A Guide to Getting Started with Healthcare DevSecOps in Salesforce

Ripping the Band-Aid

autorabit

Introduction

Healthcare companies have a bit of a balancing act on their hands at all times—not only are they responsible for the well-being of those that seek their services, but they are also responsible for protecting the sensitive data of these individuals. HIPAA is a government regulation that outlines specific requirements for how electronic protected health information (e-PHI) needs to be handled. As stated on HHS.gov, healthcare companies are required to:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

A Salesforce DevSecOps pipeline is a great way to introduce new applications and updates to address these needs as they continue to emerge and evolve. But for healthcare companies that don't currently utilize a DevSecOps approach, getting started might be a little intimidating. However, the need for strong systems and data security is non-negotiable.

Here are 7 things healthcare companies need to keep in mind when establishing their Salesforce DevSecOps strategy:

1. Examine Current Processes
2. Identify Goals
3. Consider Automation
4. Establish Organizational Structure
5. Address Data Governance
6. Maintain Focus on Data Security
7. Plan for Worst-Case Scenarios

01

Examine Current Processes

Healthcare companies likely have an existing system for developing updates and applications to address their technological needs. This could include something as simple as patching their internal systems and going all the way to creating applications that are to be used directly by their customers.

It will be impossible to find the best way to improve these processes if you don't take the time to analyze them. What works? What needs to be refined? Are there opportunities to cut superfluous functions?

The information gathered in this stage will set the course for your healthcare company's approach to implementing Salesforce DevSecOps tools and strategies moving forward.

FIRST STEPS

The best resource you have to learn how things are currently going is to speak with your team members. This includes those in management positions, developers, and even team members that make use of the products once they are released.

Each group can provide its insights into processes that are operating smoothly and those that need improvement. Pay attention to areas that require large amounts of time to perform repetitive tasks—these are great opportunities to utilize automation, which we'll discuss a little later.

Compile the insights you've gained from these interviews to put together recommendations and areas of interest. Keep these opportunities for improvement in mind as you enter the next stages of the Salesforce DevSecOps planning process.

> *CodeScan really has saved us a lot of time in doing code reviews. We had the opportunity to let our developers install it in the VS Code IDE and CodeScan did everything else."*
>
> SHESHANT K.

02

Identify Goals

> *"AutoRABIT has helped us add a lot of automation to our software development lifecycle. I highly recommend it!"*
>
> FORREST COOK

We've mentioned the essentiality of regulatory compliance for healthcare companies. And while this needs to be a major concern when planning out your Salesforce DevSecOps strategy, it won't be the only one.

Taking the time to define a set of goals will align your efforts and direct your decisions as you put systems in place.

DevSecOps is known to provide a series of benefits like higher release velocity, improved data security, and stronger products. However, the way this plays out will be different for every instance. What factors and results are important to your healthcare company in particular?

FIRST STEPS

Work with representatives from various departments such as development, security, operations, and even customer success to put together a list of goals for your DevSecOps pipeline. The insights you gain from these conversations will grow deeper and more informative as the pool of opinions grows larger.

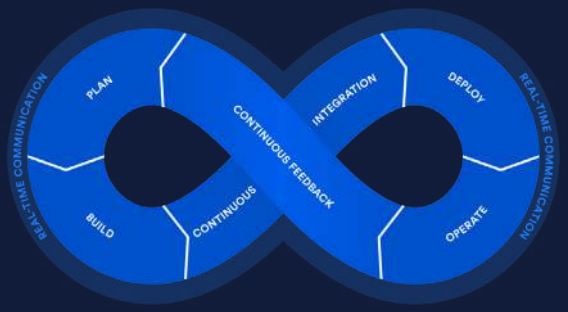
This could include items such as more releases per year, faster production cycles, heightened code quality, increased data security, and more. Organize your goals by importance.

Consider these goals along with the examination of current processes to see which items need the most work. There's a chance your current system is already accomplishing some of your goals, which is great. Carry those processes over to your Salesforce DevSecOps strategy as long as they don't interfere with other goals.

This list can be used moving forward to assess the success of your new practices. And if your goals aren't being met, it will be easier to find ways to adjust your strategy to better address them.

03

Consider Automation



Keeping costs low and productivity high is a significant goal of Salesforce DevSecOps. And a major way this is accomplished is to utilize automated tools as much as possible.

Processes such as code reviews can be incredibly time-consuming, labor-intensive, and repetitive. This leads to mistakes that can have wide-ranging impacts not only on the quality and the security of a release. Healthcare companies simply can't afford to leave themselves vulnerable to these types of mistakes.

Automation solves these problems by taking these repetitive and error-prone tasks out of the hands of your team members, allowing them to focus on more important aspects of the DevSecOps pipeline.

FIRST STEPS

Weigh your examination of current processes against your goals to find areas in need of assistance. Then, take some time to research the types of automation available to your team and highlight those that best address your goals.

Here are a few examples of Salesforce DevSecOps automation that would benefit just about every healthcare company.

- **Static Code Analysis:** Automates the code review process to provide total visibility into code health from the moment it's written.
- **CI/CD:** Integrates code from multiple sources into a single source of truth and packages it for deployment into production.
- **Data Loader:** Imports and exports files, metadata, and dependencies between Salesforce orgs to enable teams to build and test across the release cycle.
- **Data Backup & Recovery:** Schedule repeated snapshots of your Salesforce environment to be stored to assist with recovery from a data loss event.

Establish Organizational Structure

DevSecOps combines the efforts of three teams—development, data security, and operations—to work toward a singular goal: secure and high-quality updates and applications. The number of team members can grow large so everyone needs to know their role, whom they report to, and their expected duties.

A team member that doesn't know where to go for information or doesn't understand their role will be a drag on overall productivity. This can even lead to errors that have a negative impact on the update or application itself. A little planning goes a long way to avoid this and offers concrete benefits to healthcare companies.

FIRST STEPS

You already have a plan in place for what you hope to accomplish and what automated tools will be utilized to help work toward these goals. Now it's time to build your team around these processes. Build out a hierarchy of roles that positions your team members to best address the various aspects of the Salesforce DevSecOps pipeline.

Clearly define the roles and expectations. Consider each stage of the development lifecycle and the people you'll need to fulfill the duties:

- Planning
- Development
- Testing
- Integration
- Deployment
- Monitoring

Encourage collaboration and open communication between the various teams working in each DevSecOps stage. It's important for team members to also understand the roles of those around them so there is no confusion about where to go when someone has a question.

05

Address Data Governance

Now that your systems are almost in place, you need to consider the data and files you will be using to process your information. A quality pool of data is essential to proper functionality, accurate reporting, and informed decisions.

Data governance refers to the proper handling of your Salesforce data through intentional principles and practices. Internal standards and categorization are upheld by dedicated team members within a variety of departments to ensure important system data isn't lost or mishandled. And when it comes to healthcare companies and the applicable regulations, proper handling of data is non-negotiable.

FIRST STEPS

The executive team should meet to define a data governance strategy and put together a mission statement. This will include defining the goals of your program as well as the framework that will be used to address proper data handling.

Your data governance framework outlines the roles, processes, and expectations for your team. This is essential to making your data governance efforts beneficial to your Salesforce DevSecOps pipeline.

Identify members of your team to address system data. Managers will be needed to oversee operations, but these roles will need to be assigned within each department:

- **Data Owners:** Monitors the quality of data as it moves throughout company systems. Works to ensure the data is handled according to company standards.
- **Data Stewards:** Produces reports after analyzing the available data.
- **Data Users:** Interprets the collected data according to company guidelines.

A strong data governance strategy helps your DevSecOps teams by providing high-quality information and insights to direct their operations.

> *"AutoRABIT is a well-blended suite of solutions that complemented our Salesforce Release Management efforts."*
>
> JAKEER H.

06

Maintain Focus on Data Security

The difference between DevOps and DevSecOps is that the latter places stronger importance on data security. And as we discussed with government regulations, data security needs to be a constant focus for healthcare companies.

Data security considerations need to be injected into every stage of the development lifecycle. This helps ensure vulnerabilities don't slip between the cracks and show themselves in live environments.

There are simply too many threats to the data security of a healthcare company to be completely confident. Instituting multiple layers of security gives you the best chance of remaining secure and compliant.

FIRST STEPS

As with most aspects of Salesforce DevSecOps, proper communication is a major part of properly addressing data security. Facilitating collaboration between departments and stages of the development lifecycle minimizes simple mistakes that can blossom into data security threats.

We've discussed how automation can help speed along processes and heighten security, but it can also support a data security strategy. Static code analysis, for instance, provides alerts the moment an error is introduced into the code repository. This keeps it from creating errors that open vulnerabilities in applications and updates.

Cybercriminals get a lot of attention for the threat they pose to healthcare companies, and for good reason. However, it's important to remember that something as simple as a team member error can also result in costly and disastrous data loss events.

Plan for Worst-Case Scenarios

But even with strong data security measures in place, there is always the potential for a cyberattack, data breach, or data loss event. Part of a healthcare company remaining compliant is having emergency systems in place to minimize the consequences of this type of occurrence.

Being caught without a failsafe would be an absolute disaster. So while it might be unpleasant to think about worst-case scenarios, it is essential to have procedures and protocols in place to get your system back to operations and protect sensitive data.

FIRST STEPS

Backup snapshots of your system and customer data need to be continually updated and stored. This information will be critical to getting your system back online after a data loss event. Every minute your system experiences an outage costs money and potentially compromises sensitive information. This is why you must also have a data recovery tool to reinstitute data from the backup repository.

A quality data backup and recovery tool will also offer the ability to encrypt sensitive data, further protecting it from exposure even in the case of a data breach.

Put together a disaster plan and frequently revisit it to make sure it is current. This is a non-negotiable aspect of a full data security plan which will also impact your ability to remain compliant.

Conclusion

Salesforce DevSecOps has a lot to offer healthcare companies. The speed, quality, and customizability of a DevSecOps pipeline cater to the unique needs of the various aspects of the healthcare industry. And beyond that, the data security benefits directly impact the strict needs of regulatory compliance related to handling sensitive information.

Getting started with Salesforce DevSecOps doesn't have to be intimidating—all you need is some thoughtful planning. Following the steps outlined in this ebook will offer a path toward secure and reliable updates and applications.

It's important to remember that Salesforce DevSecOps is a journey, not a destination. There will need to be tweaks and refinements. Your needs and expectations are going to evolve. The tools and procedures utilized in your DevSecOps pipeline will need to evolve along with them.

Healthcare companies serve a crucial role in society. Salesforce DevSecOps can help make this difficult job a little easier.

WHO WE ARE

autorabit

AutoRABIT is a Continuous Delivery suite for SaaS platforms. We automate and accelerate the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides static code analysis, automated metadata deployment, version control, advanced data loading, orgs and sandbox management, test automation, and reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, and offers disaster recovery, and endpoint data protection on the Cloud. CodeScan provides full visibility into code health from the first line written through final deployment into production. Record Migrator provides automatic bundling of all feature dependencies for Salesforce managed packages and deployment of templates ensuring fast, efficient, and seamless releases.

VISIT US TODAY TO LEARN MORE

www.autorabit.com

★★★★☆ G2 CROWD