How Secure is Your COVID-19 Screening Process?

While life is slowly regaining a sense of normalcy as Covid-19 related precautions begin to ease up across the United States, businesses are starting to implement new screening processes to help remain open and curb the virus's spread. While these processes may fall within the CDC's recommended guidelines for contact tracing and can help keep cases low, participating companies may have unknowingly set themselves up for legal and PR difficulties down the road through their handling of HIPAA regulated information.

Many companies are collecting Personally Identifiable Health Information (PHI), such as temperature and previous Covid-19 exposure, during at-the-door screenings without knowing the laws and requirements surrounding this data. Proper protection of this information is paramount, as failing to do so can lead to fines from the Department of Health and Human Services (HHS) ranging anywhere from 100 to 50,000 USD (Cohen, 2019). Also, the unwarranted use or release of this information can seriously tarnish a company's reputation.

Why Protecting Personal Health Information (PHI) Is So Important

Both the release of and failure to protect Personally Identifiable Health Information violate the HIPAA Privacy Rule, a subset of the Health Insurance Portability and Accountability Act (HIPAA) signed into law by President Clinton in 1996. Proper compliance with HIPAA requires access controls for all Personally Identifiable Health Information, transparent employee vetting and accountability procedures, and policies outlining who has access to this information and when. Data this sensitive is best safeguarded digitally, where access controls are easy to implement. However, if a cloud-based solution is in use, the host company must follow similar compliance guidelines.

Any solution used should encrypt data both in transit and during storage and secure it through role and group-based policies that allow access to permitted individuals. Any data hosts involved should also have procedures in place for the unlikely event of a data breach that can remediate the effects and notify affected parties promptly.

How Electronic Content Management (ECM) Can Help

While HIPAA compliance can be complicated and timely to implement correctly, the right ECM solution can make securing sensitive data relatively painless. Square 9's new Return to Work Essentials solution, for example, creates a screening environment that eliminates physical contact, provides the necessary controls to access sensitive information, and stores the data in a HIPAA compliant environment to help protect against fines and breaches. Square 9 Softworks is HIPAA, SOC 1, and SOC 2 compliant, allowing you to focus on what's important.

For more information on this and other useful business, solutions visit www.Square-9.com.

Marketing Communications Specialist **Alexa Pritchard** is the dynamic voice behind Square 9 Softworks. Delivering highly effective messaging across reseller channels, end user communities and outside agencies, Pritchard develops, drives and executes communication plans that effectively support Square 9's overall marketing goals and objectives. To learn more visit www.square-9.com.