and compliance.*





## Introduction

Whether you're in the healthcare or health insurance business, you have a serious responsibility to safeguard IT systems and data. You have to protect them from identity theft, financial fraud, competitive spying, and even employee snooping. You must also provide accountability to regulatory agencies concerned with your organization's compliance with the Healthcare Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX)

The information that must be protected encompasses patient data, insurance data, personnel files, payroll, financial reports, research, and even email. Failing to secure this information can mean huge fines, lawsuits, and the long-term loss of your customers' trust. Yet to provide adequate security, in a manner that is not burdensome to employees can be a major challenge. This becomes more challenging when one considers how highly mobile healthcare workers often are. For example, teaching hospitals get a seasonal influx of medical interns who all require accounts. This produces a backlog of users who need network and application access for their jobs. Some then wind up borrowing co-worker IDs, creating a major security risk

*Pinnacle Security Solution's pinSpark suite is specifically designed to help hospitals and health insurers quickly deliver the appropriate security access permissions required by employees.*

## Driving Risk Reduction, Governance and Compliance with pinSpark

Achieving good IT governance, risk management, and compliance with federal and state regulations are all key concerns of every IT healthcare administrator.

IT administrators at healthcare providers and insurers must implement a system of governance to reduce the risk of security breaches and ensure compliance with government and industry regulations. Creating and enforcing governance is, obviously, a potentially costly issue for organizations with thousands of employees needing access to sensitive data residing in dozens or hundreds of different computer systems

In fact, the cost of compliance, as well as the potential financial loss due to theft of sensitive customer data or corporate intellectual property, can add up to hundreds of thousands of dollars -- even millions -- in

losses to a company. **According to the IT Policy Compliance Group's 2008 Annual Report on IT Governance, Risk and Compliance, companies that have well-defined and automated governance and compliance systems had 96% lower financial losses from the theft of customer and competitive data, and 50% less in annual expenditures for regulatory compliance.** Who you allow to access your IT systems, how much access they have, and how you monitor, audit and automate that access directly translates into financial losses or gains for your organization.

To help IT executives determine how great a risk the organization faces in terms of data access and potential non-compliance, pinSpark provides a comprehensive risk profile, based on which employees, and how many of them, have access to different applications. Administrators can view reports and dashboards and drill down into specific fields to see additional details with pinSpark's Business Intelligence Reporting tool.

To reduce the time and cost of provisioning employees, and to ensure it is done in accordance with the complicated set of policies that many healthcare organizations must enforce, pinSpark also provides automated role creation and management. IT and business managers can quickly create, change, assign, certify, and de-assign roles via a user-friendly interface according to a pre-determined system of governance.

CIOs and CISOs must be able to provide auditors with proof of compliance with federal regulations. pinSpark provides a certification management component that checks and certifies that IT security processes comply with the defined policies.

For example, under SOX, organizations must maintain Separation of Duties – the person who bills a vendor should not be the same one who records a payment from that vendor. Likewise, HIPAA has privacy restrictions that govern access to patient data. pinSpark's Access Certification Compliance component allows administrators to assign separation-of-duty warnings to different roles and will send an alert to the administrator when a separation of duty violation occurs. Depending on the severity of the SOD violation, the alert may take the form of an immediate email or a simply a warning about it included in a monthly report.



## Role Engineering and Modeling with pinSpark

Role creation and management entails grouping various account privileges and access rights into a single profile, or role, such as “New England Customer Service Rep.”. Employees with the same job or, at least, similar IT needs, can be assigned the same role. By the same token, people may have multiple roles, such as “ER medical staff” plus “cardiologist” and thereby given additional privileges. Roles can speed the provisioning process by enabling IT to activate many employee accounts at once, rather than painstaking going through account after account, password by password, employee by employee. A user-centric interface makes role creation especially easy in pinSpark, and provides role suggestions, role assignment, and customizable role-based reports.

## How Does pinSpark Help Achieve Regulatory Compliance?

Pinnacle Security Solution's pinSpark enables hospitals and insurers to achieve compliance, boost productivity, and drive down costs in five key areas:

**Fast Role-Based Provisioning.** Assigning account access by roles enables IT to vastly speed up the process of provisioning employees with network IDs and passwords. Roles can be created for common positions or for whole departments in which workers all use the same applications. IT administrators can modify roles for specific individuals. It can also help IT deal with temporary workers by creating generic temporary roles for common jobs –visiting medical specialists or IT consultants, for example. The roles are pushed out to an automated provisioning or identity and access management system, such as those from CA, IBM, BMC, Novell and others.

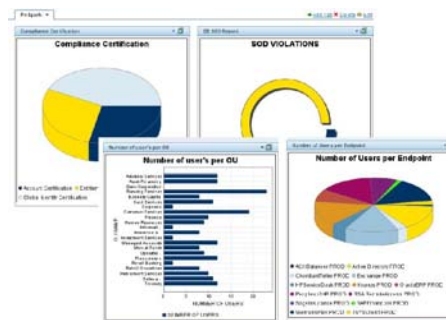
**IT Audit Controls--Monitoring and Access Certification.** pinSpark's Role Management and Usage Monitoring keeps track of who, when, and which applications or systems were accessed. The Risk Management module uses this data to provide intelligent risk reduction, generating reports on potential risks, decayed roles, accumulated access. The Compliance Access Certification function certifies that the company is in compliance with defined policies—including those based on regulatory requirements mandated by HIPAA and SOX.

**Separation of Duties.** The former payroll manager who now works in claims adjudication or billing should not still have access to payroll data. But too often, old access rights follow employees to their new positions. pinSpark prevents this by performing Separation of Duty (SOD) checks based on corporate or specific regulatory policies and then doing the necessary remediation.

**Flexible Delivery Options** The pinSpark is a modular suite and is available as an in-house application or as a Software-as-a-Service (SaaS) subscription. An organization can subscribe to pinSpark's SaaS version, which frees it from the initial capital investment and the ongoing maintenance/support required of in-house solutions.

**Assurance in Real-Time.** When it comes to your organization's critical business information, real-time visibility of user access is key. With easy-to-understand dashboards, pinSpark makes real-time monitoring and management of user access simple.

- Easily view compliance certification status and SOD violations with drill-through capabilities
- Ensure the escalation and remediation of user access threats
- Monitor current user access activities against historic data and trends
- Quickly build, generate and export customized reports based on the data you need now



## Role Management, Governance, and Compliance in One Package

Perhaps the most important value provided by pinSpark's IT access governance and security features is that they are all included in a single, integrated suite. Our enterprise solution provides a single, comprehensive package of: role, risk, policy, certification, and reporting management functions suited for medium to large healthcare provider and payer organizations. It's an all-in-one solution developed to meet the complex IT compliance and security needs of healthcare providers and payers; pinSpark is user-friendly, easy-to-deploy, and an affordable cure for chronic IT security and compliance maladies.



## **About Pinnacle Security Solutions, Inc.**

Headquartered in Alpharetta, Georgia, Pinnacle provides the industry's most comprehensive role-based access governance – pinSpark. pinSpark minimizes the user access risks that threaten large organizations by automating the complex processes that determine who has access to critical business information. This allows companies to reduce user administration cost, mitigate user access risk and enforce regulatory compliance in a way that's simple and cost-effective.

For more information on pinSpark, please visit [www.pinsecure.com](http://www.pinsecure.com). Or call 1-888-504-8472



**Pinnacle Security Solutions, Inc.**  
12600 Deerfield Parkway,  
Suite 100,  
Alpharetta, GA 30004  
[www.pinsecure.com](http://www.pinsecure.com)  
[sales@pinsecure.com](mailto:sales@pinsecure.com)