DATA SECURITY SUMMARY

HARDWARE & NETWORK

- **Commercial Data Centers:** (Primary and DR Site): US location, SOC2 Type 2 audited, Video Surveillance and On-site guard 24x7, Multi-factor Authentication (including individually issued badge) required for access.
- **Servers:** Virtualized machines architected for high availability (automatic failover).
- **Operating System:** Our SaaS applications run on current version Windows Server OS. Security patching at least monthly.
- **Monitoring:** Multiple layers of automated, proactive monitoring 24x7.
- **Anti-virus:** Malware and anti-virus protections on all servers. Continuous monitoring and patching/updates at least monthly.
- **Network:** Firewalls protecting all servers and our network. Continuous monitoring and cyber protections are in place.

BACKUPS & DISASTER RECOVERY

- **Disaster Recovery:** Our "Primary Site" systems continually replicate to a second "DR Site." This allows us to have a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) under 1 hour.
- **Backups:** In our "belt and suspenders" approach to data protection we supplement our Disaster Recovery method (described above) with system, file, and database backups.

COMPLIANCE & AUDITING

- We use third party auditors and adhere to these industry best practices
- **SOC2 Type2:** Audited annually.
- **CVO/NCQA:** Audit bi-annually.
- **Penetration Testing and OWASP:** Tested annually.
- **Vulnerability Testing:** Tested quarterly.
- **HIPAA:** All our systems are designed to adhere to HIPAA requirements for privacy.
- **GDPR:** We provide extra protections for Clients who need us to adhere to GDPR standards.

SOFTWARE

- **Language:** Our custom, proprietary SaaS solutions are based on current .Net framework
- **Testing/Quality Assurance:** Our software development lifecycle (SDLC) uses multiple phases of testing (unit testing/Dev, QA, and UAT). The QA Testing is performed by an independent testing team using hundreds of testing scripts that include security testing and regression testing. Before a release to production all code is reviewed by the Information Security Team during the development/testing process. All software goes through a thorough security review at the time of release and is tested annually against the OWASP Top Ten and other common threats for vulnerabilities.
- **Updates:** Software releases for small system improvements or addressing bug defects occur at least monthly. Major updates or new function releases occur at least quarterly.

DATABASE & DATA PROTECTION

- **Database:** Microsoft SQL Server is our standard database management system. All client data is housed within the application database and accessed by our SaaS solutions.
- **Client Segregation:** All Client data for a particular database – LOGICALLY segregated by Client ID. Client data is not visible to another Client.
- **Encryption ("data at rest"):** Our SQL Server databases are fully encrypted, as well as backups of the database, using AES 256 strong encryption.
- **Data Masking:** In addition to database encryption, sensitive data such as passwords and PII are masked when displayed on a screen by the application.

FILE & DATA TRANSMISSION

- **"Data in Transit":** All web pages of the application are encrypted by HTTPS and TLS so that information moving from the SaaS application to your browser (data in transit) is secure.
- **API**: Our SaaS applications use a RESTful API for 3rd party system integration. Our APIs utilize OAUTH authentication, secured by a 256-bit SSL cert that is all software-based protection.
- **Secure FTP (myCM):** Some clients in myCM use a third-party relationship for compliance management. Client-vendors receive myCM case information through a secure, encrypted "SFTP" folder that is unique to them.
- **Secure FTP (SanctionCheck & LicenseCheck):** Communication of lists and exclusions are submitted via secure and encrypted methods.
- **XML (myCM):** Microsoft SQL Server is our standard database management system. All client data is housed within the application database and accessed by our SaaS solutions.

INTERNATIONAL DATA PRIVACY FAQ

Your key questions about international data protection

Q How does Ethico identify GDPR data for the hotline?

A Ethico has dual verification system for reports that may contain GDPR information. During the setup process, any client who has locations in the EU or related states will automatically be assigned a category named, "GDPR". Any report that comes in from an EU or related state will be assigned the "GDPR" category. Also, as part of the review process by our QA Team, the reviewer will mark the "GDPR" check-box identifying these calls as GDPR. Two data points allow Ethico to be able to identify reports related to GDPR at any time. We are able to provide clients and their reports information in a timely fashion due to this. If a reporter contacts Ethico directly, we will notify the client of any data requested within one business day. Ethico will wait for up to one-business day for the client to respond to any data requests. If the client has not responded at that time, Ethico will act according to GDPR guidance.

Q How long does Ethico hold onto hotline data for countries with data privacy laws?

A Ethico has determined that all call records pertaining to countries with international data privacy laws will be retained for 6 months. After 6 months, all report data will be purged from the system. A shell of the report will remain with a note that this report has been removed according data privacy guidelines.

Q How does Ethico identify GDPR and international data for SanctionCheck?

A In order to identify records in SC that are GDPR related, we provide clients with a field that they fill out when uploading their files to the system. All searches done against these names will be flagged as "GDPR." This flag is how we identify any information that is provided in accordance with GDPR data privacy laws. If a data requester requests for change or deletion, we will respond to the client who performed the search within one-business day. Ethico will wait up to one business day for a response from the client for instruction on how to proceed with the request. If the client does not respond in this period, Ethico with fulfill the request based on GDPR data privacy guidance.

Q How long does Ethico hold onto GDPR data for SanctionCheck?

A Since SC is a system of audit for checking employees, vendors, physicians, board members, and volunteers against sanction databases, we will save any records and search results for 2 years for any entity tagged as "GDPR." After the 2-year time period all search information, will be completely purged from our system leaving only a shell of the search with a note that this person "has been removed" in accordance with GDPR guidelines.

Q Does Ethico have a Data Processing Agreement in place with Clients within the European Union (EU) and vendors, who have potential access to Client Data?

A Yes, Ethico has data processing agreements in place, which include the standard contractual clauses (EU 2010/87)

Q How does Ethico keep up with the ever changing data privacy laws?

A We are constantly reviewing the security frameworks to ensure any international data transfer meets all necessary security regulations. We monitor data security regulations in countries around the world to make sure we are current with data privacy laws. We have a system that tells us of the privacy changes, requirements, how it relates to our processes, and recommendations on changes we need to make.

Q Does Ethico comply with international data privacy laws and which ones?

A Ethico is compliant with data privacy standards around the world. These include but are not limited to: GDPR, LGPD, PIPEDA, Singapore PDPA, EU Whistleblower Directive, SOX, HIPAA, CCPA, UK FCA, Australian Privacy Act, etc.