Dated: 17 August 2017

Data Security and Confidentiality Policy
Appointment Connector

Introduction

Maintaining security and confidentiality of appointment data is a priority at HealthEngine.

This document outlines data policies set by HealthEngine to maintain the integrity of appointment data transmitted between our servers and your health practice when using the **Appointment Connector**.

These data policies have been approved by:

Dr Marcus Tan
Founder, CEO & Medical Director, HealthEngine

Marcus is an experienced healthcare executive and company director with 20 years of clinical and commercial experience in startup and publicly listed organisations.

A Fellow of the Royal Australian College of General Practitioners with an Executive MBA from the Australian Graduate School of Management, Marcus has held senior management positions as Medical Director and Managing Director for a national clinic group and a health management consultancy.

A Fellow of the Australian Institute of Company Directors and Australian Institute of Management, Marcus has chaired and held director roles for over a decade with the Divisions of General Practice, GP Networks and Medicare Locals. He currently serves on the executive council of the Australian Medical Association (WA) and is a director and data/eHealth Lead for the WA Primary Health Alliance, chairing the Metro South WA Primary Health Network.

Marcus is a board member of the CRC for Spatial Information (Health) and an Adjunct Associate Professor in Health Leadership & Management at Curtin University.

Dated: 17 August 2017

Data Security

HealthEngine minimises the amount of data transmitted between our servers and your PMS. Data is always transmitted using Transport Level Security (TLS) on an as-need basis. Sensitive data is encrypted at rest, within the database.

HealthEngine web sites and mobile application are subject to penetration testing and security reviews, adhering to stringent Australian Digital Health Agency operating standards.

Appointment Connector and SideBar software packages are digitally signed to prevent tampering. The download manager ensures software dependencies, such as encryption libraries, are kept up-to-date.

HealthEngine does not transmit or store data from your PMS other than that outlined herein.

Data Usage

Collection of Appointment Availability Data

The Appointment Connector collects appointment availability data from your practice management software (PMS) in order to synchronise available appointments between HealthEngine and your PMS. HealthEngine only has knowledge of the available time slots for the practitioners at your health practice.

Importantly, no de-identifiable patient information is collected.

Insertion of Booked Appointment Data

The Appointment Connector can optionally insert details of an appointment booked via HealthEngine into your PMS, and match a booked appointment to an existing patient record or create a new patient record if one is not present.

HealthEngine uses patient data collected from our booking form for transmission to and insertion into the PMS, and optionally extracts basic patient contact details from your PMS and non-sensitive details, to assist with matching a booked appointment to an existing patient record.

HealthEngine does not gather or utilise any other patient data from the PMS for this purpose.

Patient Communication Data

From time to time, and with your consent, HealthEngine offers a Patient Communication service to educate patients about availability of online bookings at your practice.

To facilitate this service, the Appointment Connector is required to fetch the names, mobile numbers, e-mail addresses, age, and time of last appointment for your patients, strictly for the purpose of allowing HealthEngine to determine eligible recipients and to act as a messaging gateway for the patient communication campaign. No other identifying information or medical information is sought in this process.

All information is transmitted securely to HealthEngine, and no information is ever passed on to a third-party.

Patient Medical Records

With your consent HealthEngine is able to offer value added services to patients and practitioners, such as medication management and unified communications.

To facilitate such optional services, and with explicit consent from the patient, the Appointment Connector extracts medical history, strictly for the purpose of allowing HealthEngine to act as a messaging gateway. No other identifying information or medical information is sought in this process.

All information is transmitted securely to HealthEngine, and personal health information is not disclosed to third parties.

HealthEngine does not collect or store any other patient data from the PMS for this purpose.

Data Storage

Appointment Data

HealthEngine securely stores basic appointment availability data (date, time, appointment length, and practitioner name) on the HealthEngine servers to facilitate the process by which patients book an appointment via the HealthEngine website, HealthEngine mobile apps, and associated practice website plug-ins and mobile apps.

HealthEngine does not collect or store patient data from the PMS for this purpose.

Patient Communication Data

If you have opted into the Patient Communication service, HealthEngine is required to securely store the names, mobile numbers, e-mail addresses, age, and time of last appointment for your patients on the HealthEngine servers, strictly for the purpose of allowing HealthEngine to determine eligible recipients and to act as a messaging gateway for the patient communication campaign.

HealthEngine does not collect or store any other patient data from the PMS for this purpose.

Patient Medical Records

By opting into value added services, and having obtained explicit consent from the patient, HealthEngine is required to securely store encrypted medical data received from the Appointment Connector, strictly for the purpose of allowing HealthEngine to act as a messaging gateway. Only the designated recipients will have the ability to decrypt such data.

HealthEngine does not collect or store any other patient data from the PMS for this purpose.

If you have any questions about our data policies, please do not hesitate to contact us via e-mail at info@healthengine.com.au or call us on 1300 377 639.