salesforce platform

Salesforce Shield for Healthcare

How a new level of trust and security makes it possible for the healthcare industry to confidently move to the cloud.

salesforce platform

Contents

salesforce platform

Introduction

There are tremendous changes underway in the healthcare industry. Technological innovations are transforming how care is diagnosed, treated, and managed. Unprecedented regulatory changes are affecting how healthcare is insured and paid, and breakthroughs in life sciences research are making potentially life-changing headlines every week. Consider the Affordable Care Act and outcome-based reimbursement policies which call for the industry to increase its focus on patient satisfaction and care through incentives and mandates.

Consumer expectations are also changing as people expect increased information and digital interaction when it comes to managing their care. There is no doubt that the most successful healthcare companies going forward will be those that best embrace technology; those that unlock data buried in legacy systems and electronic health records (EHRs) to improve patient relationships, care, and medical outcomes; those that effectively utilize new data analytics techniques to drive new innovations and treatments; and those that securely leverage cloud computing and mobility.

According to the "Salesforce 2015 State of the Connected Patient" report, patients are increasingly embracing new communication channels and ways to review their health data via email, text, and web portals.

76% of patients are confident that their doctors are sharing health records between them for a holistic view of their health.

Of course, cloud and digital connectivity must be embraced securely on systems people trust. Some healthcare companies are hesitant to utilize the opportunities technology provides because of regulatory compliance and cybersecurity concerns. Those fears, however, should be allayed. As you'll see in this e-book, improved compliance, security, and governance features – such as those found within Salesforce and its premium, built-in Shield security services – provide the capabilities healthcare entities need to achieve faster feedback between doctors and patients, more accurate and swifter workflow for insurers, and improved research, development, and commercial opportunities for life sciences companies.

salesforce platform

CHAPTER 1

Increase of Cybersecurity Risks and Regulatory Demands in Healthcare

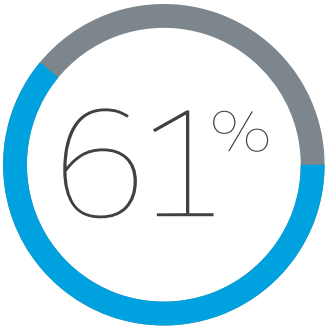
Technology wields big potential for improving the management of our health. Both healthcare providers and insurance companies have the opportunity to revolutionize healthcare in significant new ways, thanks to digital technology. From wearables that encourage users to take extra steps throughout the day, to mobile apps that instantly share patients' data, all make the future of healthcare bright.

Mobile devices and apps top the list of technologies that patients would like to see included in their healthcare experiences. Beyond mobile tools, 61% of insured Millennials are interested in 3D printing devices to aid their health, according to the "Salesforce 2015 State of the Connected Patient" report.

However, realizing this vision is not easy, and few industries face the same risks and surveillance as healthcare does. The impacts of data breaches can be devastating to individual privacy if medical history is leaked.

Medical device and pharmaceutical companies can incur hefty regulatory fines – up to $50,000 per violation or per record under the Health Insurance Portability and Accountability Act (HIPAA) – for the loss of stolen intellectual property.

Insurance companies also need to be on constant guard to protect sensitive data and to fight potential medical identity theft to avoid damages to brand trust and reputation.



of insured Millennials are interested in 3D printing devices to aid their health.

"Salesforce 2015 State of the Connected Patient"

CHAPTER 2

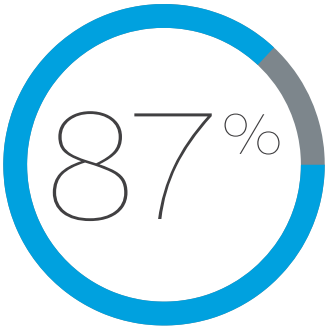
Security and Compliance Challenges in Healthcare

Challenges for Healthcare Providers

When it comes to regulations to protect consumer health information, providers are on the front lines. This is in part driven by increasing cybersecurity risks around consumer health data. Provider health data breaches that expose personal health information (PHI) are becoming too common. According to the Department of Health and Human Services, 31.7 million Americans have been affected by data breaches that have leaked PHI – approximately 10% of the population.

Regardless of whether non-compliance leads to actual security breaches, the costs of regulatory fines and reputational damage may become so high that strong security and compliance could well prove to be a competitive advantage for organizations that can effectively avoid them. This is especially true for companies that give patients a choice of healthcare options, such as selecting a clinic or a medical device.

To mitigate such risks, healthcare providers need to ensure that their systems are securely built, managed, and maintained. They have to deploy and manage hardened applications, identity and access management software, and intrusion detection and prevention systems to ensure a higher level of security and compliance. Healthcare companies are taking the necessary steps to secure their systems. According to the "2015 HIMSS Cybersecurity Survey," 87% of respondents said that information security has increased as a business priority, as they work on ways to improve network security, endpoint protection, data loss prevention, disaster recovery, and information technology continuity.



of respondents said that information security has increased as a business priority.

Healthcare Information and Management Systems Society: "2015 HIMSS Cybersecurity Survey"

salesforce platform

Challenges for Health Insurance Companies

Insurance companies hold a tremendous amount of patient data. As is the case with providers, this data is subject to strict regulations to ensure protection and integrity of sensitive member information such as PHI. Compliance standards set forth by HIPAA demand that insurers be more efficient, publicly disclose exposed medical PHI, and comply with all HIPAA regulations for handling patient data. On the other hand, the number and severity of attacks to insurers has never been higher. According to the FBI, cybercriminals can sell healthcare information for $50 a record – a figure much higher than credit card or banking data.

The connected insurance member creates many opportunities to improve customer care by giving insurers more reliable and steady data regarding patient health. Additionally, thanks to mobile and web apps, insurers can engage their members directly by helping them manage their wellness, pull insurance card information, find providers, and create an emergency patient profile. But all of this data must be stored and handled securely, on technology platforms people can trust.

Just as is the case with providers, health insurers face tight technology budgets and resources coupled with a rising cybersecurity skills gap, which makes it challenging for health insurance organizations to obtain the resources and staff they need to keep their business-technology systems secure.

salesforce platform

Challenges for Medical Device and Pharmaceutical Companies

Few enterprises hold more valuable data than the intellectual property of pharmaceutical companies and medical device makers. A single case of mishandling clinical trial data, if not tracked, disclosed, and corrected in a timely manner, could send the company's stock value plummeting, jeopardizing years of effort and research.

Pharmaceutical companies must address the high risk of security threats against their intellectual property from internal and external users. Additionally, pharmaceutical companies are subject to extensive compliance requirements for trial information, and how that information is accessed and changed. They are required to keep and constantly audit the integrity and security of a single trial's data for up to 10 years.

To manage risks and address compliance requirements, life sciences companies spend billions annually to protect their data in on-premises and cloud environments.

And, just as is the case with providers and insurers, life sciences firms face significant challenges finding the right talent to secure their data. Device makers have the additional challenge of finding the expertise they need to build secure devices and the associated software and application programming interfaces (APIs).

salesforce platform

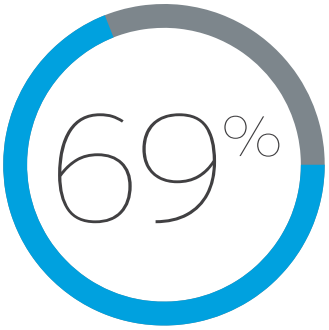
CHAPTER 3

Addressing Patient Data Security with a Trusted Cloud

Over the past five years, healthcare organizations have come to embrace the cloud. In fact, 87.5% of Healthcare providers are comfortable with the cloud, according to a study by IDC Health Insights in 2016.

According to another study, "What's Next in Cloud Security" by Group 451 (March 2016), 69% of survey respondents said that they plan to move more regulated data to the cloud in 2016. This is made possible by their improved ability to meet regulatory and internal requirements to manage risks to sensitive data, through features such as end-user-activity monitoring.

The Salesforce platform, including Health Cloud, natively provides healthcare companies with robust security features at the infrastructure, network, and application layers. Additionally, healthcare companies can safeguard their sensitive apps and data with granular controls including two-factor authentication, role-based user access policies, and record and field-level encryption. Healthcare companies can create trusted collaborative environments where practitioners, team members, and partners can work together.



of survey respondents said that they plan to move more regulated data to the cloud in 2016.
"What's Next in Cloud Security" by 451 Research

salesforce platform

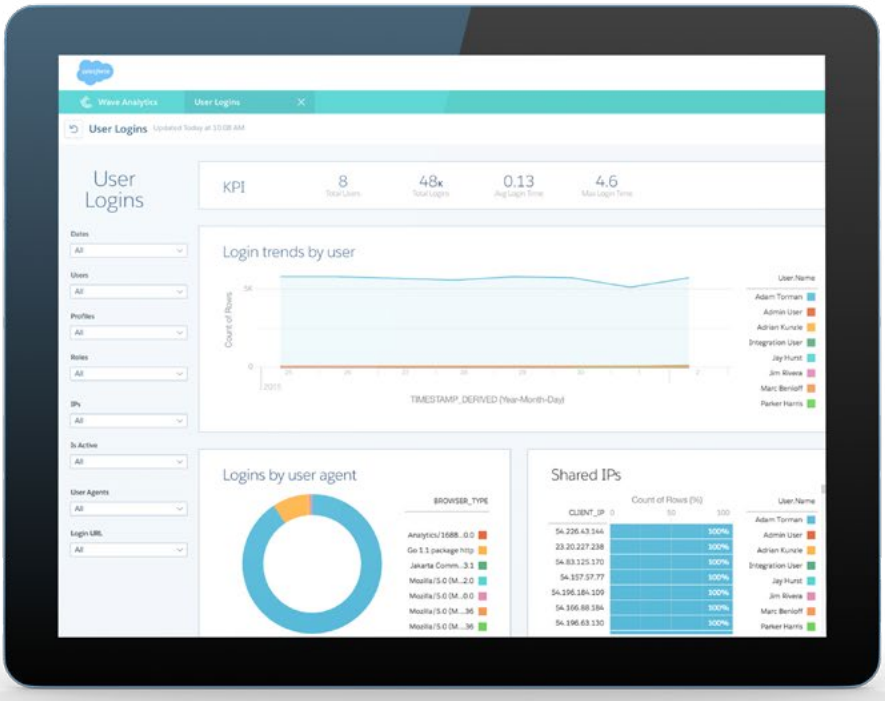
Monitor, Prevent, Protect, and Audit Sensitive Data in the Cloud

For customers who need additional levels of security, compliance, and governance, such as those in healthcare, we offer Salesforce Shield, a premium set of integrated services built natively into the Salesforce platform. Salesforce Shield provides customers with granular visibility into who accessed the data and what they did with it; the ability to encrypt sensitive data (such as PHI at rest) without losing the data's business functionality; and the ability to automate HIPAA audits with data retention and retrieval policies.

MONITORING

Identify actionable security and user insights.

Event Monitoring provides healthcare companies with comprehensive visibility into their Salesforce apps, so IT, security, and audit teams always know exactly who is accessing what data, and from where. Shield also alerts teams of any abnormal usage patterns that need looking into. Event Monitoring makes it easy for detailed activity monitoring of users and data, allowing administrators to see when someone prints a page or list view, accesses a particular patient record, changes ownership, refreshes a list, or even exports sensitive patient data.

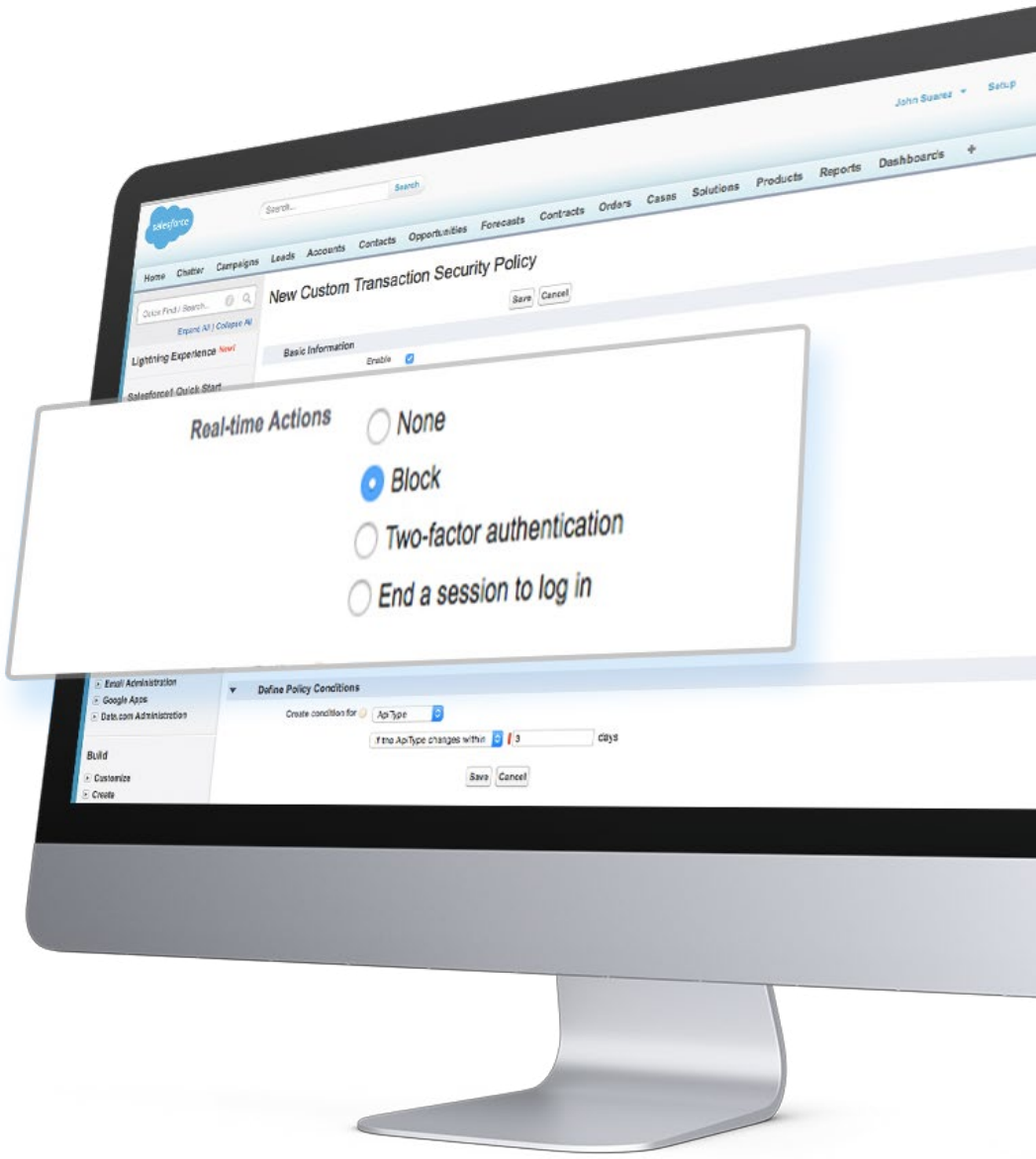


salesforce platform

PREVENTING

Mitigate risks coming from internal users.

The Transaction Security service, part of Event Monitoring, makes it possible to reduce some of the risks associated with compromised user accounts, malicious attacks, and honest mistakes that violate policy. With Transaction Security, healthcare companies can create custom security policies for their organizations. For instance, should access to Salesforce data be attempted from an unauthorized device, or if records are being acted upon in an unsanctioned way, the suspicious event can be evaluated or blocked, or an admin can be alerted.

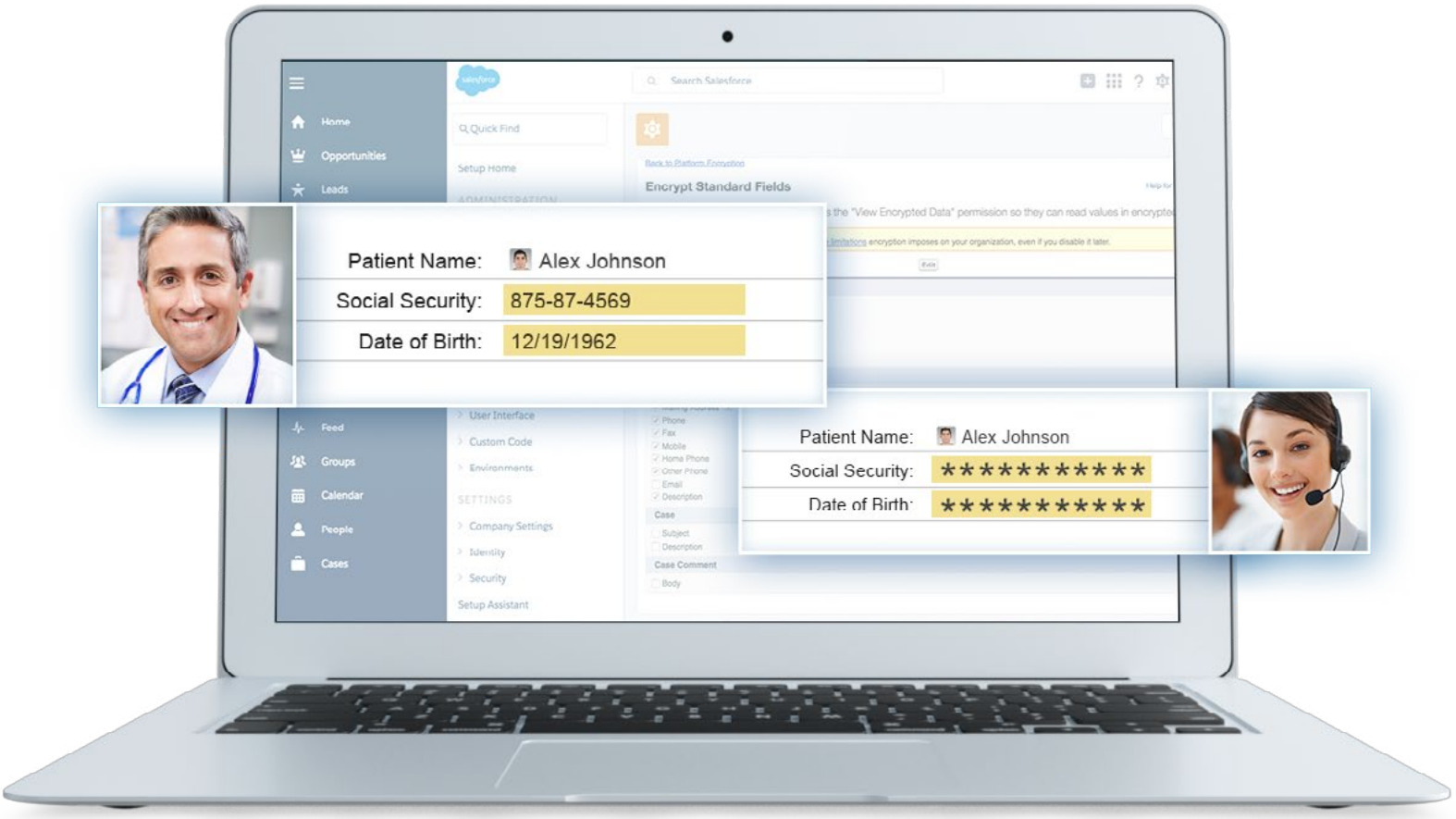


PROTECTING

Strongly encrypt data without losing usability.

Salesforce Shield's Platform Encryption service makes it easy to encrypt data at rest by using strong certified standards while making every field "encryption-aware," so that features that use encrypted fields – such as workflows, search, and more – still function. So there's no reason to sacrifice usability for security. This is because data at rest is encrypted at the metadata layer, making it possible for application functionality to remain intact.

Platform Encryption can be set up with a simple click on the application UI and uses a sophisticated, FIPS 140-2-certified, HSM-based, key management architecture. The key management approach gives customers complete control over the lifecycle of encryption keys.



salesforce platform

AUDITING

Easily manage compliance and security audits.

HIPAA audits can be daunting, especially for your data in the cloud. Salesforce Shield's Field Audit Trail provides security analysts and auditors with the tools they need to rewind and view historic user and data activity. They can easily witness the state and value of data at any time by using simple queries against that data.

Most importantly, healthcare companies may want to retain regulated data only as long as they have to, because excess retention may become a liability. Field Audit Trail lets companies set up policies so that specific data can be automatically archived or discarded after a specific period of time.

Field Audit Trail provides up to 10 years of history for up to 60 fields per object.

CHAPTER 4

Salesforce Shield: Use Cases in Healthcare

Event Monitoring

PROVIDERS

With Event Monitoring, healthcare providers can see what data the medical staff is accessing, when they accessed it, and where they accessed it from. Multiple members of staff in a provider network might be interacting with a single record, and comprehensive view to usage behavior can expose individual security warning signs (e.g., a suspicious download of a VIP's patient data).

INSURERS

Event Monitoring helps insurance companies keep sensitive member data secure from internal threats. For example if a service agent tries to access too many member accounts, or if accounts are accessed from a strange IP address, Event Monitoring identifies the suspect user actions. And, if there was a suspected data breach four weeks ago, an administrator can turn to Event Monitoring to find out if any non-authorized people accessed PHI data.

PHARMACEUTICAL AND MEDICAL DEVICE COMPANIES

There's nothing more valuable and regulated in life sciences than intellectual property and clinical research data. Event Monitoring allows pharmaceutical and medical device makers to know when clinical trial data is accessed, who accessed it, where it was accessed from, and when it was accessed. Event Monitoring also tracks events in which data is shared, and monitors logins and views of trial data from suspicious geographical regions.

Transaction Security

PROVIDERS

Healthcare providers can configure Salesforce Shield to notify security teams or administrators if a non-authorized employee purposely or inadvertently attempts to print a view of patient records with medical history data. Salesforce Shield also allows organizations to block certain types of activities as they happen and to require additional authentication (such as touch ID) for certain events.

INSURERS

When someone uses an unknown device in an attempt to log in or download insurance member data (including social security numbers and insurance IDs), Salesforce Shield comes to the rescue by stopping the activity and notifying the appropriate team members.

PHARMACEUTICAL AND MEDICAL DEVICE COMPANIES

Administrators can configure Salesforce Shield to identify and stop data exfiltration by internal users. For example, if, for an unknown reason, a trusted insider at a medical device or pharmaceutical company attempts to download an unusually high number of records with sensitive intellectual property or trial data, Salesforce Shield stops the activity and alerts the company's internal security team.

Field Audit Trail

PROVIDERS

Healthcare providers can easily pinpoint mistakes in patient records with Salesforce Shield's Field Audit Trail. For example, during an HIPAA audit, an audit trail identified a member's health data as inaccurate and showed that six years prior, a nurse had mistakenly changed the doctor's note from "negative" to "positive." The auditor was able to easily retrieve and review the record, without going through piles of papers or folders of spreadsheets.

INSURERS

Field Audit Trail can help healthcare insurance companies keep track of activities by external organizations. For example, a company decided to audit the activity of all of its third-party vendors to see if they made any changes to records that didn't pertain to projects they were working on. Field Audit Trail reported that there weren't any significant changes except for a few grammar updates during the two-year period that was examined.

PHARMACEUTICAL AND MEDICAL DEVICE COMPANIES

When the Securities and Exchange Commission (SEC) comes calling regarding changes in stock pricing, pharmaceutical and medical device companies can turn to Field Audit Trail. For example, when a biopharmaceutical company's stock price was suspiciously volatile prior to a big drug announcement, the SEC suspected insider trading of information ahead of a clinical trial. In an audit with the SEC, Field Audit Trail showed the regulators that there was no indication of suspicious manipulation of data within the pharmaceutical company during the time frame in question.

Platform Encryption

PROVIDERS

Platform Encryption is designed to retain critical app functionality – like search, workflow, and validation rules – while encrypting data at rest. For example, a provider used a third-party gateway solution to encrypt sensitive patient data (PHI) within Salesforce as an additional level of security. As a result, the company's workflow rules for notifying a doctor via email about a new patient enrollment didn't work properly because the email included the patient's date of birth. Platform Encryption allows providers to encrypt date-of-birth data at rest for an extra level of compliance, while still allowing workflow rules to function properly.

INSURERS

With Platform Encryption, health insurance companies can balance their data security needs with their business needs. For example, an insurance company had contractual obligations with some of the employers they serve – they would not store members' personal data in clear text in the cloud, no matter how secure their provider's data center was. To meet this requirement, the insurance company implemented Platform Encryption to protect sensitive data within Salesforce, while continuing to capitalize on the growth and efficiency of service provided by the Salesforce cloud.

PHARMACEUTICAL AND MEDICAL DEVICE COMPANIES

Encrypting data at rest is a point-and-click process with Salesforce Shield's Platform Encryption service. For example, a pharma company started to keep records of, and collaborate on, multiple new clinical trials within the Salesforce platform. They created a lot of custom fields to store sensitive trial data, then realized they needed to encrypt each field at rest as an extra level of protection. Instead of involving all the cryptographers, developers, and other technical and security professionals, they asked their Salesforce admin to apply encryption-at-rest to those fields – which he did simply by clicking a checkbox for each field.

Conclusion

There's no doubt that patient relationships are quickly transforming as regulations change and more people demand increased digital interaction when it comes to how they receive care. Healthcare companies need to deliver these capabilities to their patients, customers, and partners in ways that unlock data buried in legacy systems – in a trusted, secure way. Salesforce Shield and the Salesforce trusted cloud make it possible for healthcare companies to strengthen compliance and improve security, while allowing them to leverage valuable business functionality across all key digital channels.

Is Salesforce Shield right for your business?

LEARN MORE

Chat with an expert – call us at 1-844-463-0828.

CONTACT US