

## IT Security Compliance Engineer

Love small teams? Want to do important and challenging work? Wildflower Health is seeking a self-starting, analytical and problem-solving IT Security Compliance Engineer.

### About Wildflower Health

Wildflower Health offers a healthcare solution that connects women and families to better care by breaking down silos among providers, payer and best-in-class partners. We deliver personalized experiences that simplify the healthcare journey for families with a combination of human touch and digital tools. Our model fuels the transition from fee-for-service to value based care.

The company's products support families during every life stage, from preconception and pregnancy, through pediatrics and adult health, supporting common episodes of care over time. Wildflower Health's software is highly configurable for health enterprise clients to reflect their health services and benefits, creating a highly personalized experience for application users. The company's applications are offered to consumers worldwide by leading health plans, hospitals and health systems, and employers.

### About the role

Wildflower Health is looking for a candidate to serve as its IT Security Compliance Engineer to facilitate, manage, and maintain its information systems, compliance and security posture. This position is perfect for someone with 3-7 years of experience in compliance and information systems security, operations, or healthcare regulations, especially for those seeking to develop a strong background in all of the above.

The primary responsibility will be managing and executing Wildflower's comprehensive information systems security and compliance plans to minimize risk in technical capacities, including but not limited to owning and managing operations of the information systems to ensure alignment with the internal security and compliance procedures, such as performing policy compliance, audit logging, and virus checking. The ideal candidate has technical, hands-on experience reviewing logs and remediating vulnerabilities.

**Bonus points** for any IT infrastructure support experience.

#### ❖ Daily tasks

##### Compliance

- Provide evidence for internal Risk and and Compliance tool

- Manage both manual and automated technical processes to adhere to current IT Security policies
  - Manage anti-virus, DLP, password management, patch/updates on end users' computers and IT infrastructure, etc.
- Maintain and manage security processes tied to critical security and compliance controls
  - Review access logs, perform user disables upon termination, track and manage access escalations/modifications, etc.
- Perform risk analysis and provide prioritized remediation recommendations to engineering teams
- Perform internal risk assessments
- Assist in the development, maintenance, and revision of policies, standards, procedures, and guidelines of security programs

#### IT and Security

- Provide IT administrative support (e.g. securing laptops/servers)
- Build out IT Security workflows and policies (i.e. monitoring and patching vulnerabilities via logs)
- Monitor, manage and remediate application vulnerability scanning services and associated risk
- Build proactive security automations aimed at decreasing manual remediation work
- Advise, manage and enhance current monitoring processes for security tooling and data
- Support and maintain critical security infrastructure
- Help improve our detection capabilities by executing on existing engineering projects and tooling improvements
- Monitor incidents as they arise with systems/products, translate engineering team response and action into incident reports and remediate incidents
- Review and assess vendor security assessments

#### ❖ To be successful, we are looking for:

- 3 - 7 years of IT Security Compliance experience
- Hands on experience with cloud platforms/technologies, such as AWS
- Strong understanding of Linux, Mac OS, and Windows desktops and servers
- Ability to understand and articulate security risks, as well as propose solutions and/or mitigate controls
- Attention to detail and organization
- Ability to thrive in a fast-paced environment, learn new skills proactively, support other team members, and work independently
- Ability to accurately prioritize and timely execute tasks

- Dedicated to maintaining documentation
- Superior communication skills (presentation, written, and verbal) to effectively interact with all levels of professional staff. Ability to explain complex concepts simply
- Strong problem solving and analytical skills
- Work collaboratively with cross-functional partners to develop creative solutions to complex challenges
- Understanding of organizational IT policies and compliance to them
- An analytical mind for problem solving, abstract thought, and offensive security tactics.
- Proactive identification of areas of improvement and suggest projects to improve controls while maintaining a positive team atmosphere

❖ Preferred:

- Bachelor's degree in Information Technology, Computer Science, or other technology-related discipline.
- Understanding and experience with HITRUST framework