THE ROYAL VICTORIA EYE AND EAR HOSPITAL DUBLIN

Request for Quotation # RVEEH-004-26

Self-Service Kiosk Terminals, Kiosk OS Integration, and Associated Software Licensing

Schedule A—The Requirements

29 July 2026
Date of Publication

7 August 2026, 16:00:00h GMT
Deadline for Questions

26 August 2026, 13:30:00h GMT
Deadline for Submissions

Schedule A—The Requirements

This RFQ contemplates the provision of a self-service patient check-in kiosk solution, kiosk operating system configuration, patient-system integration, associated software licensing, implementation services, annual support and maintenance, and optional hosting and patient-call/display functionality. The Successful Respondent will provide a complete, secure, supportable and operational solution suitable for use in a public healthcare environment.

Respondents are invited to provide information on solutions which deliver the following:

1—General Requirements

1.1 The Supplier shall provide a complete solution comprising, as applicable:

a. four (4) kiosk units / hardware
b. backend software/application
c. frontend/kiosk client software/OS
d. integration, configuration, & implementation services
e. end-user training
f. go-live Support
g. go-live on or before 31 December 2026;
h. annual support & maintenance;
i. hosting/cloud charges (as the case may be); and
j. past experience with solution integration in an HSE Hospital or similar environment.

1.2 The Supplier shall ensure that the proposed solution is suitable for deployment in a public healthcare environment and can be supported for the duration of the Contract Term and any Option Period(s) exercised.

1.3 The Supplier shall identify all assumptions, dependencies, exclusions, third-party products, third-party services, hosting dependencies, licences, support limitations and implementation prerequisites within its Response.

2—Functional Workflow Requirements

2.1 Respondents shall describe how the proposed solution supports patient check-in and related front-of-house workflows.

2.2 The response should address, where available:

a. patient identification and validation;
b. check-in confirmation;
c. appointment/clinic/session selection;
d. patient instructions and on-screen messaging;
e. waiting-room or queue-management support;
f. exception handling where a patient cannot complete check-in;
g. administrative visibility or reporting;
h. multilingual support, where available;
i. accessibility support;
j. privacy safeguards for patient-facing screens; and
k. configurable workflows by clinic, location, department, session type or patient pathway.

3—Kiosk Hardware Requirements

3.1 Respondents shall provide a specification for each proposed kiosk model, including:

a. kiosk form factor, dimensions and mounting method;
b. screen size and screen type;
c. touch-screen technology;
d. processor, memory, and storage;
e. operating system;
f. integrated scanner, printer and/or peripheral devices;
g. network connectivity;
h. power requirements;
i. physical security features;
j. accessibility features;
k. warranty period;
l. expected useful life;
m. replacement-parts availability; and
n. cleaning, infection-prevention and maintenance instructions.

3.2 The minimum expected hardware profile is a patient-facing self-service kiosk with a touch screen, integrated or associated receipt/thermal printer, a stable floor-mounted configuration and/or desk/table configuration, where proposed, with hardware suitable for repeated use in a public hospital environment.

3.3 Respondents may propose alternative kiosk models or configurations where they meet or exceed the functional, accessibility, security and operational requirements of this RFQ.

4—Kiosk Operating System & Endpoint Configuration

4.1 The Supplier shall describe the proposed kiosk operating system and endpoint configuration.

4.2 The solution shall support secure kiosk-mode operation, including as applicable:

a. restriction of user access to authorised kiosk functions only;
b. prevention of unauthorised operating system access;
c. automatic application launch and recovery after restart;
d. controlled update and patch management;
e. peripheral/printer driver management;
f. logging and monitoring of kiosk status;
g. remote support arrangements approved by RVEEH;
h. local user/account hardening
i. EN 301 549 compliance;
j. WCAG 2.2 Level AA compliance;
k. secure network configuration; and
l. physical and logical security controls appropriate to a patient-facing device.

4.3 Respondents shall identify any RVEEH ICT dependencies, including network ports, firewall rules, certificates, device-management requirements, domain requirements, remote-access requirements, antivirus/endpoint protection assumptions and any local administrator access required.

5—Frontend & Backend Software & Licensing Requirements

5.1 Respondents shall identify and price all software components required for the proposed solution, including as applicable:

a. check-in server/application licence;
b. kiosk client licence;
c. integration/interface licence;
d. patient-call/display/multimedia module licence;
e. media player or screen client licence;
f. annual software support and maintenance;
g. hosting or cloud service charge;
h. database or middleware licence;
i. third-party software licence; and
j. any additional licence required for production, test, backup, disaster recovery or support environments.

5.2 Respondents shall state whether each licence is perpetual, subscription-based, annual, named-user, concurrent-user, device-based, transaction-based, server-based, module-based, or otherwise calculated.

5.3 Respondents shall identify all one-time and annual/recurring charges and the basis on which those charges may increase during the Contract Term and any Option Period(s).

5.4 Respondents shall identify whether RVEEH may add additional kiosks, screens, clients, modules or licences during the Contract Term and the pricing basis for such additions.

6—Patient-System Integration Requirements

6.1 The solution shall support integration with RVEEH's patient administration, scheduling and/or patient management environment as required by RVEEH.

6.2 Respondents shall describe their interface approach, including:

a. HL7 or equivalent interface capability;
b. directionality of data flow;
c. patient lookup/check-in workflow;
d. appointment or attendance matching;
e. handling of cancelled, rescheduled or missing appointments;
f. error-handling and exception workflows;
g. interface monitoring;
h. audit logging;
i. data validation;
j. test environment requirements;
k. cutover and go-live approach; and
l. support and troubleshooting arrangements.

6.3 The Supplier shall provide interface setup, local interface configuration, testing and sign-off services sufficient to place the agreed integration into operational use.

7—Hosting, Cloud, & Data Residency

7.1 Respondents shall state whether the proposed solution is locally hosted, Supplier hosted, Cloud hosted, hybrid, or otherwise deployed.

7.2 Where Cloud or Supplier-hosted services are proposed, Respondents shall identify:

a. hosting provider;
b. hosting region/country;
c. backup region/country;
d. data residency;
e. sub-processors;
f. support access locations;
g. disaster recovery arrangements;
h. business continuity arrangements;
i. encryption arrangements;
j. monitoring arrangements;
k. data retention and deletion arrangements;
l. exit/transition arrangements; and
m. any data transfer outside Ireland, the EEA or the United Kingdom.

7.3 Any hosting arrangement shall be subject to RVEEH security, ICT, data protection and governance approval before implementation.

8—Cybersecurity & Data Protection Requirements

8.1 Respondents shall describe the security controls applicable to the proposed solution, including:

a. user and administrator access controls;
b. authentication and authorisation model;
c. role-based access, where applicable;
d. audit logs;
e. encryption in transit;
f. encryption at rest, where applicable;
g. vulnerability management;
h. patch management;
i. secure remote support;
j. backup and restoration;
k. incident notification;
l. data minimisation;
m. data retention and deletion;
n. subprocessor management; and
o. support for RVEEH's compliance with applicable Data Protection Laws.

8.2 Respondents shall identify whether the solution processes patient-identifying data, appointment data, attendance data, contact details, location data, device logs, support logs or any other personal data.

8.3 Respondents shall provide sufficient information to support RVEEH's completion of any required security assessment, data protection assessment, Data Processing Agreement and/or DPIA.

9—Implementation, Testing, Training, & Go-Live

9.1 Respondents shall provide an implementation approach covering:

a. project management;
b. kick-off and discovery;
c. workflow design;
d. technical design;
e. hardware delivery and installation;
f. software configuration;
g. operating system configuration;
h. integration/interface setup;
i. testing;
j. user acceptance testing;
k. administrator and key-user training;
l. go-live readiness;
m. go-live support; and
n. transition to support.

9.2 Respondents shall identify estimated timelines, RVEEH dependencies, required RVEEH resources, risks, assumptions and required decision points.

9.3 Go-live shall be subject to completion of agreed testing and RVEEH acceptance of go-live readiness.

10—Support & Maintenance

10.1 Respondents shall provide a support model for the full solution, including:

a. software support;
b. kiosk client support;
c. integration/interface support;
d. operating system support responsibilities;
e. hardware warranty and maintenance;
f. printer/peripheral support;
g. hosting support, where applicable;
h. security update and patching responsibilities;
i. support hours;
j. incident severity levels;
k. response and resolution targets;
l. escalation process;
m. account management; and
n. service review arrangements.

10.2 Respondents shall identify any support exclusions, consumables exclusions, travel/expense charges, out-of-hours charges, remote-support limitations or dependencies on RVEEH ICT resources.

11—Reporting, Hardware, & Software Performance Requirements

11.1 The Supplier shall provide reporting services as reasonably required by RVEEH, which may include:

a. administrator dashboard;
b. support incidents;
c. uptime/availability;
d. kiosk availability;
e. interface incidents;
f. transaction/check-in volumes, where available and approved;
g. service-level performance;
h. security incidents;
i. patch/update history;
j. hardware faults;
k. training delivered;
l. change requests; and
m. outstanding risks or issues.

11.2 The Supplier shall participate in service review meetings on a quarterly basis or as reasonably requested by RVEEH.

12—Environmental, Accessibility and Operational Requirements

12.1 Respondents shall describe environmental and sustainability considerations, including energy consumption, packaging, hardware lifecycle, replacement parts, reuse/recycling options and end-of-life disposal.

12.2 Respondents shall describe how the proposed kiosk solution supports accessibility for patients and safe use in a public hospital environment.

12.3 Respondents shall identify any cleaning, infection-prevention, physical safety, or public-area operational considerations relevant to the proposed hardware.

13—Optional Patient-Call, Display and Multimedia Module(s)

13.1 Respondents may propose optional patient-call, waiting-room display or multimedia display functionality.

13.2 Where proposed, Respondents shall describe:

a. patient-call number or identifier display;
b. wait-time or location display;
c. screen/client licensing;
d. display hardware requirements;
e. media player requirements;
f. bracket/mounting requirements;
g. content management;
h. configuration and support model;
i. annual support charges; and
j. whether the module is required for the core solution or optional.