S19 SAFE19

COVID-19 CLEARINGHOUSE

IntelliCorp
a Cisive company

FREQUENTLY ASKED QUESTIONS

WHAT IS SAFE19?

Through IntelliCorp's parent company, Cisive, our SAFE19 solution is a secure, paperless, central repository specifically designed to handle the uploading, validation, and compliance reporting on COVID-19 test and immunization data.

WHO WILL HAVE ACCESS TO THE DATABASE?

Government Entities, Healthcare Facilities, Employers and Schools will have access to the database.

HOW DO PATIENTS ENSURE THEIR PRIVACY?

Cisive's SAFE19 meets HIPAA and FCRA privacy standards. SAFE19 will not disclose any personal identifiable information to the end user. Participants will also be signing a consent for the results of the test to be used for their credential.

HOW DO YOU DETERMINE THE CRITERIA FOR GIVING SOMEONE A "SAFE19" CREDENTIAL?

Criteria will be designed by the client based on what they are trying to achieve. We will only be allowing FDA approved tests to be used. We expect this to be a very fluid and dynamic environment and very likely that there may be changes by the FDA as more testing becomes available. We are also expecting the introduction of vaccinations when they are available and those records can be verified and factored into the SAFE19 approval standards based on the clients unique requirements.

WHAT HAPPENS IF NO RECORD IS FOUND?

The applicant will have the option to upload documentation if they have been tested. The applicant will also be given the option to perform a titers test to check for antibodies, or get a vaccine once one is available.

WILL I BE ABLE TO CONTRIBUTE MY INFORMATION TO THE DATABASE?

Yes, each person who has had a test performed will have access to contribute their information to the database if it is not already included. SAFE19 allows for mobile document upload, where our investigators will verify the authentication of the record.

WHAT HAPPENS IF THE FDA PULLS ACCREDITATION FOR A TEST AS MORE INFORMATION COMES AVAILABLE?

The SAFE19 solution is designed to accommodate a variety and evolving series of testing and vaccination standards. The credential made available in the mobile app can re rescinded at anytime providing for real time control of all credentials to accommodate any scenario that may present itself.

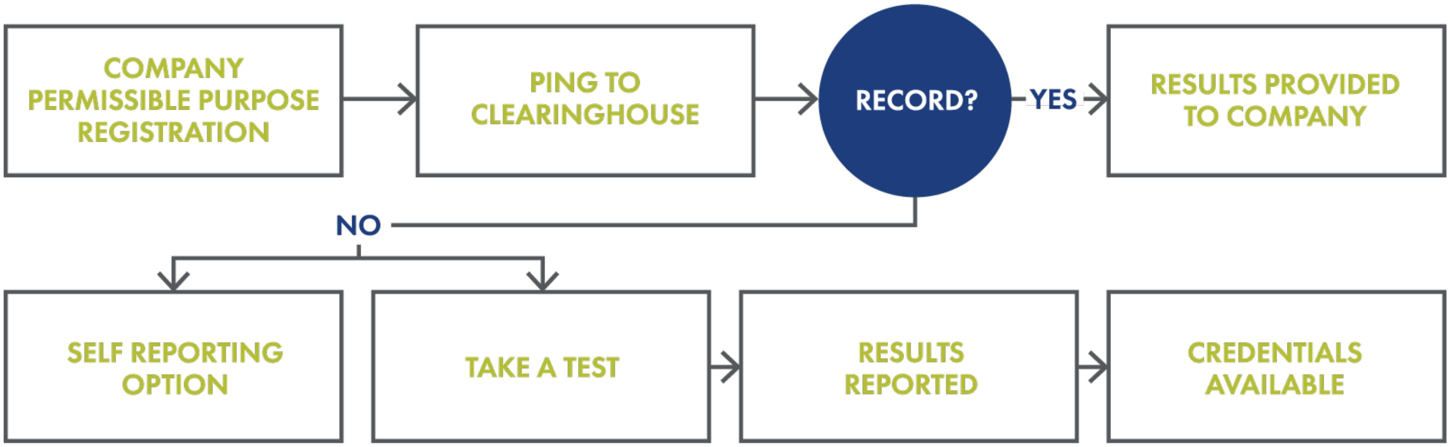
WHY SAFE19?

SAFE19 is backed by Cisive who has been in business for over 40 years. We're able to leverage our experience and technology with expertise in this space. Our current technology is currently utilized by federal, state and local governments in addition to healthcare facilities and businesses of all sizes.

WHAT IF A PARTICIPANT CLAIMS THEIR STATUS IS INACCURATE?

Cisive provides all participants a dispute resolution Help Desk to contact by phone or email. This process is similar to consumer disputes protected by FCRA guidelines.

HOW DOES THIS WORK?


COMPANY PERMISSIBLE PURPOSE REGISTRATION

PING TO CLEARINGHOUSE

RECORD?

YES

RESULTS PROVIDED TO COMPANY

NO

SELF REPORTING OPTION

TAKE A TEST

RESULTS REPORTED

CREDENTIALS AVAILABLE

WHERE ARE YOU GATHERING YOUR DATA FROM?

All data is derived from the primary source. This includes healthcare facilities, labs and clinics, pharmacies, health departments, and third party sources.

IS THE DATA SECURE?

Safeguarding Personal Information

All client data is maintained encrypted at rest in Cisive's centralized storage system using AES-256. Backups are also encrypted. Full backups of dynamic data are completed every night from storage system snapshots. Weekly backups include static data and applications. Ten days of on-line snapshots and two weeks' worth of backups are maintained onsite in a secure location within our secure data center and weekly backups are taken off site Monday morning and stored at Iron Mountain. Month end backups are maintained indefinitely at Iron Mountain.

In addition to electronic security policies, Cisive supports the protection of PII including no-browsing policies. Cisive has also implemented various mechanisms, firewalls, and technological tools which keep the entrusted data safe from nefarious systems and individuals, and has a formal security policy for protection of assets, facilities, and resources which is reviewed by all employees as part of regular security training.

Data Privacy

Cisive has never experienced a breach of data. Cisive does maintain a formal Data Breach Notification Policy that covers the incident response process, local notification procedures, reporting requirements, and privacy incident reports. Cisive also employs a SIEM device and has contracted with Arctic Wolf to monitor all server logs from Firewall/IDS systems, network equipment, webservers and domain controllers.

Cisive maintains logical controls that are programmed into the system that allow clients to only see their own data, and within a given client only allow access to that data to which the user is entitled based on their role. Cisive also maintains separate development, test, demo and production environments.

Secure Data Transfer

Depending on the type of data/protocols needing to be transmitted, Cisive can support encryption methods including but not limited to SSL v3, SFTP, TLS, PGP and GPG. Standard website communication utilizes SSL 3.0 encryption, as well as TLS encrypted email and SFTP for bulk file pickup and drop off. No data is ever transmitted over straight HTTP, or any other insecure protocol, for any reason. All data at rest is AES 256-bit encrypted using SQL2008 encryption routines. All data in transit is encrypted using SSL.

Cisive closely monitors published security alerts as prescribed by US-CERT and the US Department of Homeland Security. Cisive encrypts all data that is being sent to and from client via the internet. Cisive monitors all external internet connections, MPLS circuits between sites, all network switches and routers, websites/web processing functions, applications level processing servers, database server, VO-IP servers and VMWare Hosts. Cisive utilizes VMWare Management console to monitor system performance as well as home built tools that monitor specific parts of the system and automatically notify IT personnel of issues with the system.

When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception. Vendors, third-parties, departments and business functions are required to employ Cisive-approved encryption solutions to preserve the confidentiality and integrity of, and control accessibility to, where this data is processed, stored or transmitted. Cisive is audited annually for operating effectiveness of specific controls in place over the processes required supporting employment screening services in a SSAE 16 Type II report and no defects were found. Cisive contracts with a highly respected information security firm to conduct regular external and internal vulnerability scans and penetration testing, and will share these reports with our clients upon request.

Cisive conducts an annual SSAE-16 Type II report through an outside independent auditing firm who then issues a final report/attestation to its findings. The attestation not only covers the "data center" but Cisive's Research Division and the controls in place for the production of background screening reports. In addition, we are audited annually by several client financial services firms using ISO standards and have no high risk defects.

WHAT WILL THIS INFORMATION BE USED FOR?

This information will be used to primarily help employers, schools, events, etc. determine whether an individual possesses the COVID-19 antibodies.

intelliCorp
a Cisive company