Last updated 01/07/2019

MyDispense Policies

This document describes policies relating to the use of MyDispense.

Contents

Introduction

MyDispense is an online pharmacy simulation tool that allows students to practice dispensing in a safe environment. The system is designed to allow learners to build knowledge, improve cognitive proficiency and develop professional values and attitudes.

Since its inception in 2010, MyDispense has had a significant impact on teaching at Monash Faculty of Pharmacy and Pharmaceutical Sciences. To date Monash students have completed over 146,000 dispensing exercises.

Since 2013 Monash has worked with international partners to make MyDispense available to other schools of pharmacy. In 2014 a strong collaboration with schools of pharmacy in the USA was established. Since then the use of MyDispense has grown enormously with the system now being used in over 75 schools of pharmacy across the world and over 500,000 exercises completed by students globally.

Last updated 01/07/2019

Terms and acronyms

MyDispense

An online simulated community pharmacy, developed by Monash University.

MyDispense core system

The code that is common to all MyDispense installations. The core code contains all of the common features to make the base version of MyDispense function properly. The base version of MyDispense is based on the Australian dispensing process.

Region overwrites

Files that modify the core code to adapt it to a specific region.

MyDispense Instance (aka 'instance' & 'production instance')

A single installation of MyDispense hosted on the Amazon AWS EC2 system. An instance includes the hosted virtual machine, the operating system, webserver & database stack and the MyDispense application.

Partner institution

A university, school of pharmacy or other organisation that partners with Monash University Faculty of Pharmacy and Pharmaceutical Sciences to share the MyDispense simulation.

Partner representative

The individual at a partner institution nominated as the principle contact for MyDispense notifications and correspondence.

Data owner

The individual or role at the partner institution that is responsible for the integrity of users' personal data on the partner instance.

Versions

A specific revision of the MyDispense software. MyDispense follows a Major.Minor.Revision version naming system. Major versions contain major features and breaking changes. Minor revisions include minor feature changes and improvements and revisions are for bug fixes and small improvements.

Authentication

The process of checking a user's credentials (username and password) when they login to MyDispense. There are two options for authentication:

- *Internal* – this uses the authentication system within MyDispense. Usernames and passwords are encrypted and stored within the system.
- *External*/SSO (single Sign On) – users are authenticated by the university's systems and the authentication pass/fail is sent to MyDispense.

Last updated 01/07/2019

How Monash works with partner institutions

How we share MyDispense

MyDispense is shared freely – there is no charge for an institution using the software for educational purposes. In addition, Monash provides hosting of the system for each institution (detailed below).

Each institution has its own 'instance' of MyDispense. An instance is essentially a virtual server, located in a data centre nearest to the geographic location of each partner institution. **Each instance is totally separate with no possibility for unintentional crossover of user data.**

Authorised MyDispense managers, based at Monash University, have access to each instance in order to provide technical support, upgrades and bug fixes. Normally there are two Monash manager accounts per instance, these accounts reside with the lead developer and the MyDispense project manager. No other Monash user accounts are routinely created on a partner instance.

What we do at Monash University

In addition to developing and updating the MyDispense software, Monash University carries out the following tasks for partner institutions:

1. Instance creation

Each partner institution receives a MyDispense 'instance'. Monash purchases each instance on the Amazon Web Services (AWS) platform. AWS has a cloud hosting service called Elastic Cloud Compute (EC2) [1], which provides secure and scalable virtual servers for our instances.

2. System setup

Monash performs the initial server setup and software installation to get MyDispense up and running. We then create a local administrator account, which is allocated to a nominated local member of staff. The local administrator is responsible for giving subsequent local users an appropriate level of access.

3. Authentication and Single Sign On

Monash will configure the local instance so that users can authenticate (login) to MyDispense via a secure login system. There are two options for authentication, internal and Single Sign-On (SSO).

- Internal authentication is performed within MyDispense and requires each user to be emailed with an activation link, for this reason users' email addresses are stored in the local MyDispense database.
- Single Sign-On requires users to login via their institutional portal, using their existing username and password. Monash works with local IT and security teams to set up a secure trusted relationship between MyDispense and the local SSO system; authentication is then managed by the local SSO system. SSO integration does not require the storage of user emails within MyDispense and is the preferred authentication method.

[1] Amazon EC2 Website

4. Customisation

Monash will perform customisation work on each instance in order to make it more locally relevant. The system is configured to conform to local dispensing practice and regulations. In addition, virtual patient and prescriber addresses are modified with local postal/ZIP codes etc. Occasionally, more detailed customisation work is carried out, such as language translation, but this is not routine.

Supporting MyDispense users

Monash provides detailed user guides and instructional videos to allow local users to quickly become proficient in the use of MyDispense. Monash also provides technical support via email. We will normally respond to queries within 24 hours. However, since MyDispense is a free service, we cannot enter into service level agreements to guarantee response times. To date, we have received much appreciation for our responsiveness and the quality of our support.

User data stored in MyDispense

The absolute minimum of personal information is stored in MyDispense - see table below:

User type	Data stored			
Staff	username	email address	Role (administrator, instructor or examiner)	
Student	username	email address*	metrics on interaction with the exercises within MyDispense	Exam performance (if applicable)

* If we integrate with a university's single sign-on system, we do not need to store student emails.

Last updated 01/07/2019

Acceptable Use Policy

MyDispense Code of Conduct

Users of MyDispense are bound by the following code of conduct:

- MyDispense will only be used for educational purposes.
- Users of the system are expected to keep their login information private.
- MyDispense must not be used for unlawful, offensive or otherwise improper activities.
- Content, such as medical images, added to MyDispense, should be free from third-party copyright. Alternatively, permissions should be obtained to use third-party party material.
- Inappropriate use should be reported to an appropriate authority within the local institution.
- Student users shall not copy content from the system (such as prescriber information, patient information, product images and voicemail recordings). Screen shots may be taken if permitted by local teaching staff.
- Student users are allowed to save and print PDF copies of their feedback from MyDispense.

Amazon AWS

In addition Monash University staff, responsible for MyDispense, are bound by the AMAZON AWS Acceptable Use Policy, which can be found on the AWS website at https://aws.amazon.com/aup/

Last updated 01/07/2019

Security Policy

System level access

Access to the operating system, database, webserver and other low-level components is restricted to selected Monash personnel only.

Shell access to MyDispense instances requires public key authentication. There is no password-only shell access to MyDispense instances. Keys to the servers are stored and backed up in a secure environment.

Firewall rules are as follows:

- HTTP/HTTPS access allowed from all servers
- SSH access only from selected IP addresses
- Nagios and SSH port access to our primary development / monitoring server.
    - These are for server monitoring and are only open to the monitoring server IP address.

Vulnerability Management

- We do not outsource development on MyDispense
- We restrict all remote administration access (SSH) to servers based on IP (firewall) and key-based authentication. This is to prevent shell access and installation of software as a basic precaution.
- All submitted data does not leave the server, except in the form of backups and rendering pages to a user.
- We employ mandatory https on servers with a hostname, either through LetsEncrypt or an institution issued HTTPS certificate.
- We have a monitoring system of all servers using Nagios.
- 3 keys exist that have Sudo access to production servers. They are kept on secure local storage only.
- We monitor CVE's, evaluate how they may affect us and, if necessary, implement fixes.
- All logins to MyDispense are logged.
- Firewall IP address whitelisting is used for SSH access.
- Note that by default users are able to sign up for a MyDispense account (which can be disabled), but new accounts have no access to any content until they have been enrolled in a unit. All new accounts created using this method are, by default, student accounts and have no access to admin functions.
- We monitor AWS status during outages.
- SSO - via SimpleSamlPHP and PHPCas, with custom solutions also Implemented.
- Note that access roles are defined inside MyDispense, not the SSO solution.
- For non-SSO login we have a password complexity check.

Last updated 01/07/2019

Privacy Policy

It is our policy to store as little personally identifying information (PII) and external information as possible for the running of MyDispense. MyDispense includes no external analytics libraries (such as google analytics) and each institution has its own server to ensure there is no data crossover.

The minimum personal data required for MyDispense is the username of each user. If users log in to MyDispense using the internal authentication system, then an email address is required for each user.

Data gathering

Data in MyDispense (outside of the external data noted elsewhere) is gathered only from use of the software. We do not use any third party data gathering libraries (such as Google analytics) and all resources required by MyDispense are hosted on the server itself. All images and scripts reside on the server and we have strict content policies (using web server configurations) to ensure that external resources cannot be loaded.

Privacy

Management of user accounts is the responsibility of the data owner at the partner institution. The data owner may have administrator access to the local instance of MyDispense or they may delegate that access to another person.

If a user requests to have their data removed from MyDispense, this is be considered to be at the discretion of the partner institution and subject to their regulations. Monash staff can advise and assist with the management of user data, but the final responsibility lies with the partner institution.

Monash staff will not create or remove user accounts without the written (e.g. email) authority of the partner institution.

Data storage

We store the following external data:

- Username
- Email Address
    - Required for non-SSO login
    - Only used to send account activation and password reset emails
- Password
    - Only required for non-SSO accounts.
    - SSO accounts will store no password information.
- IP address
    - Stored when logging each login to the system
    - Stored as the last ip address used after login
    - Stored when an assessment exercise is opened (to confirm that the student accessed that exercise and from where)
    - Stored when an exercise is submitted
    - Stored when an assessment is submitted
- Browser type (used for metrics and future development information)
    - Example: Firefox 45
    - Stored when an exercise is completed by the student

Administrator users may have their first name and last name entered, but it is not required by MyDispense. The name is used to help identify administrator users when providing access to exams and units.

Progress data

When a student submits an exercise, MyDispense will log that completion to two locations: `metrics` and `Exercises Students`. Internally `exercises students` is used to provide the student automated feedback on their completed exercise and stores all the data necessary to display that information. For example, the exercises student data would contain the labels that the student created during an exercise, so we can compare it against the exercise data.

When a student resets an exercise, the exercises student is cleared and the exercise is available for completion again.

`Metric data` contains a copy of the student username, along with a number of counts for each time they used a particular part of the software and other miscellaneous data (such as browser type and time taken to complete the exercise). For example a count may be the number of times the student opened the label screen.

Metrics are not removed when the student resets an exercise. So we can view a student's progress over time in MyDispense and determine how many exercises have been completed in MyDispense.

MyDispense will also store sections of feedback that the student got correct in a 1 (correct) or 0 (incorrect) format so general statistics can be formed of student performance. Currently we only use metrics to count the number of exercises completed on each MyDispense instance (counting the # of rows in the database table).

Institutions can use these metrics for research purposes (only on their own metric data) and Monash will provide these data on written request. For example, an institution may use metrics from a set of exercises to write a research paper on the effectiveness of MyDispense. Individual metric data will never be shared or provided to a different institution without permission.

A future feature may expose these metrics for consumption by administrators and students, who will be able to access only their own data.

Assessment data

For assessments we store student marks for each assessment criterion in an exercise. We also store the final marks and examiner's comments. These data can be exported to a CSV file and can also be exposed to students (individual students only) using the Assessment release feature (MyDispense 5.3+).

Last updated 01/07/2019

Change Control Process.

Change control is a systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, services are not unnecessarily disrupted and that resources are used efficiently.

Scheduled changes

The MyDispense product roadmap

The MyDispense product roadmap details the major developments, updates and enhancements planned for the software in the following 12 months. The product Roadmap will be published on the MyDispense website https://info.mydispense.monash.edu. The product roadmap sets the strategy for major and minor version updates.

The roadmap will be updated after every major or minor release of MyDispense. If a roadmap change occurs mid-development, partner institution representatives will be informed of the changes and feedback may be provided on the roadmap change.

MyDispense is developed by a very small team and we are unable to give a definitive release date for any feature.

User notification policy

Our policy is to keep all partner production instances on the same MyDispense version number. This greatly simplifies maintenance and updating of all our instances.

Partner institution representatives are notified in advance of all updates that contain major changes or changes that could disrupt teaching.

Changes are automatically pushed to production instances unless requested otherwise. Partner institution representatives may negotiate a deferred update time if the scheduled time is not convenient.

End users are notified of any updates or feature changes by the change information panel which appears after user login.

Any planned changes that involve the removal of existing features will involve partner representatives being notified first. If there is objection to the removal of a feature, this will be resolved by discussion with partner representatives.

Part of the upgrade process will involve an update of the relevant user documentation.

The changelog document, which is published on the MyDispense website, will be updated after a software update.

Unscheduled changes

Bug fixes

A bug fix is regarded as a repair to the MyDispense code where the fix does not alter the expected behaviour of the software. Users should not notice a bug fix unless they have experienced the bug themselves.

Bug fixes are an unscheduled change to the MyDispense code and are often given high priority in order to always have the software behaving as it should.

Bug fixes are automatically pushed to production sites without consultation with partner representatives unless the fix has User Interface implications, in which case a notification will go out before the fix is pushed.

Users are notified after a fix has been pushed by the change information panel which appears after user login.

Special requests

Partner representatives occasionally request minor additions to MyDispense functionality. These changes are by necessity:

- Easy and quick to implement.
- Required in a timely fashion where the inclusion of the feature into the product roadmap would entail too much of a delay.
- Of low impact to other users. Requested changes that alter the user interface significantly or that may cause confusion for established users will need to be included in the product roadmap.

Special requests often only affect the single instance of the requesting organisation.

Where a special request is implemented that has broader effect, users will be notified by the change information panel which appears after user login.

Last updated 01/07/2019

Disaster Recovery Plan

Backups

As part of our disaster recovery and risk management processes, we take backups of the MyDispense database and uploaded file data. Backups are taken to ensure that we can restore an institution's environment.

Occasionally, backups may be used temporarily for the purpose of testing, development and bug fixing. For example: A bug may be identified on an institution site that we are unable to replicate in our current development environment. We may then use a backup of that institution site and deploy it to a development site to login (using a secure development only login system) and troubleshoot that problem. This has happened several times in the past and is one of the main uses for backups. The development site is decommissioned immediately after the problem has been resolved.

Backups summarised:

- Backups will not be used for any other purposes than the above and will never be given to another institution without written consent.
- Database backups are taken nightly and file backups weekly (for files uploaded) for disaster recovery purposes.
- Backup data is currently only stored on Australian sites. If requested we can restrict this further.
- Backups may be used in development to fix bugs and investigate other issues. This also serves as a test function for backups
- Restore is simple using a database .sql file and copying webroot contents.

What data is taken in a backup?

- Database (via SCP)
  - Full .mysql file of the database, containing all tables and data.
  - Database backups happen nightly and monthly.
  - The nightly backups are retained for a week before being overwritten by a new backup from the next week.
    - For example, a backup taken on Monday the 1st will be overwritten by the backup taken on Monday the 8th.
  - Monthly backups are taken each month and are stored for a year and are overwritten by the next year's monthly backup.
    - For example, the June 2017 backup will be overwritten by the June 2018 backup.
- Files (using Rsync)
  - These are files uploaded as part of using MyDispense, such as images and documents.
  - File backups are taken twice a week and overwrite any changes made from the previous backup.
    - For example, if the backup taken on Monday has an image removed from the backup on Friday, that image will be removed from both backups.
  - The following files are backed up:
    - Rx Medication images
    - OTC medication images
    - Patient images
    - Prescriber signatures

- PDF attachments
- JPEG attachments
- Voice mails (.mp3)

Where are backups stored?

Backups are taken using two linux utilities SCP (Secure Copy) and rsync (over SSH). Both of these utilities use encrypted methods of taking backups and employ SSH key based authentication for security. Database backups are executed on each institution server using a scheduled job (cron) and the resulting backup is then transferred using SCP to our development server in Australia.

File backups are executed manually and involve running a script on the Development server. The development server then uses Rsync to connect to each production server and copies any changes to the uploaded files from each server and stores them separately. Once Rsync has been executed, all of the backups (including the database backups) are copied from the development server to one of two secure development machines.

For additional redundancy, the backups are replicated to other services to ensure that data-loss is less likely.

Those services are:

- Monash shared drive
  - Located in a private MyDispense folder where only administrators have access
- Dev backup NAS
  - Backed up using Apple Time Machine
- Backblaze
  - Cloud based data storage service

Metadata is gathered through use of the MyDispense software only. We use no 3rd party metadata systems

Note that by default users are able to sign up for a MyDipsense account (which can be disabled), but new accounts have no access to any content until they have been enrolled in a unit. All new accounts created using this method are student accounts and have no access to admin functions