Data Protection considerations

for Aviva DigiCare+ Workplace

An introduction to Aviva DigiCare+ Workplace

The information provided within this document will help your technical teams to understand the implications of Aviva DigiCare+ Workplace from a security perspective. Please note, the generic subjects listed are for guidance purposes only and are not exhaustive. If you have any additional questions that are not covered within this document, please email **digicare@aviva.com**.

Brief summary of Aviva DigiCare+ Workplace

The primary objective of Aviva DigiCare+Workplace is to provide your employees with access to a number of digital health services, which include an annual health check and health consultation, digital GP appointments with NHS registered private GP's, mental health and nutritional consultations and a second medical opinion service.

The Aviva DigiCare+ Workplace app has been built by Square Health Limited (Square Health), a third party provider.

Registration for the employer is by invitation only. The employer is then responsible for adding employee data.

NOTE: The service is a non-contractual benefit that Aviva can change or withdraw at any time.

Contents

Aviva due diligence

1. What high level supplier assurance framework does Aviva operate in?

Aviva have assessed the following terms of diligence from a risk and procedures perspective:

- system security
- clinical governance
- financial risk.

2. What activity does Aviva undertake when on-boarding new suppliers?

Aviva's on-boarding process covers:

- IT security
- data security
- financial security
- supply chain diligence
- sanction checks.

3. How does Aviva ensure that suppliers are legally bound to provide an adequate level of security protection to Aviva data or services?

Aviva's comprehensive contract covers all aspects of service delivery and supplier management.

4. What assessment is undertaken to assure that suppliers IT security processes are adequate?

Penetration testing is completed independently of the supplier, over and above the due diligence categories listed in question 1.

Contents

The collection of personal data

1. How will personal data be collected?

During the registration process, it is the role of the employer to share employees' email addresses with the service provider Square Health, by uploading data into the Square Health Customer Portal. Any personal data is collected via the mobile app with the permission of individual employees. This means that the employee is in complete control of the personal data Square Health receives.

It is the responsibility of the employer to upload employee email data.

After an employee has registered with Aviva DigiCare+ Workplace, they will be in control of any further data they provide in-app through the Aviva DigiCare+ Workplace services.

2. What data will employees be asked to provide?

Employees will be asked to share the following data with Square Health:

- Title
- First name
- Last name
- Date of birth
- Email address
- Home address
- Postcode
- Gender
- Smoking status

As part of your medical profile you may be asked to share the following data with Square Health:

- Current medications
- Chronic conditions
- Comorbidities
- Allergies
- Height
- Weight
- GP details

Contents

The collection of personal data

3. What security training is provided to staff at Square Health?

Security awareness training is provided within 6 weeks of the start of their employment and annually thereafter.

4. How else will Square Health use the personal data provided?

Square Health will only use employee personal data in accordance with their privacy policy. Most commonly, they will use personal data in the following circumstances:

- Where processing is necessary for medical diagnosis, the provision of health or social care or treatment.
- Where they need to comply with a legal or regulatory obligation.

Square Health will never share users' records to any third party not involved in the provision of services between us (other than if required for the purposes of improving medical care and services i.e. to the Care Quality Commission) unless they expressly consent to this (i.e. for continuity of care). More information can be found in the Square Health privacy policy, which you can find **here** and which is presented to users at the point of registration for Aviva DigiCare+ Workplace.

5. Are any categories of sensitive data collected?

Yes. At the point of booking a consultation, the Aviva DigiCare+ Workplace app provides users with the ability to input medical notes relating to symptoms, if they choose to.

In addition, Aviva DigiCare+ Workplace will collect and store medical notes data and call recordings, following a consultation. It will also collect data associated with the use of the private prescription service. Data will also be collected on any fit notes and referral letters provided to a user.

Where Square Health use special category data, including medical data, they are required to confirm any additional lawful basis for the processing of such data, which will most commonly include the following circumstances:

- Where processing is necessary for medical diagnosis, the provision of health or social care or treatment.
- Express consent that is freely, affirmatively and transparently given in respect of the processing described.

In addition to the data protection laws Square Health adhere to, they also respect the common law right of confidentiality in relation to a user's health and medical data.

Contents

The collection of personal data

6. Where will personal data be stored?

Health data is stored securely by Square Health using a world class leading platform that meets a broad set of international and industry-specific compliance standards such as ISO 27001, SOC 1 and SOC 2. All personal data is stored within the European Economic Area (EEA).

7. Will any personal data be made available by Square Health to Aviva or other third party providers?

Personal data that a user provides can only be accessed by authorised Square Health staff. Personal data, outside of that already provided to Aviva in the eligibility data, will not be made available to Aviva unless the user explicitly consents to this.

8. Will any personal data be made available to employers?

Employers will not be able to see any data relating to their employees' use of the service. Future development may allow employers to obtain management information data at an aggregated level, but this is not currently available.

9. Do Square Health hold an IS 663600 - ISO 27001 certificate?

Yes. You can view a copy of the certificate **here**.

10. Where is the Privacy Policy for the Aviva DigiCare+ Workplace mobile app found?

You can view the Privacy Policy **here**.

Contents

Customer Portal data and security

The Customer Portal, accessed through a browser, allows the Customer Manager (or administrator at the company) to:

- add and invite employees and maintain their information
- view and edit account information
- add and maintain users of Aviva DigiCare+ Workplace
- check the activity log for all its users
- trigger invitation emails to employees
- access promotional materials.

1. How do Square Health keep the Customer Portal data secure?

All confidential information is stored and communicated securely using industry leading, AES 256 end-to-end encryption. All access is controlled and audited through Square Health's internal systems.

2. What happens to the Customer Portal data if a user cancels their policy with Aviva?

Customer Portal data will remain held by Square Health for ten years.

3. What company data is stored in the Customer Portal?

The following company data stored in the Customer Portal:

- Company name
- Companies House number
- Business address
- Contact name for Customer Manager (or administrator at the company) plus additional customer portal managers
- Customer Manager email address
- Customer Manager phone number

Contents

Customer Portal data and security

4. What employee data is stored in the Customer Portal?

Only the employee email address is stored in the Customer Portal. This is the employees corporate email address, unless it is amended by the employee via their own mobile app to a personal email address.

5. Who can see Customer Portal data?

All portal managers (e.g. Customer Manager or administrator at the company) who are registered by the employer, as well as authorised Square Health personnel.

6. What MI can be exported from the Customer Portal?

The following MI can be exported:

- Employee first and last name (available once registered)
- Employee email address
- Employee app status

7. Who manages company employee data?

The employer (or administrator at the company) manages company employee data.

8. What are the terms and conditions of the Customer Portal?

The Customer portal terms and conditions can be accessed via the Customer Portal. You can view a copy **here**.

9. What web browsers is the Customer Portal accessible through?

The customer portal is a web-based service only and is not accessible via mobile applications.
It is available through the following web browsers:

- Chrome 55, 56, 57
- Safari 9, 10 (Mac only)
- IE 11 (Windows only)
- Firefox 52, 53, 54-
- Edge 14 (Chromium version Windows only)
- Chrome Mobile - Latest version
- Safari Mobile - Latest version
- Samsung Mobile - Latest version
- Chrome v49-53
- Safari 8 (Mac only)
- IE 10 (Windows only)
- Firefox 45-51

Contents

Customer Portal data and security

10. Where is Customer Portal data stored?

Data for Aviva DigiCare+ Workplace is held by AWS (Amazon Web Services) in UK – London & Ireland.

11. What happens to employee data once a user is de-registered?

The employee will be able to access their personal information held within the Aviva DigiCare+ Workplace app for 12 months from de-registration.

12. Where is the Privacy Policy for the Customer Portal found?

The Customer Portal Privacy Policy can be found **here**.

13. How is data retained for a leaver?

Data is retained securely and in accordance with Square Health's Privacy Policy. If a user wants to request data held in the Aviva DigiCare+ Workplace app they can request this via the app within 12 months of the day their account was de-activated or de-registered.

14. Is personal identifiable information stored, managed and/or accessed?

Yes, all details are fully encrypted and stored electronically. Only authorised Square Health staff can access the personal data and information stored from previous appointments. Square Health will not share any medical information with Aviva, the employer, or any other third party, unless the employee consents for them to do so. The private GP will only share medical notes with an NHS GP for the purpose of continuity of care if the patient gives express permission for them to do so. If the employee closes their account, Square Health holds their details in line with their Privacy Policy.

Contents

The processing of personal data

1. For what purpose(s) will collected personal data be processed?

Square Health may also use personal data provided to communicate updates to employees relating to Aviva DigiCare+ Workplace.

Personal data will also be processed by Square Health to create a personalised profile for the user and drive the user experience.

2. Is Square Health a data controller?

Square Health is a data controller. This means that Square Health will collect and process employee information in the ways described in the **privacy policy**. Square Health use RSA encryption to transfer information between a user's device and the Square Health servers. All data is encrypted at rest, which means the data stored on their systems has been encrypted.

3. What are the password processes for the end user?

Users can choose to change their password in-app at any time, and if they reset their password using a link on the login page, they will be provided with a system-generated strong password. Square Health can change passwords at the back-end, and upon doing so will invalidate any current mobile session. Passwords are required to be greater than 8 characters using at least three combinations of strength enhancing characters (upper case, lower case, special and numerical). Passwords are not subject to forced expiry. Passwords are also hashed and encrypted.

4. What are the password processes for Square Health?

Square Health operates a privileged systems access which is subject to passwords of greater than 8 characters using at least three combinations of strength enhancing characters (upper case, lower case, special and numerical). Passwords are subject to forced expiry after 60 days, and 5 failed logins will trigger a lockout. Passwords are also hashed and encrypted.

Contents

The processing of personal data

5. What documented policies, standards and procedures and guidelines are maintained by Square Health?

Square Health have a documented Information Security policy, Information Security standards, and Mobile Application Development standards, as well as comprehensive privacy policies. The corporate (or intermediary) can request copies of these documents by emailing **digicarehelp@squarehealth.com**

Contents

Employee data rights

1. How is personal data kept up to date and accurate?

During the registration process, the employee is responsible for the accuracy of personal data. Once an eligible employee has created an Aviva DigiCare+ Workplace account, they are responsible for keeping their information up-to-date within the app.

2. Is there a way for users to request a correction of inaccurate or incomplete data?

Users can contact Square Health on **digicarehelp@squarehealth.com** to do so.

3. Is there a way for users to request access to their data, or for personal data to be deleted upon request?

Users have legal rights under data protection laws in relation to their personal data. Information about how users can exercise their rights and information about data retention can be found in the Square Health privacy policy, which you can find **here**.

4. Is there a way for a user to withdraw consent?

If a user wishes to withdraw consent, they can do so by closing their Aviva DigiCare+ Workplace account through the relevant settings page within the app. By closing their account, they will no longer have access to the Aviva DigiCare+ Workplace services.

5. Is there any automated profiling within the app, and can users request they are not subject to this decision making?

There is no automated decision making within the Aviva DigiCare+ Workplace app.

Contents

Data retention policy

1. Is there a retention policy for all personal data?

Data is held by Square Health for 10 years in accordance with NICE guidelines.

In the event that a user's eligibility for Aviva DigiCare+ Workplace ceases, they will retain 'read only' access to ensure they are able to access their medical history through the service.

Where Square Health have anonymised personal data, or collected aggregated data for research or statistical purposes, Square Health may continue to use that data indefinitely without further notice to you or the user, as applicable.

2. How do users make a subject access request?

Users can ask Square Health for a copy of all the personal information they hold about them. They can contact Square Health at the below address:

Email: **data.protection@squarehealth.com**

Write to: **The Data Protection Officer at Square Health Limited, Crown House, William Street, Windsor, Berkshire SL4 1AT**

Contents

More about the Aviva DigiCare+ Workplace app

1. What type of application is Aviva DigiCare+ Workplace?

Aviva DigiCare+ Workplace is a Native Mobile Application.

2. Which mobile application best practice does the Aviva DigiCare+ Workplace adhere to?

The Aviva DigiCare+ Workplace service adheres to the SDLC policy aligned to ISO27001.

3. How is data encrypted?

Data is encrypted during transit using HTTPS, and at rest with AES 256 end-to-end encryption. Personal Identifiable Information is not stored on the mobile device.

4. How is data protected?

Production data is not available to developers or used in a non-production environment. Intrusion protection and detection systems are in place. Infrastructure penetration and application testing is carried out at least annually.

5. What authentication is used?

Native Application Controls are used to authenticate access to the application, via username and password. Passwords are hashed using SHA-256 or stronger. Once a user has registered on the Aviva DigiCare+ Workplace app, biometric authentication (such as fingerprint ID or facial recognition) can be activated in-app, if the device they are using supports this. Authentication credentials are stored on the device using AES 256 end-to-end encryption.

6. What alternative accessibility provisions are in place within the app for customers with additional support requirements?

All audio within the app is live (during video consultations with the medical professional) therefore captions or text alternatives are not applicable. Use of colour is not used as the only visual means of conveying information, indicating an option, prompting a response, or distinguishing a visual element. Text and colour can be amended with contrast and size depending on the user's own device settings, and text is used to convey information rather than images of text where appropriate. Pages do not contain any content which flashes more than three times in any one second period. Flash is below the general flash and red flash thresholds.

Contents

More about the Aviva DigiCare+ Workplace app

7. Where is the Privacy Policy for the Aviva DigiCare+ Workplace mobile app found?

You can view the Privacy Policy **here.**

8. Where are the terms and conditions for the Aviva DigiCare+ Workplace mobile app found?

Terms and conditions can be viewed within the app when a consultation is booked or when registering for access to the Aviva DigiCare+ Workplace app.

9. What type of testing is performed?

Full penetration testing of the Aviva DigiCare+ Workplace app has been carried out using an independent CREST accredited company and will be carried out in future as part of an annual cycle. Any vulnerabilities identified, including during annual cycles, are assessed and treated for the risk that the vulnerabilities pose. Due to the sensitivity of the content, we are not able to share copies of the reports.

10. What Business Continuity and Disaster Recovery Plans are in place?

Business Continuity and Disaster Recovery plans for Square Health exist and are reviewed every three months and tested every six months. Data is recovered from the latest back up of up to 24 hours should the system fail. This recovery from system failure can take between 0-72.hours.

11. What are the public URLs for the app and play stores?

For iTunes (iOS): **https://apps.apple.com/gb/app/aviva-digicare-workplace/id1531444866**
For Google Play: **https://play.google.com/store/apps/details?id=co.uk.aviva.app.group**

12. Is systems access controlled by unique IDs?

Yes, systems access are controlled by unique IDs.

13. How often are user and system accounts reviewed and approved for appropriateness?

User accounts and system accounts are reviewed every three months.

Contents

How to contact us

If you have any further questions or would like more information about Aviva DigiCare+ Workplace, please get in touch with your usual Aviva contact, employee benefits adviser or financial adviser. Alternatively, you can visit **aviva.co.uk**.

GR06381 07/2022