HeartFocus

HeartFocus Deployment and Security White Paper

Published
November 2025

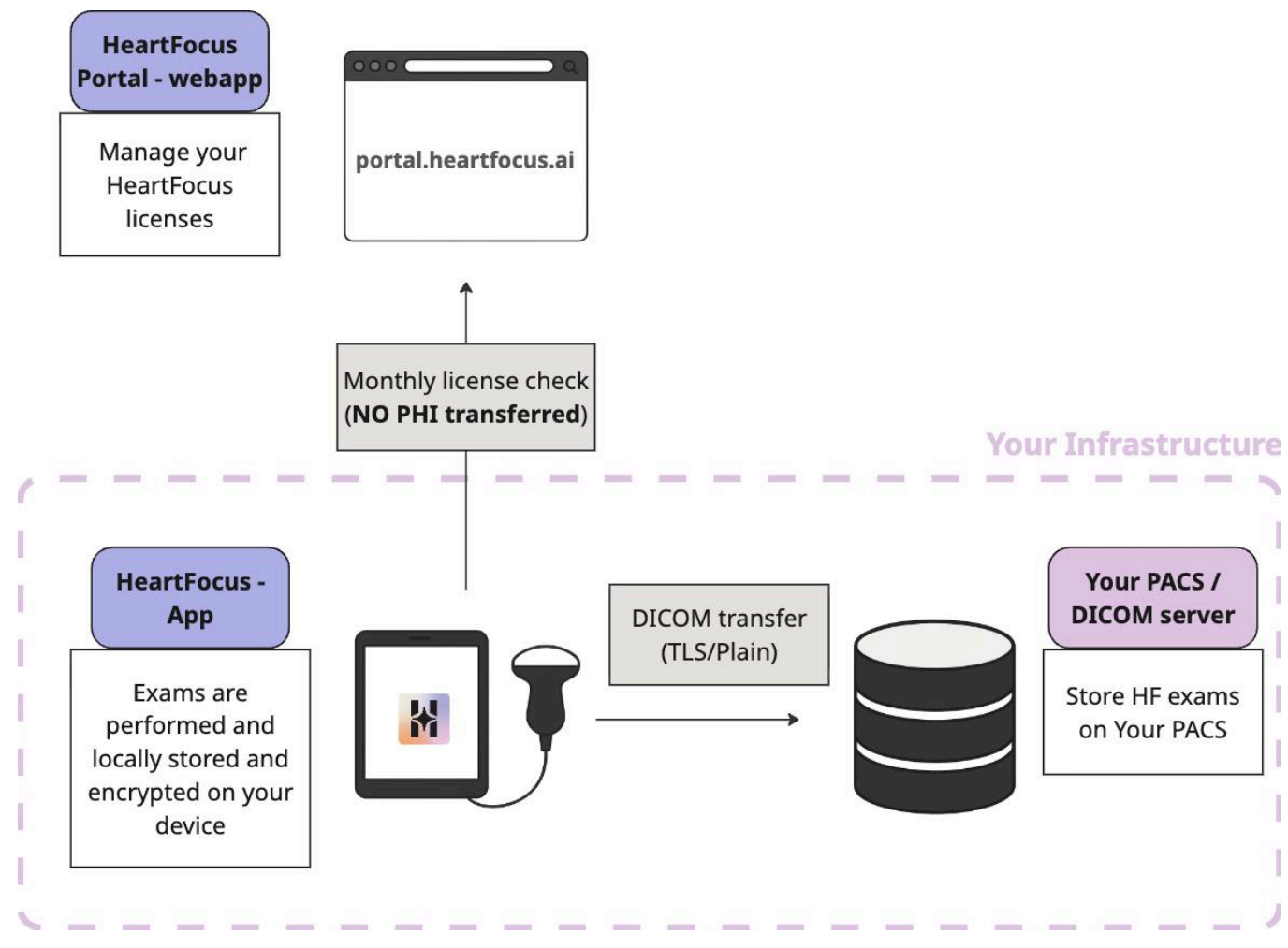
DESKi

Executive Summary

HeartFocus is an **FDA-cleared** iPad application developed by **DESKi** that provides real-time AI guidance to acquire cardiac ultrasound exams. The app runs fully on-device, with no cloud processing.

- **Secure, Offline Workflow :** HeartFocus works entirely offline; it only needs internet access once every 30 days to verify the probe-linked software license (no PHI involved).
- **No PHI Ever Sent to DESKi :** All scans stay encrypted on the iPad. DESKi does not access, collect, store, or transmit any patient data.
- **Simple License Model via HeartFocus Portal :** Licenses are tied to ultrasound probe serial numbers, not user accounts. The HeartFocus Portal is used only for license purchase and probe–license linking, and contains no patient data.
- **Hospital-Controlled DICOM Integration :** Operator or Sites configure their own PACS endpoint. HeartFocus sends scans via DICOM C-STORE using customer-selected settings (TLS or plain). DESKi does not operate any servers in the clinical workflow.

Bottom line: HeartFocus is FDA-approved, secure by design, PHI-free, and integrates cleanly into existing PACS workflows without adding infrastructure or additional risk.



Introduction

This white paper is intended for customers who are interested in, or currently integrating the HeartFocus product into their hospital IT environment.

We provide an overview of HeartFocus network infrastructure, network architecture, and security controls that will help your institution navigate a successful integration.

This document is targeted at clinical, IT, and security professionals. Portions of this document will assume familiarity with network architectures, operating systems, encryption, and security controls.

Echocardiography & HeartFocus

Echocardiography is a non-invasive medical imaging technique that uses standard ultrasound technology to visualize the heart. It allows clinicians to assess the heart's structure and function, measure its size, evaluate pumping strength, and detect a wide range of cardiac abnormalities.

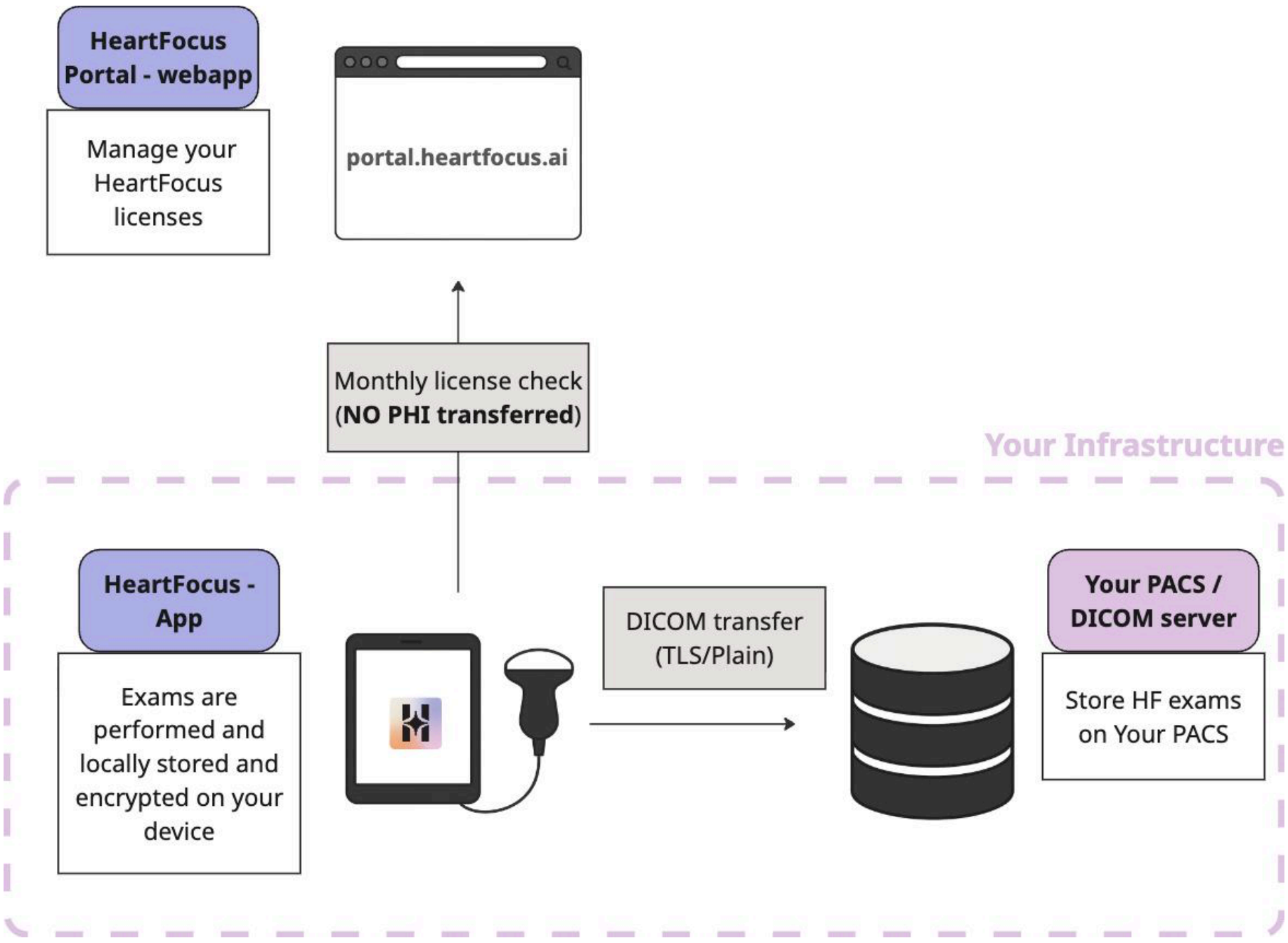
The HeartFocus software is an app that provides real-time user guidance during echocardiography to assist the user in acquiring anatomically standard diagnostic-quality 2D echocardiographic views. It supports the acquisitions of 10 echocardiographic views, including Parasternal Long-Axis (PLAX) and Apical 4-Chamber (A4C). The collected exams can be transferred between experts and sites using DICOM protocols.

HeartFocus assistance operates entirely offline, without requiring a cloud server to provide its core functionalities. All collected medical data/PHI is stored locally on the user's tablet. This data is never transferred to a server controlled by DESKi.

HeartFocus Product Ecosystem

The HeartFocus product ecosystem comprises the following components:

1. HeartFocus iPad App installed on your iPads
2. HeartFocus Portal
3. DICOM Connection (TLS or Plain)
4. Your PACS inside your infrastructure



HeartFocus iPad App

HeartFocus App can be downloaded from the Apple App Store. HeartFocus App supports in real-time the acquisition of cardiac ultrasound images.
When the examination is complete, HeartFocus App enables file saving and sending of all the entire ultrasound exam to a DICOM server. The DICOM server configuration can be specified by the hospital IT team in the HeartFocus App settings.

HeartFocus Portal

HeartFocus may currently be used with Butterfly iQ+/iQ3 Probes once these are linked to a valid HeartFocus software license. License management is performed on the HeartFocus Portal website, where users can purchase licenses and link licenses to the Butterfly iQ+/iQ3 Probes using their probe serial number. The HeartFocus software license is attached to each ultrasound probe and not to the user account.

DICOM Connection (TLS or Plain)

The HeartFocus App can be configured so that the user can send the exam to the hospital PACS/DICOM server over a TLS or a Plain DICOM connection.
The DICOM server configuration can be specified by the hospital IT team in the HeartFocus App settings.

Secure by design

This section will provide a high-level overview of how HeartFocus is secure by design.

Major Data and Network Questions Answered

The subsequent table addresses key inquiries regarding data and network aspects.

Question	Answer
Does HeartFocus App transmit any PHI to the Cloud?	No, HeartFocus App operates on the device (i.e. offline) and stores exams on your device locally. No PHI is sent to the cloud during scanning. Nevertheless, you may send your exam files to a PACS system by using the built-in DICOM connection.
How are patient scans stored and protected?	Scans are stored and encrypted locally on the mobile device belonging to the hospital. No PHI data is sent to DESKi servers.
How does the HeartFocus App communicate with PACS?	The HearFocus App can be configured to work with your PACS setup via a DICOM connection. DICOM TLS is supported.
How does the HeartFocus App check the software license?	HeartFocus App checks the HeartFocus software license validity every 30 days by contacting the HeartFocus Portal.
Does the HeartFocus App need an internet connection?	HeartFocus operates entirely offline, without requiring a cloud server to enable its core functionalities. However, the App does require an internet connection at least every 30 days to verify the HeartFocus Software license validity.

HIPAA compliant

By design, the HeartFocus App is designed so that DESKi does not receive, maintain, or transmit Protected Health Information (PHI) on behalf of any covered entity or business associate. As such, HIPAA regulations do by default not apply to our operations.

Separation of concerns

The HeartFocus Portal only provides license management (probe serial number ↔ license; admin identity like name/email/phone). The Portal holds no patient data.

Login-less workflow

Clinicians don't need a login to use the HeartFocus App. Licensing is validated against the probe serial number when scanning.

Secure Development Lifecycle (SDLC)

DESKi follows a "secure by design" approach whereby security is treated as a top priority at all stages of HeartFocus and application development. We implement controls such as threat modeling, code review, regression testing, static code analysis, vulnerability scanning, SBOM on request, and penetration testing.

Coordinated Vulnerability Disclosure (CVD)

At DESKi, we believe that collaboration with the security community is essential for maintaining the highest standards of safety and security for our HeartFocus product. Our Coordinated Vulnerability Disclosure (CVD) program provides a clear framework for security researchers and other third parties to responsibly report potential vulnerabilities.

This approach ensures that any identified security issue is addressed and resolved by our team before it is publicly disclosed, preventing potential exploitation and protecting our customers and their patients. We are committed to working transparently and constructively with anyone who submits a report.