SECURITY & COMPLIANCE FAQ'S

Can you provide sanitized copies of system architecture diagrams and data flow diagrams, as they pertain to the service being provided?

A system architecture diagram is available upon request.

Do you perform security reviews of your application source code? Please explain.

Yes, we incorporate a code review step into our normal development process for every significant code change. A component of this is validating adherence to web security best practices.

Do you enforce network segmentation between trusted and untrusted networks? (i.e., Internet, DMZ, Extranet, etc.)?

Yes, back-end servers are segmented from Internet-facing servers using a firewall that blocks traffic with principle of least privilege. Back-end servers can only be accessed on limited ports from Internet-facing servers and our company intranet.

Will you store customer data or configuration information in your infrastructure? If so, how will you protect this data?

Yes, the data we store is generally low in sensitivity and is stored encrypted at rest.

What protocols will you use to protect application data in transit (e.g., TLS, SSL, SFTP, FTP/S)? Please provide technical details, including version information.

Data are transmitted over HTTP using TLS 1.0, TLS 1.1, and TLS 1.2.

If using encryption to protect data at rest and/or data in motion, please briefly describe your encryption key management processes.

SSL certificates, which encrypt data in motion, are stored in an encrypted and password-protected KeePass database that is backed up using Google Drive. Access to this database is restricted to several administrative employees.

Do you follow a formal software development process that includes application security requirements? Please explain.

Yes, our team has years of experience developing public-facing web applications that handle PHI, and stays current with web security best practices. We apply this knowledge when developing new features and use it to validate all code changes in the code review stage of our development process.

Do you purge application data according to a defined data retention schedule? Please explain.

Not as long as a customer's subscription remains active. However, we will purge data after a 60-day grace period following termination of a subscription.

How will you secure customer data in your backups?

Backups are stored encrypted at rest.

Please describe procedures in place to destroy and/or dispose of electronic media.

Electronic media destruction and disposal is handled by our cloud service provider, which complies with most rigorous security standards. See: http://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx.

Do you use non-production systems to prohibit the storage and use of production data in non-production (e.g., test and development) applications?

Yes, non-production data is used in our test and development environments.

How do you ensure that sub-contractors and other third parties handle customer data securely?

Sub-contractors and consultants are limited in access to development and test environments, which contain non-production data only.

Please describe the process used to enforce strong authentication (e.g., complex passwords, multifactor tokens, certificates, biometrics).

Strong authentication can be enforced using single sign-on technology to offload authentication to the customer's system where they have full control of the authentication process.

Do you have a position or organization responsible for overseeing the company's overall security program? If so, please describe the responsibilities of the position or organization.

Yes, this role is satisfied jointly by the management of our company. Responsibilities include protecting our customers' data and privacy through proactive measures, fostering a security-aware company culture, and responding to security incidents immediately and with transparency.

Are you an InCommon participant, and/or do you support SAML2?

We support the following single sign-on technologies: SAML2, WS-Federation, and OAuth for Google Apps.

Please describe your process to grant, modify, review, and terminate user access.

User access can be controlled through the application's UI by an administrator or offloaded to the customer's authoritative directory using single sign-on technology.

Do you have a documented change control process? If so, does the change control process address security requirements and emergency changes?

Yes, all changes are version controlled and go through a review process before they're promoted to our production environment.

Do you run and monitor a process to ensure that all systems are protected with the most updated virus protection software? Are users made aware of their responsibilities in preventing the spread of viruses and other malicious code?

Systems that store executable files obtained from an external source as well as employee computers are protected with updated virus protection software.

How is administrative access controlled? Please describe additional security controls that may be applicable to accounts and systems with administrative privileges, including access review frequency and source IP address whitelisting.

Administrative access is controlled by granular permissions coupled with multiple levels of application layer authorization checks. These are configured with the principle of least privilege in mind. Additional security controls are available through use of single sign-on technology to offload authentication to the customer's system where they can enforce IP address whitelisting and other custom rules.

Do you rely on one or more cloud service providers? If so, please confirm which controls are maintained by you and which controls are maintained by your management).

Yes, our cloud service provider handles patch and log management for the network and operating system layers. We maintain control of patches and changes to the application as well as to our database service.

Do you require all users to have unique user accounts on systems that store, access, and/or transmit customer data?

Yes, we do

Do you have a process to identify and patch vulnerabilities affecting network infrastructure, applications, and operating systems in your environment? If so, please describe.

Our cloud service provider handles the network and operating system layers. We have a logging and review process in place to identify application-layer vulnerabilities and an automated deployment process to patch these in a timely manner.

Does your organization have system and/or process certifications? If applicable, please provide current attestations.

Our cloud service provider has the following attestations:

- SOC 1, SOC 2, SOC 3
- PCI-DSS
- FERPA
- ISO/IEC 27001, ISO/IEC 27018
- Many others, see: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx

Do you have any security certifications for the data center(s) where customer data will be stored and/or processed? Please explain.

Yes, our cloud service provider has an extensive list of security certifications. See: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx

Do you have a process to address audit recommendations and to ensure compliance with security policies and standards?

Yes, we work with customers to meet their security requirements to the extent that they align with the sensitivity of data that we store.

Please describe (at a high level) the technical and operational controls you have implemented to help you detect and respond to security events and incidents.

We have implemented multiple layers of programmatic security assertions within our application that generate logs and halt execution when a potential risk is identified. These logs are reviewed regularly and if a real security risk is identified, it is addressed immediately and with highest priority. Also, our cloud service provider takes a rigorous approach to detecting and responding to network and infrastructure-level security events and incidents.

Do you have a disaster recovery plan (DRP) and a business continuity plan (BCP) for all systems and business processes supporting customer data?

Yes, all data is asynchronously replicated to a secondary data center located in a different state than our primary data center. If a disaster affects our primary data center, we can have our full infrastructure back online in the secondary data center within one day.

What is your expected recovery time for the services provided?

One business day is the worst-case scenario.

Do you conduct penetration testing to assess the security of your perimeter network (e.g., firewall, routers, remote access servers, web applications)? If so, how often are tests conducted?

Network-level penetration testing is performed on a regular basis by our cloud service provider.

What measures do you take to guarantee data integrity?

We store three copies of all customer data within a primary data center and three copies within a geographically-disparate secondary data center. Additionally, we perform differential database backups every hour, full database backups every week, and we archive database backups for a period of 90 days.

Please explain how you would communicate with customers during an emergency or an outage.

Messaging is handled by posting informational updates to our application's normal URL and by emailing customers when services are restored. ligns with their needs.

Do you regularly log reports and inform customers in the event of any security incidents and take corresponding measures?

We inspect logs on a daily basis and have automated monitoring in place to trigger alerts when abnormal conditions arise. Additionally, our hosting provider has comprehensive logging and monitoring controls already in place for our server and network infrastructure.

We expect timely notification of both possible and confirmed data breaches before any other parties are notified. Please describe the communication protocols by which you will interact with your customers.

Customers are notified by email as soon as possible when a confirmed data breach is discovered. In addition, the assigned Customer Success Manager will call the customer's primary contact to personally inform them of the situation.

What measures do you take to guarantee service continuity?

We build redundancy into every layer of our software and hosting infrastructure from a mirrored database back-end, to a farm of load-balanced web servers, to geographically redundant storage. Also, our software is hosted in the public cloud, which allows us to scale quickly and automatically to handle increased usage load.

Have you filled out the Cloud Control Matrix?

Yes, version 1.1 is available upon request and we work to complete newer versions as they are released.

What measures do you take to guarantee speed, response time, and bandwidth?

We take performance seriously and use an APM solution to continuously monitor our software. We also use automated infrastructure scaling, available through our hosting provider, to accommodate spikes in usage volume. We continually and proactively optimize our software and infrastructure, but also react very quickly to patch performance problems that do arise.

Upon termination of our subscription, what assistance is provided for migrating and transferring our data to a different service provider?

We listen to our customers and want to help them succeed. To this end, we are continuously enhancing our software and are willing to work with the customer and build custom enhancements in order to better meet their needs. In the unfortunate event that a customer decides to cancel their subscription, we provide bulk data export capability free of charge. This capability is useful for migrating data to a different service provider. Assistance beyond this and other self-service tools is available but will be billed at an hourly rate.

Do you permit audits carried out by your customers or a trustworthy third party in close cooperation with your customers? Will you immediately remedy any insufficiencies and inadequacies uncovered during an audit?

We are willing to cooperate with our customers to conduct audits and remedy any inadequacies that impact the security or stability of our software as long as such requests are reasonable given the sensitivity of data we handle.

We are subject to various state and federal compliance frameworks. Information shared with vendors is subject to such compliance. Please indicate all applicable compliance frameworks and demonstrate that such compliance has been achieved.

We take security seriously and follow many industry best practices. Our application is hosted in Microsoft Azure data centers that maintain compliance with numerous compliance frameworks including FERPA, HIPAA, and PCI DSS. That said, we primarily handle data that is low in sensitivity, but we are happy to work with our customers to achieve a level of compliance that aligns with their needs.

If we detect a security or performance concern, please describe the process to obtain support. Distinguish between routine and emergency requests.

Customers have a dedicated FMX Customer Success Manager assigned to them. In the event of a security or performance concern, you can contact the manager by emailing support@gofmx.com or by phoning the manager at their direct office line. For emergency requests, the support@gofmx.com email is recommended because it is sent to multiple Success Team members in addition to your dedicated Success Team Manager.

How do you test your software?

All changes to our software must pass a battery of automated tests, manual exploratory tests, and receive approval from management before they are released to our production environment. Testing is conducted in an environment that is identical in configuration to production, but contains no production data.

What is your patch release schedule?

Routine patches are released weekly. Deployment automation allows us to release a hotfix without taking our website offline.

How do you monitor your application?

We monitor our application using an APM solution that triggers email and pager alerts when abnormal conditions arise. We respond to alerts immediately during normal business hours and within several hours after business hours.

Describe the physical security and environment control capabilities in place for data centers and workspaces where customer information may be accessed, stored, or processed.

Our servers are hosted in Microsoft Azure data centers. Microsoft employs numerous measures to protect from power failure, physical intrusion, and network outages, and complies with stringent industry standards for physical security and reliability. For more information, see: https://www.microsoft.com/en-us/trustcenter/Compliance.