CoverMyMeds

Software as a Service System

System and Organization Controls 3 Report

(formerly Service Organization Control 3 Report)

For the period

March 1, 2016 to February 28, 2017

;

KraftCPAs PLLC

CoverMyMeds, LLC

SOFTWARE AS A SERVICE OPERATIONS

Columbus, Ohio

System and Organization Controls 3 Report
Over the Security, Availability, Processing Integrity, Confidentiality, and Privacy Principles

FOR THE PERIOD
MARCH 1, 2016 TO FEBRUARY 28, 2017

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of CoverMyMeds, LLC:

We have examined management's assertion provided in Section II that during the period March 1, 2016 through February 28, 2017, CoverMyMeds (CMM) maintained effective controls over their Software as a Service (SaaS) system at its Columbus, Ohio location for the Security, Availability, Processing Integrity, Confidentiality, and Privacy principles set forth in Trust Service Principles (TSP) Section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* [American Institute of Certified Public Accountants (AICPA), *Trust Services Principles and Criteria*] (applicable trust services criteria), to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical), use, or modification to meet CMM's commitments and system requirements;
- the system was available for operation and use to meet CMM's commitments and system requirements;
- the system processing was complete, valid, accurate, timely, and authorized to meet CMM's commitments and system requirements;
- the information designated as confidential was protected by the system to meet CMM's commitments and system requirements; and
- the system's collection, use, retention, disclosure, and disposal of personal information is in conformity with the commitments in CMM's Privacy Policy.

CMM's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the SaaS covered by its assertion is included in Section III. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of CMM's relevant controls over the Security, Availability, Processing Integrity, Confidentiality, and Privacy of the SaaS system; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, CMM's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, during the period March 1, 2016 through February 28, 2017, management's assertion referred to above is fairly stated, in all material respects, based on the AICPA Trust Services Criteria for the Security, Availability, Processing Integrity, Confidentiality, and Privacy principles.

Kraft CPAs PLLC

Nashville, Tennessee
May 23, 2017

II. MANAGEMENT'S ASSERTION

covermymeds®

2 MIRANOVA PL, 12TH FLOOR · COLUMBUS, OH 43215
22901 MILLCREEK BLVD, SUITE 240 · HIGHLAND HILLS, OH 44122

II. MANAGEMENT'S ASSERTION

May 23, 2017

During the period March 1, 2016 through February 28, 2017, CoverMyMeds (CMM) maintained effective controls over our Software as a Service (SaaS) system at our Columbus, Ohio location, for the Security, Availability, Processing Integrity, Confidentiality, and Privacy principles set forth in TSP Section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* [AICPA, *Trust Services Principles and Criteria*] (applicable trust services criteria), to provide reasonable assurance that:

- the system was protected against unauthorized access (both physical and logical), use, or modification to meet CMM's commitments and system requirements;
- the system was available for operation and use to meet CMM's commitments and system requirements;
- the system processing was complete, valid, accurate, timely, and authorized to meet CMM's commitments and system requirements;
- the information designated as confidential was protected by the system to meet CMM's commitments and system requirements; and
- the system's collection, use, retention, disclosure, and disposal of personal information is in conformity with the commitments in CMM's Privacy Policy.

The description of controls included in Section III identifies the aspects of the SaaS system covered by our assertion.

Matt Scantland

_____

Matt Scantland, CEO
CoverMyMeds

III. DESCRIPTION OF CONTROLS PROVIDED BY COVERMYMEDS

III. DESCRIPTION OF CONTROLS PROVIDED BY COVERMYMEDS

A. OVERVIEW OF ORGANIZATION & SERVICES

Company Information

CoverMyMeds (CMM) is a healthcare technology company providing Software as a Service (SaaS) and communication solutions linking pharmacies, physician practices, and payers. CMM was founded in 2008 and, at all times during the period, was a privately-owned limited liability company.

Services Provided

CMM provides physician offices and pharmacies a one-stop, all-drug, all-payer solution to manage the more than 170 million medication prescriptions annually rejected by payers due to Prior Authorization (PA) requirements. Products include integration points for pharmacies and physicians as well as workflow management solutions for payers. The service enables pharmacies and physicians to initiate PAs and send them to payers to make the final determinations for covering the prescribed medications.

CMM delivers services on both their website (www.covermymeds.com) and through integrations with established clinical software systems such as pharmacy dispensing systems and Electronic Health Record (EHR) systems. These integrations use Application Programming Interfaces (APIs) that are developed and operated by CMM. Third-party networks may be employed by CMM for transaction connectivity or eligibility services.

For the purposes of this document, Electronic Prior Authorizations (ePA) are defined as CMM PA transactions that are not faxed. It does not refer to the National Council for Prescription Drug Programs (NCPDP) published ePA standard.

Front-End Dashboards

CMM provides dashboards for pharmacy and physician users to manage and initiate the PA or ePA process. These applications include access to many different PA forms for different payers and pharmaceuticals. Additionally, payer dashboards are available for PA workflow management tasks such as making determinations, creating tasks, and adding notes to PA. CMM also provides an uptime website or dashboard for customers to check service availability.

PA Processing

CMM has applications and services that integrate with payer systems for the purposes of completing the PA process. CMM sends the PA via a high-volume distributed infrastructure. Depending on the integration point, the PA is sent via fax or electronically. CMM's fax infrastructure handles PA transmission for payers who do not have ePA integration or use CMM's PA workflow management.

Data

CMM stores a large amount of protected health information (PHI). The stored PHI consists largely of "pharmacy prescription" information, demographics, and drug information, insurance plan information, and a limited amount of lab and medical chart information.

CMM does not store financial information or credit card numbers. Generally, social security numbers (SSN) are not stored except where Medicare PAs may use SSN for a patient identifier. CMM is not subject to Payment Card Industry Data Security requirements.

B. ORGANIZATION & ADMINISTRATION CONTROLS

Talent Management

CMM hiring practices require that employees undergo a formal background check and healthcare sanctions check in addition to the interview process to ensure experience is commensurate with the job requirements. All CMM employees are required to sign and acknowledge confidentiality agreements upon hire. Personnel with security, availability, processing integrity, confidentiality, and privacy responsibilities have specific job descriptions.

As part of CMM's culture of security, training is conducted annually to communicate CMM's polices to all employees. New hires attend security and privacy training upon hire and annually thereafter. Acknowledgement and acceptance of training is tracked for all employees. CMM employees also participate in an annual performance appraisal process.

CMM has established security, availability, processing integrity, confidentiality, and privacy policies and procedures in addition to operational policies and procedures. These documents are reviewed annually by management. CMM assigns role-based ownership to policies and procedures for the purposes of review and revisions. The policies and procedures formalize the technical, physical, and administrative controls to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, and their specifications for implementation. The Privacy Officer, Security Officer, or senior management is responsible for authorizing exceptions to the policies. CMM has a non-compliance policy. Employees who are not compliant are subject to disciplinary action.

Risk Assessment & Risk Management Practices

CMM has a policy which establishes the requirements for periodic risk assessments and network and website penetration testing. CMM contracts with an independent third party to conduct an annual risk assessment, which also considers requirements of HIPAA as part of the engagement. This addresses HIPAA's annual risk assessment requirement. CMM contracts an independent third party to conduct a periodic penetration test, which includes:

- Application penetration testing,
- Internal network penetration testing, and
- External network penetration testing.

In addition, the Infrastructure department will perform at minimum quarterly internal and external vulnerability scanning. Penetration test and risk assessment findings are reviewed by management and corrected if the risk is unacceptable.

Security and Privacy Program

CMM's Information Security department is responsible for the security and privacy programs. Information Security is an independent function reporting to executive management. The Security

Operations team within the Shared Technology department is primarily responsible for implementing and configuring secure technology and tools, as well as using the tools to protect CMM. Additionally, the Internal Infrastructure team is responsible for the execution of the access control process.

CMM has a Privacy Officer, Compliance Officer, and Security Officer as members of Information Security who are responsible for privacy and security. The Privacy Officer, Compliance Officer, and Security Officer provide ongoing monitoring and oversight of the Security, Compliance, and Privacy programs. The Privacy Officer is identified in the new hire and annual privacy training. A compliance hotline exists for employees to anonymously report compliance and privacy concerns, and a non-retaliation policy has been established.

The Privacy Officer reviews the Privacy Policy annually and recommends any changes, which are approved by Senior Management. Changes to the Privacy Policy are communicated via the intranet, and employees are notified through an email alert. The Privacy Officer and Compliance Officer monitor changes in legal, industry, and other business areas and update policies and procedures to reflect changes to requirements. The Privacy Officer and Compliance Officer also consult with outside legal counsel annually to determine if any changes are required to policies and procedures as a result of changes in legal or industry requirements. CMM reviews the Privacy Policy and Notice of Privacy Practices on an annual basis and updates the documents as necessary. The updated Privacy Policy and Notice of Privacy Practices are then published to the website for customers and patients.

Privacy Policy, Notice, and Personal Health Information

CMM publishes the Privacy Policy, Notice of Privacy Practices, and Terms of Service on its website at www.covermymeds.com under the Privacy Center. CMM includes links to the Privacy Center before login and in the header of applications where PHI is collected. The Privacy Center includes the most current Privacy Policy. A copy of CMM's Privacy Policy is included as an appendix to this report in Section IV.

CMM handles PHI for patients through the PA process at the request of a doctor, pharmacist, insurance company or other healthcare professional. The Privacy Policy contains an objective description of the entities and activities including the operating jurisdictions, types of information covered, and the sources of information. Only the personal information required by an insurance company to complete a PA or process a claim is collected and stored by CMM. Other uses and disclosures of PHI not described in the Notice of Privacy Practices will be made only when CMM receives written permission on an authorization form. CMM has designated the Privacy Officer as the individual with responsibility for handling all authorized disclosures of PHI outside of normal business operations. After authorization has been received from the data subject, CMM updates the disclosure tracking log with the data subject's information, the date of the disclosure, and the reason for the disclosure.

CMM contracts with covered entities to provide PA processing operations and notifies these entities when a patient requests amendments or access to records. Because CMM is a business associate, covered entities are responsible for making determinations of access and/or amendment requests. Once the covered entity has made the determination, CMM will either provide the data subject with the records requested or make the proposed amendments, or inform the data subject of the reason for denial. Patients may obtain an accounting of disclosures of the data subject's PHI by requesting the information directly from the Privacy Officer. Instructions and contact information for obtaining this information are included in the Notice of Privacy Practices published on CMM's website.

Confidential information is retained for no longer than necessary to fulfill the purposes stated above, or for any period otherwise specifically required by law or regulation. CMM's internal policy is to retain all confidential information for a period of 11 years from the date of origination. CMM will destroy information in a manner reasonably certain to prevent loss, theft, misuse, or unauthorized access. When media and hardware are retired, CMM wipes the disk image and all data residing on the device. CMM obtains a certificate of destruction to ensure that all media was discarded properly.

Data Classification and Destruction

CMM's business practice is to classify all data as confidential. Policies have been established to address protection requirements, access rights and access restrictions, and retention and destruction procedures. The Privacy Policy specifically addresses protection requirements for personal information as well as use, retention, and disposal of personal information.

Terms of Service and Business Associate Agreements

CMM functions as a Business Associate for users who are Covered Entities (e.g., providers, plans, or PBMs). CMM is contractually obligated to its clients and vendors as a Business Associate under both HIPAA and the HITECH Act.

CMM uses a standard Business Associate Agreement (BAA) with most providers and may execute customized BAAs with large health systems, pharmacies, and payers that pay prescription drug claims. Customers who establish their CMM account through a CMM partner are informed of their choices and provide consent through signing a BAA or establishing a Master Services Agreement (MSA).

The Terms of Service and BAA include the privacy obligations and security requirements for users and refer to CMM's Privacy Policy. To use CMM services through www.covermymeds.com, users must agree to the Terms of Service to either establish an account or to look up an existing PA record. According to the Terms of Service, users must be licensed healthcare providers or employees of a licensed healthcare provider to use CMM's services.

Healthcare professionals using the CMM SaaS product are required to make changes to their own user information and their patients' personal information directly on the CMM site, as stated in the Privacy Policy and Terms of Service. Customers can access their user information in the Preferences tab after logging into the service. Customers may update patient's personal information related to a PA directly on the CMM site to ensure it is complete and accurate. Contact information is provided for those customers that require assistance. CMM identifies the consequences of withdrawing consent in the Privacy Policy.

Third Parties

The Privacy Policy states that CMM does not sell, rent, or share personal information with parties who are not affiliated with CMM, except in rare situations when permitted or required to do so by law. In addition, CMM does not disclose personal information to non-affiliated third parties except where required by law. CMM may share personal information with trusted companies that CMM has hired to provide services, such as colocation data center services and network security monitoring. CMM only shares information collected with parties with which they have a BAA.

In cases where there is potential for CMM's vendors to come into contact with PHI, they are

contracted to only perform the services that they have been hired to provide. In addition, they are required to comply with HIPAA's security provisions to protect such personal information through the execution of a BAA. The BAAs contain provisions that state that the subcontractor will notify CMM of any actual or suspected unauthorized disclosure of PHI in a timely manner. Additionally, the BAAs state that the subcontractor must comply with security and privacy obligations, and contains provisions that grant CMM the right to audit the Business Associate's security and privacy policies and procedures as necessary.

Incident Response

CMM has a documented Incident Response Policy and procedures for security and privacy, which includes:

- Handling security and privacy incidents received by either employees or customers,
- Documentation requirements, and
- Customer notifications.

CMM has several communication channels with customers including telephone, email, chat, and direct partner relationships. Customers or partners who have availability, security, or privacy complaints may report through these channels. The Privacy Policy and the Notice of Privacy Practices contain the official communication channels for privacy inquiries, complaints, and disputes for both customers and patients.

CMM tracks and responds to any validated security, confidentiality, or privacy incidents. Examples include purposeful or accidental PHI disclosure, PHI misplacement, loss of data, unauthorized access, system compromise, and physical break-ins. The Infrastructure and Development departments notify employees via email, and the Operations department notifies customers using email and/or telephone.

C. TECHNICAL & SYSTEMS OPERATIONS CONTROLS

CMM has implemented technical and administrative controls according to industry best practices and is fully compliant with current HIPAA rules. CMM consolidates information from attorneys and guidance from industry standards such as Open Web Application Security Project (OWASP) and National Institute of Standards and Technology (NIST).

Infrastructure

CMM colocates its infrastructure at an off-site data center facility and maintains redundant infrastructure at a separate facility. These facilities provide full environmental controls with power redundancy and physical security. The data center also provides and manages redundant Internet connectivity for CMM.

High-traffic applications are load-balanced across multiple servers and all essential parts of the stack are redundant and highly available with automatic failover. CMM owns their core infrastructure including systems, servers, storage, switches, firewalls, and load balancers.

Infrastructure Change Control

CMM has production change control processes that apply to software releases and infrastructure

changes. CMM's policy and procedures for production infrastructure changes include scheduling, a detailed plan, backout procedures, verification, and testing. Once an authorized employee requests a change, the change is authorized by either a peer review or management approval, depending on the level of risk. Change control procedures assign system change and maintenance duties, including patch management, to ensure proper responsibility and accountability. The change management process includes notification of key participants regarding any changes that may affect system security. The person responsible for the change will notify employees using methods such as verbal communication, chat, or email.

CMM has a patch management process for identifying and applying updates. CMM's Infrastructure department monitors vendor and industry security mailing lists for software updates. Once necessary updates are identified, a risk-based patch management policy applies. If a high priority security vulnerability is identified, but a vendor has not yet supplied a patch, CMM will implement a solution to mitigate the vulnerability until an official patch is released. The patch management software installs an agent on all user workstations and detects patches that are necessary based on software installed on the machine and installs the necessary patches.

Data Encryption

CMM requires encryption of PHI and confidential information when in transit and at rest. Data containing PHI must be encrypted prior to leaving CMM's data center. Data sent from CMM's network is transmitted over the Virtual Private Network (VPN) or the public Internet with 256-bit Transport Layer Security (TLS) encryption, in accordance with Federal Information Processing Standards (FIPS) 140-2 and the relevant NIST publications. CMM utilizes multi-factor authentication for remote VPN access.

When stored on production infrastructure, disk data is encrypted using the built-in hardware support of CMM's Storage Area Network (SAN). In addition, all employee workstations use disk encryption that is enforced through enterprise configuration management tools. PHI is not stored on removable media with the exception of that which is necessary for the purpose of backups or recovery. PHI stored on tapes, any removable media, or physically transported, is encrypted using strong encryption.

Disaster Recovery and Business Continuity

CMM has a formal business continuity and disaster recovery plan that covers backups, off-site storage, and testing. CMM tests the plan annually.

CMM stores backups using a fully redundant disk array. Disk-based backups are the primary source of backups for all practical day-to-day needs. Disk-based backups are tested through standard day to day business use. Database backups are tested when ad hoc requests are made to refresh a full size test environment. Access to the backup software is restricted.

In addition to disk-based backups, backup replication is performed nightly for long-term retention and off-site storage. Backup Operators will perform backup replication on all data that would be required to restore CMM's services in case of a complete loss of the primary disk-based backups. Backup Operators store replicated backups in a secure CMM facility that is separate from the primary data center.

SLAs

CMM has a designated SLA and Notifications Policy and procedures, which addresses both internal and external notifications in case of an availability incident. CMM adheres to SLAs negotiated with its customers. CMM tracks each availability issue through a tracking log that documents information about the outage including duration, affected areas, fixes, and the communication method. The Technology team is responsible for responding to alerts in case of a production issue at all hours. Monitoring tools provide alerts that enable the team to respond promptly.

D. LOGICAL SECURITY CONTROLS

Employee Access

CMM has policies and procedures that address access controls, preventing unauthorized access, acceptable use, and infrastructure administration. CMM employees are granted the least privileges necessary to fulfill their duties as part of their role and only granted domain user access within AD. Privileged access within AD is restricted to employees with a suitable role and business justification. The CMM Internal Infrastructure team performs a quarterly access review and upon status change to ensure access granted is consistent with employees' roles and that no access exists for terminated employees.

The Infrastructure department is responsible for maintaining a procedure for provisioning access and provisions user access based on role and need to perform job functions. Upon an employee's termination, CMM removes the employee's system access.

Firewalls

CMM's internal network is protected by firewalls that are configured to filter traffic and allow pass-through traffic of only authorized protocols. There is deep packet inspection on the firewall to provide virus detection on the network itself. CMM manages an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) to prevent and detect threats to perimeter security. CMM uses a Managed Service Provider (MSP) to monitor and analyze the IPS/IDS logs. If a matter requiring immediate attention arises, the MSP notifies CMM promptly.

A Network Access Control (NAC) appliance is in place to prevent unauthorized devices from connecting to the corporate network. CMM maintains a network diagram that documents its systems and boundaries. Network switches divide the network into logical segments and forward packets into their assigned segments. Access to make modifications to network device configurations, along with operating systems that support these devices, is restricted to authorized personnel to prevent unauthorized changes. CMM's database access is restricted to authorized individuals or applications only.

User Authentication

CMM requires the use of a unique user ID and password to access the network. Systems, network, and other technologies utilized at CMM require strong passwords to reduce the risk of brute force attacks.

CMM provisions remote access via VPN on a case-by-case basis to those who have a business

justification as part of their role and are subject to the same Acceptable Use Policy as when on the corporate network. CMM uses multi-factor VPN authentication.

CMM uses an endpoint protection suite for virus, malware, and system vulnerability protection for workstations and systems commonly affected by malware. Update files for users outside of the office are pulled from the vendor. Update files for users inside the office are pushed from the server.

Customer Account Creation and Terms

CMM establishes contractual security, availability, and privacy requirements with users based on the type of customer and their needs. Depending on the user, this may include accepting the Terms of Service and Privacy Policy on the website, signing a BAA, and/or establishing a MSA with SLAs. Contract templates were developed by outside legal counsel and compared to the Privacy Policy and procedures. Support information for prescribers, pharmacists, and partners for using the application can be found online through the "Help" option at www.covermymeds.com. CMM customers are responsible for creating user accounts and their employees' access management. CMM requires users to log on with a user name and password. Users are required by the Terms of Service to keep their login information confidential and to discontinue use upon termination from the company through which they access CMM.

Data Partitioning

CMM uses a multi-tenant architecture to allow authorized users access to only their client's or patient's data. A permission table manages the relationship between a PA request and the users or groups that can access the PA in CMM's system.

To access an ePA record, a registered user must login to the service and must have the designated permissions to view a specific ePA. Non-registered users can access specific ePA records only after accepting the Terms of Service and Provider Agreement and must have the designated key ID code, the patient's last name, and the patient's date of birth. Only registered users, or users with a valid key, have access to view a PA form and can download or fax that form.

E. PHYSICAL SECURITY CONTROLS

CMM production servers are housed at secure third-party data centers, which provide full environmental controls with power redundancy and physical security. Access to the data centers is restricted to Infrastructure staff and is granted only after approval by the SVP of Shared Technology. Visitors to the data centers require a prior ticket notification to the data center and must be escorted by an authorized CMM employee.

In addition, CMM maintains an on-site server room that houses the development environment as well as serving as the backup location for disaster recovery purposes. The on-site server room has physical and environmental protections in place. Physical access is removed upon termination of employment.

F. SYSTEM DEVELOPMENT LIFE CYCLE

CMM technology is built with a modern, multi-tenant architecture developed entirely in-house by CMM employees. The platform consists of modular applications, integrated through a Service Oriented Architecture that supports internal applications and external integration partners. CMM's

applications are web-centric, communicating primarily through web services.

Software Development Process and Life Cycle

CMM has documented development change control procedures that ensure all changes to the applications include a deployment plan, risk mitigation test plan, and change schedule. The development databases do not contain confidential information.

CMM developers and test engineers assess risk, including mitigation strategies, prior to deployment of any code changes as part of the SDLC. The risk assessment and mitigation process is built into the overall SDLC process through activities such as Pair Programming, peer review, code review, and through test-engineering activities performed by someone other than the developers.

Testing takes place throughout the development process. CMM has dedicated test engineers who work closely with their developers. Test engineers use a mix of automated and manual testing, with a bias towards automating anything that will be repeated. Applications have automated test coverage as well as automated functional testing. CMM provides this test coverage using unit-testing frameworks that are part of their migration and deployment process. Authentication and authorization tests are also included in automated unit testing. CMM supplements automated unit testing with functional human testing, which occurs prior to deployment on testing servers. After a deployment, they also provide human testing on the live systems.

CMM has documented emergency change procedures, which ensure these changes are documented and authorized timely.

G. PROCESSING INTEGRITY CONTROLS

PA Processing

When a PA is required by a plan to authorize payment for medications, the pharmacy or prescriber must start a PA request. CMM provides methods for pharmacy and physician users to manage and initiate the PA request. Pharmacies or prescribers can initiate a PA via CMM's Front-End Dashboards, an integrated Pharmacy Dispensing System, or the prescriber's Electronic Health Record System. These applications include access to many different PA forms for different payers and pharmaceuticals. Although it is the user's responsibility to submit the appropriate PA, CMM assists in the form selection process by using algorithms that use information entered by the end-user. This data may include, but is not limited to, the patient's state, the drug name, strength and dosage form, the name of the patient's healthcare plan or an associated Bank Identification Number (BIN), Processor Control Number (PCN), and RxGroup.

Before an end-user can initiate a PA, certain fields are required to be entered and valid to ensure that processing is not delayed. For example, the patient's name, the drug, date of birth, fax number for the physician, and other fields mutually agreed upon or specified by an industry standard must be entered before the request can be sent to the prescriber. The user is responsible for entering an appropriate and valid fax number for the prescriber. In the event that a fax to the prescriber cannot be processed, a fax failure notification email is sent to the user. Finally, the NPI, prescription frequency, quantity, number of refills, duration of treatment, and prescriber signature must all be completed before the PA can be sent to the benefit plan.

CMM has field validations in place to reduce data entry errors and to ensure that values entered meet requirements defined by the payer. In the event that invalid data is detected, the application returns an error message or will not allow the submission of the PA to the payer until all required fields are included. For example, the application will not accept a number less than 10 digits for the NPI, which is a unique 10-digit identification number required by HIPAA for all healthcare providers in the United States.

If a payer uses CMM's PA management suite, ePA plus PA workflow management tools, PA processing happens electronically and can be automated using payer-specific rules and logic. For those payers that do not connect directly to CMM, PAs are submitted to payers via fax. CMM provides PA status updates to providers through various channels including, electronically to our users via the CMM website, Pharmacy Dispensing System, and EHR System or via fax for non-user providers.

In addition to field validation checks, CMM monitors the PAs being processed via real-time dashboards that show data patterns over time. This allows the CMM team to take action quickly if anything unusual should develop. When there are processing errors, CMM's monitoring tools send real-time alerts to the appropriate staff via email and chat room notifications.

CMM also provides an uptime website or dashboard for customers to check service availability. CMM's back-end service sends email reminders to customers regarding PA status.

IV. APPENDIX

IV. APPENDIX

A. SUBSEQUENT EVENTS

One significant event occurred subsequent to the period covered and prior to the date of the service auditor's report. CoverMyMeds was acquired by McKesson Corporation, an American pharmaceutical company, on April 1, 2017.

B. COVERMYMEDS PRIVACY POLICY

CoverMyMeds LLC ("CoverMyMeds") is a limited liability company organized under the laws of the State of Delaware and is headquartered in Ohio. CoverMyMeds collects and shares only the minimum necessary amount of information required to provide our valuable services to our website users.

The servers that host the company's website are located in the United States, and any personal details you provide to us will be processed by CoverMyMeds in the United States. By using this website, you agree that the laws of the State of Ohio, without regard to conflict of laws principles, will govern all matters between you and CoverMyMeds relating to your use of this website.

If, after reviewing this document, you have questions, please contact us at privacymatters@covermymeds.com or at the physical address listed at the end of this Privacy Policy.

PLEASE NOTE: Your continued use of covermymeds.com (the "website") constitutes your approval of and agreement to this Privacy Policy. The use of this website is governed by the Terms of Service posted on the website.

ALSO, PLEASE NOTE: Any capitalized terms used but not specifically defined in this Privacy Policy have the same meanings as in the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations, as amended from time to time (collectively, referred to as "HIPAA"). For the sake of convenience, this Policy refers to your information and your patients' information collectively as "your information."

What information do we collect about you?

In general, you can visit covermymeds.com without telling us who you are or revealing any personal information about yourself or your patients. However, in order to activate the service provided by CoverMyMeds and use the application we provide, you may need to register on our website, and in connection with the registration process and your use of the application, we will collect personal information about you. The personal information we collect about you consists primarily of demographic information, such as your name, affiliation, email address, telephone number, identification number (such as NPI or NABP/NCPDP number), your role in the prior authorization process, and contact information for other Health Care Providers with whom you work and share patient information, so that we may streamline data entry for you. We only collect this personal information if you voluntarily submit it to us when you register for and use the application and the service we provide. Your login password is encrypted and not stored in "plain text" that can be seen.

From time to time we may also conduct surveys where we will collect your answers, ideas, and preferences if you elect to participate in the surveys. We may also collect non-Individually Identifiable Information through the use of "cookies." For more details about this type of data collection, please refer to the section below on how we collect information.

To protect your security and privacy, we require that you, as the registrant, enter the personal information that you provide to us and that the information be current, complete, and accurate, although CoverMyMeds disclaims any legal duty to verify the accuracy of any personal data that you provide to us. You are free to access your personal information that we have on file by contacting us by email at privacymatters@covermymeds.com. In addition, at any time you can update your information or delete your account in the Preferences tab after you log in, or if you request that we modify or delete your personal information by sending an email to us at privacymatters@covermymeds.com with the words "UPDATE MY INFORMATION" in the subject line. Please note, however, that information that is updated or deleted may be retained by CoverMyMeds due to compliance and legal requirements. Also, please be aware that, to protect your privacy and ensure information is kept secure, CoverMyMeds will take reasonable steps to verify your identity prior to making changes to your personal information.

What information do we collect about patients?

Through use of the website, we collect information about your patients, including patient name, address, other demographic information, diagnosis and/or medical condition, treatment/medical history (including prescription medications), health insurance information, and/or financial or other relevant information, as necessary to submit coverage determination requests. The information we collect includes "Protected Health Information," as defined HIPAA. Your submission — and CoverMyMeds collection — of patient information is governed by the Terms of Service posted on this website.

How do we collect information?

As described above, you provide Individually Identifiable Information about you and your patients. Information that you provide to us is stored on our servers for later retrieval and use with the covermymeds.com application.

CoverMyMeds collects personal information through the CoverMyMeds webpage when a Health Care Provider or staff member starts or participates in the prior authorization process. In addition, we collect personal information either through the CoverMyMeds webpage or directly from a pharmacy dispensing system when a pharmacist or staff member submits a pharmacy claim through a claim adjudication system, or proactively identifies a rejected claim and starts the prior authorization process. These services are only performed at a user's request, either after viewing and accepting the Terms of Service available at covermymeds.com, or by initiating the process by submitting a claim to our BIN number.

Cookies are required for use of the covermymeds.com application. A cookie is a small amount of data, which often includes an anonymous unique identifier that is sent to your browser from a website's computers and stored on your computer's hard drive.

We may use cookies to collect general, non-personal, statistical information about the use of the website, such as how many visitors visit a specific page, how long they stay on that page, the sequence of pages accessed, and which hyperlinks, if any, they "click" on. We may also use cookies for

purposes of identification of your computer when you revisit our website and to recall your authentication information.

Depending on the type of browser you are using, your browser may be set to alert you to the use of cookies. You do not have to accept all cookies sent to you by this website; however, depending on the particular cookie you reject, you may not be able to use some of the features of this website.

How do we use information?

We use your username and password for purposes of authentication and security.

We use your patient's information for Treatment, Payment and/or Health Care Operations purposes. Generally, CoverMyMeds' services can be used to coordinate the submission of coverage determination forms and to share this information with other Health Care Providers. You initiate the process of CoverMyMeds sharing or disclosing information to other providers. Also, we may process your information to Standard or Non-Standard Data Elements, to be used by Health Plans and other third party payers to make coverage determinations. Finally, we may use aggregated, de-identified information from you and our other for business research and analysis, such as trend identification and performance enhancements. This information is blended with information from other users and is not linked to any particular individual. For example, information collected on the ways Health Care Providers use our online tool is blended with other user data to improve the functionality, speed, convenience, and overall value of the CoverMyMeds services. Information collected in response to survey questions you answer may also be aggregated and used to improve the CoverMyMeds services or for research and development purposes associated with, for example, new products or published studies.

Through covermymeds.com, you may choose to access a simple patient portal that will allow your patients to access the prior authorization forms you have created for them. The portal will also allow your patients to follow-up directly with you (or another Health Care Provider) to ensure the request forms are submitted to the Health Plan.

We will not contact any patients whose information we have collected from you in connection with your use of the covermymeds.com application, unless you have requested that we interact with the patient.

You can delete your registered account with covermymeds.com at any time. Such deletion will take effect immediately, rendering your account inaccessible; however, our system maintains the record of your account for audit purposes, and we may maintain backup copies of your information for legal and compliance purposes.

Individual coverage determination requests can be deleted. Note that if you delete a request, it can no longer be viewed by you. However, copies of all coverage determinations are maintained by CoverMyMeds for legal and compliance purposes and may be viewed by another Health Care Provider with access to the Request ID, the patient's last name, and the patient's date of birth.

What information is disclosed and/or shared with third parties?

We do not sell, rent, or share your information (identified or de-identified) with parties who are not affiliated with CoverMyMeds, except in rare situations when we believe we are permitted or required to do so by law. We may share the personal information you provide to us with trusted companies we

have hired to provide services for us, such as hosting our servers and collecting and processing information on our behalf. These companies — our vendors — are contractually bound to use personal information that we share with them only to perform the services we have hired them to provide and are required to comply with HIPAA's security provisions to protect such personal information.

We may share de-identified information you provide with our clients or prospective clients, mostly pharmaceutical manufacturers, who use this data to understand how our service is performing to make prior authorization easier to submit, and to improve their efforts at promoting our services to other Health Care Providers. We do not share any Protected Health Information (PHI) with our clients. We share limited demographic information about you and other users to our clients, specifically we share the type of user, a numeric ID, and a zip code/state, but include do not share your name, practice name, or employer.

We may also collect and group demographic and preferences information, responses to surveys and other personal information into an aggregated, non-personally identifiable form for disclosure to our clients, existing or potential business partners, affiliates, sponsors or other third parties. However, please be assured that this aggregate data will in no way personally identify you or any other visitors to the website. Other non-personally identifiable information that is collected through our use of "cookies" may be disclosed to our clients, existing or potential business partners, affiliates, sponsors or other third parties, but this aggregated data will in no way personally identify you or any other visitors to the website.

In some special circumstances, we may be required to share your information with third parties. For example, it is sometimes necessary to share general or personally identifiable information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of the Terms of Service, or as otherwise required by law. We reserve the right to share your information with third parties in such instances without first obtaining your consent.

Also, we may transfer information about you if CoverMyMeds LLC or covermymeds.com is acquired by or merged with another company, or in the event that CoverMyMeds files for bankruptcy. In such event, CoverMyMeds will notify you before information about you is transferred and becomes subject to another company's privacy policies.

Links to Other Sites

On covermymeds.com, we may provide links to other websites we believe are helpful to users of the application. For example, we may provide a link to a prescription drug company's website which contains a drug's Prescribing Information. When you click such a link on our site, you will be leaving covermymeds.com. Please be aware that the privacy policies of any third party sites you visit through links provided on this website, if any, may differ from this Privacy Policy. Therefore, you should consult the other sites' privacy policies, as we have no control over information that is submitted to, or collected or used by, these third parties.

How do we store data and maintain its integrity?

CoverMyMeds' internal staff, third party vendors, and hosting partners provide the hardware, software, networking, storage, security, backup, and related technology required to reliably and safely run covermymeds.com. Although CoverMyMeds owns the code, databases, and all rights to the

covermymeds.com application, you retain rights to the personal and patient data you submit through covermymeds.com. Ownership of website content is further described in our Terms of Service.

We retain your information for no longer than necessary to fulfill the purposes stated above, or for any period otherwise specifically required by law or regulation. After that time (or immediately, if your Business Associate Agreement is terminated, we will destroy your information in a manner reasonably certain to prevent loss, theft, misuse, or unauthorized access, except any information that CoverMyMeds has used and retains in an aggregated, de-identified fashion as described above, or if destruction is not feasible, in which case we will extend the protections of the Business Associate Agreement to such information.

How is information protected?

CoverMyMeds collects, stores, and uses personal information only with your permission, after you have agreed to the Terms of Service. If you withdraw consent to use the personal information you have provided, this will terminate the business relationship created when you agreed to the Terms of Service. CoverMyMeds will no longer share your personal information in an identifiable or de-aggregated form with any third party, and will destroy it promptly. You will no longer be able to access personal information by using the website.

Information you submit to our website is protected in several ways, including by the authentication of your username and password. Also, our "key-sharing" approach to move information from pharmacy or patient to a physician office (and vice versa) reduces the chance that Protected Health Information could be inadvertently disclosed to unauthorized parties.

All confidential information that is stored or transmitted by covermymeds.com is protected by 128bit SSL encryption, the same security used when you bank online. In addition, information processing and transfer complies with all health plan and other third party payer rules and HIPAA standards, if the website and CoverMyMeds' service is used in accordance with our Terms of Service. As already stated, we utilize the competencies of third party vendors and hosting partners to provide physical security and backup of data, and store our equipment at a secured facility designed for such purpose. Despite the security measures employed by CoverMyMeds, you should be aware that it is impossible to guarantee absolute security with respect to information sent over the Internet.

Are changes made to the Privacy Policy?

We reserve the right to update and/or change our Privacy Policy from time to time without prior notice. In the event that we update or modify this Privacy Policy, we will post the modified policy on this page, along with the date the Privacy Policy was last modified to identify when the policy was last revised. Changes are effective immediately so you are hereby advised to review this Privacy Policy regularly. The most current Privacy Policy for Health Care Providers will always be available at www.covermymeds.com/main/privacy_center. If you do not agree to the modified Privacy Policy, you should discontinue your use of our website, delete your account with us and terminate the Business Associate Agreement between us. For information on how to do so, please contact us at (866) 452-5017. Your continued use of the website shall constitute your acceptance of the terms of this Privacy Policy.

How can I ask questions or contact CMM?

We are happy to address questions about our Privacy Policy. Please send us your questions to privacymatters@covermymeds.com. Alternatively you may write to us at:

Privacy Matters
CoverMyMeds LLC
2 Miranova Pl.
Columbus, Ohio 43215
Effective Date: April 7, 2015