

Hà Nội, ngày 10 tháng 7 năm 2026

THƯ MỜI CHÀO GIÁ

Kính gửi: Các đơn vị cung cấp

Viện Huyết học - Truyền máu Trung ương có kế hoạch mời đơn vị thực hiện nội dung công việc: Xây dựng ứng dụng di động “Hiển máu”.

Kính mời các đơn vị cung cấp gửi báo giá cho Viện theo nội dung cụ thể như sau:

I. Nội dung yêu cầu gửi báo giá:

1. Đơn vị yêu cầu gửi báo giá: Viện Huyết học - Truyền máu Trung ương.
2. Mục đích báo giá: Làm cơ sở xây dựng giá kế hoạch.
3. Thời gian nhận thư chào giá: trước 16h00 ngày 20 tháng 7 năm 2026. Các báo giá nhận được sau thời điểm trên sẽ không được xem xét.
4. Yêu cầu báo giá:
 - Về giá: Theo thị trường đã bao gồm thuế VAT và tất cả các loại thuế, phí và lệ phí liên quan đến nội dung công việc.
 - Báo giá có hiệu lực tối thiểu 90 ngày kể từ ngày phát hành, trong báo giá ghi rõ số điện thoại liên hệ của Quý Công ty.
 - Đơn vị chào giá gửi kèm bản sao giấy phép đăng ký kinh doanh.
 - Báo giá phải được ký và đóng dấu.
5. Các thức tiếp nhận báo giá:
 - Hình thức: Gửi trực tiếp hoặc theo đường bưu điện.
 - Địa điểm nhận báo giá: Phòng Văn thư (phòng 132, tầng 1, Nhà H), Viện Huyết học - Truyền máu Trung ương, số 5 Phố Phạm Văn Bạch, Phường Cầu Giấy, Hà Nội.

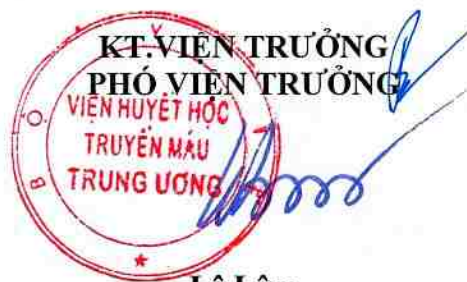
II. Yêu cầu kỹ thuật:

Chi tiết theo phụ lục đính kèm

1. Loại hợp đồng: Hợp đồng trọn gói.
2. Thời gian thực hiện gói thầu: 06 tháng.

3. Phương thức thanh toán: Thanh toán chuyển khoản trong vòng 90 ngày, kể từ ngày nhận đủ hồ sơ thanh toán gồm (Biên bản bàn giao, Biên bản nghiệm thu, Hóa đơn tài chính, Biên bản đối chiếu công nợ, Biên bản thanh lý hợp đồng).

Trân trọng cảm ơn!



Lê Lâm

PHỤ LỤC: TÍNH NĂNG KỸ THUẬT ỨNG DỤNG DI ĐỘNG “HIỀN MÁU”

PHẦN I: TIÊU CHÍ KỸ THUẬT PHI CHỨC NĂNG, KIẾN TRÚC & KẾT NỐI HỆ THỐNG

STT	Hạng mục tiêu chuẩn	Yêu cầu kỹ thuật chi tiết trong E-HSMT (Định lượng & Minh bạch)	Tiêu chí đánh giá
1	Hiệu suất hệ thống	- Thời gian đáp ứng (Response time) trung bình của các API nghiệp vụ cốt lõi (Đăng nhập, đặt lịch, tra cứu kết quả, quản lý thông báo) đạt P95 < 200ms dưới điều kiện tải kiểm thử thực tế 500 CCU. Chỉ số này loại trừ endpoint thuộc phân hệ Chatbot AI. Phân hệ Chatbot AI áp dụng tiêu chuẩn hiệu năng riêng biệt: Thời gian sinh từ ngữ đầu tiên (Time-to-First-Token) đạt ≤ 500ms đối với các câu hỏi đã được tối ưu và lưu trong Bộ nhớ đệm nhúng ngữ nghĩa (Semantic Vector Caching), đối với các câu hỏi phức tạp yêu cầu mô hình LLM sinh từ ngữ mới hoàn toàn (Raw Generation), thời gian phản hồi đầu tiên đạt mức ≤ 1.5 giây, áp dụng cơ chế Stream API đồ chữ cuốn chiếu để người dùng không phải chờ đợi, tổng thời gian hoàn thành câu trả lời trung bình đạt P95 < 2.00 giây. - Ứng dụng di động phải tải và hiển thị xong bộ khung dữ liệu Trang chủ trong vòng ≤ 1.5 giây dưới điều kiện giả lập mạng di động băng thông hạn chế (Throttling Profile: 3G Network - 1.5 Mbps Down / 750 Kbps Up, RTT 100ms). - Đảm bảo hệ thống vận hành ổn định, không suy giảm dịch vụ với quy mô kiểm thử tối thiểu 500 người dùng đồng thời (CCU) (Có báo cáo kiểm thử bằng JMeter/LoadRunner¹ đính kèm khi nghiệm thu).	Đạt/Không đạt

¹ JMeter và LoadRunner là hai công cụ kiểm thử hiệu năng (Performance Testing Tools) phổ biến nhất hiện nay trong ngành công nghệ phần mềm.

2	An toàn & Bảo mật thông tin	- 100% dữ liệu truyền tải qua môi trường Internet phải được mã hóa bằng giao thức TLS 1.3 in-transit². - Dữ liệu định danh cá nhân (PII) lưu trữ trong cơ sở dữ liệu phải được mã hóa bằng thuật toán AES-256 at-rest³. - Hệ thống kiểm soát truy cập đa tầng: Xác thực qua JWT + Refresh Token, phân quyền theo vai trò người dùng (RBAC) đến từng chức năng/nút bấm. - Ghi nhật ký hệ thống (Audit log/Audit trail): Tự động ghi nhận 100% thao tác (thời gian, tài khoản, hành động, dữ liệu bị tác động), thời gian lưu trữ log tối thiểu 12 tháng.	Đạt/Không đạt
3	Độ tin cậy & Khả năng sẵn sàng	- Cam kết tỷ lệ thời gian hoạt động liên tục của môi trường Production SLA Uptime $\geq 99,5\%$, hỗ trợ giám sát và cảnh báo tự động 24/7. - Chỉ số điểm phục hồi dữ liệu tối đa RPO ≤ 1 giờ và thời gian phục hồi hệ thống tối đa khi có sự cố RTO ≤ 4 giờ. - Cơ chế sao lưu (Backup) tự động: Chụp ảnh hệ thống hàng ngày (Daily snapshot), thời gian lưu giữ bản sao lưu tối thiểu 30 ngày, hỗ trợ cơ chế nhân bản dữ liệu liên vùng (Cross-region replication).	Đạt/Không đạt
4	Khả năng sử dụng & Tương thích	- 100% ngôn ngữ giao diện hiển thị là Tiếng Việt chuẩn. Giao diện CMS đạt chuẩn thiết kế đáp ứng (Responsive), hiển thị tốt trên các trình duyệt phổ biến (Chrome, Firefox, Edge).	Đạt/Không đạt

² Phiên bản TLS 1.3 là tiêu chuẩn mới nhất, an toàn nhất và nhanh nhất hiện nay trên thế giới.

³ AES-256 là tiêu chuẩn mã hóa đối xứng (Symmetric Encryption) mạnh mẽ nhất thế giới hiện nay.

		- Ứng dụng di động hoạt động tốt và tương thích với hệ điều hành Android từ phiên bản 10.0 trở lên (đáp ứng >97% thiết bị tại Việt Nam) và iOS từ phiên bản 12.0 trở lên, hỗ trợ dải màn hình từ 5 inch đến 6.9 inch. - Ứng dụng di động phải tương thích hoàn toàn với các công cụ đọc màn hình gốc hệ điều hành: Xác thực đạt chuẩn Google TalkBack (Android) và Apple VoiceOver (iOS)⁴. - Áp dụng cơ chế Dynamic Type Scale tăng tối đa 150% đối với các luồng nghiệp vụ cốt lõi (gồm: Trang chủ, Đặt lịch hiển máu/tiểu cầu, Bản khai y tế, Kết quả xét nghiệm, và Giấy chứng nhận). - Giao diện Web CMS phải đạt tiêu chuẩn tiếp cận nội dung WCAG 2.1 mức độ AA (Thông tư 22/2019/BTTTT).	
5	Khả năng mở rộng & Kết nối	- Hệ thống được thiết kế theo kiến trúc mở, cung cấp tài liệu mã nguồn công khai đạt chuẩn RESTful API (OpenAPI 3.0/Swagger UI) phục vụ kết nối với bên thứ ba. - Cơ chế xác thực kết nối liên hệ thống bắt buộc sử dụng chuẩn OAuth 2.0, mTLS hoặc API Key. - Kiến trúc ứng dụng dạng Container hóa (Docker + Kubernetes), có khả năng tự động co giãn theo chiều ngang (Auto-scale) khi lượng người dùng tăng đột biến.	Đạt/Không đạt

⁴ Google TalkBack (trên Android) và Apple VoiceOver (trên iOS) là hai giao thức/trình đọc màn hình gốc (Native Screen Readers) dành cho người khiếm thị, người có thị lực kém.

6	Tiêu chuẩn công nghệ phát triển phần mềm	Nhà thầu phải cam kết xây dựng hệ thống dựa trên các nền tảng công nghệ cốt lõi dưới đây nhằm bảo đảm tính tương thích hạ tầng của Viện: - Tầng Mobile App: Sử dụng công nghệ Flutter 3.x trở lên (Ngôn ngữ Dart) hoặc công nghệ phát triển đa nền tảng tương đương, đáp ứng toàn bộ các tiêu chuẩn định lượng sau: + Cơ chế Biên dịch (Compilation Quality): Hỗ trợ biên dịch mã nguồn trực tiếp thành ngôn ngữ máy (Ahead-of-Time - AOT Compilation) cho cả hai nền tảng Android (Native ARM binary) và iOS (Native mã máy), không chấp nhận các giải pháp sử dụng cầu nối JavaScript (JavaScript Bridge) hoặc đóng gói giao diện Web-view thô sơ làm suy giảm hiệu năng thiết bị. + Kiến trúc Đồ họa (Rendering Engine): Hệ thống đồ họa của công nghệ phát triển phải sở hữu bộ máy dựng hình Vector thế hệ mới (Ứng dụng cơ chế Impeller Engine hoặc tương đương), tự động tối ưu hóa và nạp trước các chuỗi lệnh đồ bóng (Shader Pre-compilation). Tiêu chí này bắt buộc nhằm triệt tiêu hoàn toàn hiện tượng giật lag khung hình đầu tiên (Shader Compilation Jitter) khi hiển thị các hiệu ứng chuyển động đồ họa tinh tế, phức tạp cho đối tượng người dùng trẻ tuổi. + Chỉ số Hiệu năng thực tế (Performance Framework): Ứng dụng hoạt động mượt mà, tốc độ phản hồi giao diện đạt chuẩn 60 FPS dưới điều kiện kiểm thử (Đo lường định lượng bằng công cụ Performance Profiler tích hợp sẵn của Android/iOS, tỷ lệ Jank frame đạt mức < 1% trên các thiết bị cấu hình tầm trung	Đạt / Không đạt
---	---	--	-----------------

	và cao cấp các dòng máy phát hành từ năm 2023 trở lại đây, sở hữu từ 6GB RAM trở lên). + Bảo mật Mã nguồn (Code Obfuscation): Công nghệ lựa chọn bắt buộc tích hợp sẵn công cụ làm xáo trộn mã nguồn chuyên sâu cấp độ cấu trúc (Mã hóa tên lớp, tên biến, cấu trúc hàm qua cơ chế Obfuscation/Bitcode stripping), có khả năng chống lại hoàn toàn các kỹ thuật dịch ngược phần mềm (Reverse Engineering) và bẻ khóa lấy cấp thuật toán kiểm tra y tế của Viện. - Tầng Backend API: Sử dụng nền tảng .NET 8 trở lên (C#), Node.js LTS, Python 3.x hoặc tương đương. Xây dựng hoàn toàn theo mô hình RESTful API, đáp ứng kiến trúc Clean Architecture hoặc Microservices. - Tầng Cơ sở dữ liệu: Sử dụng hệ quản trị CSDL quan hệ chuẩn doanh nghiệp. Hỗ trợ mô hình High Availability (HA) dạng Cluster (Master-Replica), đồng bộ dữ liệu tự động và mã hóa gốc AES-256. - Tầng Web Frontend (CMS): Sử dụng framework Angular 17 trở lên (TypeScript) hoặc tương đương (framework SPA hỗ trợ kiến trúc component-based, two-way/reactive data binding) phối hợp HTML5/CSS3. Ứng dụng mô hình SPA (Single Page Application), tách biệt hoàn toàn với Backend qua lớp API Gateway. - Tầng Trục trung gian & Lưu trữ ngầm: Nhà thầu phải cam kết xây dựng hệ thống trục trung gian quản lý dữ liệu đệm và hàng đợi tin nhắn dựa trên các tiêu chuẩn công nghệ mở, đáp ứng toàn bộ các thông số định lượng và quy trình kiểm thử sau:	
--	---	--

		1. Phân hệ Bộ nhớ đệm phân tán (In-Memory Key-Value Cache): + Công nghệ yêu cầu: Sử dụng giải pháp Redis 7.x trở lên hoặc công nghệ lưu trữ dữ liệu trên bộ nhớ RAM tương đương. + Chỉ số hiệu năng (Throughput): Tốc độ xử lý request đạt hiệu năng tối thiểu ≥ 50.000 ops/sec (operations per second - số phép tính/giây) đối với các tác vụ đọc/ghi cơ bản (lệnh GET/SET) dưới điều kiện tải hệ thống. + Tiêu chuẩn cấu trúc dữ liệu: Hỗ trợ xử lý các cấu trúc dữ liệu nâng cao (gồm String, Hashes, Lists, Sets và Sorted Sets) nhằm phục vụ thuật toán tính toán Bảng xếp hạng thời gian thực và cơ chế Khóa phân tán (Distributed Lock) chống nghẽn mạch (Race Condition) trong luồng chiếm slot máy đặt lịch hiển tiêu cầu. + Phương pháp kiểm thử nghiệm thu (UAT): Đo lường bằng công cụ kiểm thử hiệu năng chuẩn hóa đi kèm hệ thống (như bộ công cụ redis-benchmark hoặc tương đương). Tiến hành chạy giả lập tối thiểu 100.000 yêu cầu với 50 kết nối đồng thời (lệnh mã kiểm thử: redis-benchmark -c 50 -n 100000 -t get,set). Hệ thống được đánh giá là ĐẠT khi chỉ số thời gian trễ P99 (Latency) đạt mức $< 5\text{ms}$ và tốc độ hiển thị phản hồi xử lý vượt ngưỡng 50.000 ops/sec. 2. Phân hệ Hàng đợi tin nhắn bất đồng bộ (Message Queue): + Công nghệ yêu cầu: Sử dụng giải pháp RabbitMQ hoặc công nghệ tương đương đáp ứng các giao thức chuẩn mở quốc tế AMQP (Advanced Message Queuing Protocol) hoặc MQTT. Phục vụ phân phối và xử lý bất đồng bộ các tác vụ nặng (gửi thông báo Rich Push hàng loạt, gửi Email, kích hoạt tiến trình ngầm sinh file chứng nhận PDF ký số).	
--	--	--	--

		+ Chỉ số hiệu năng: Tốc độ truyền tải và tiêu thụ tin nhắn (Publish/Consume throughput) của hệ thống hàng đợi đạt công suất tối thiểu ≥ 2.000 messages/sec mà không phát sinh hiện tượng tràn bộ nhớ (Memory leak) hoặc treo tiến trình Worker ngầm. + An toàn dữ liệu (Durability): Hệ thống phải cấu hình cơ chế lưu trữ tin nhắn bền vững xuống đĩa cứng (Persistent messages) kết hợp cơ chế xác nhận phân phối tin nhắn thành công (Message Acknowledgment - ACK). Đảm bảo tuyệt đối không làm mất mát, sai lệch hoặc trùng lặp bất kỳ yêu cầu đặt lịch hay gói tin thông báo nào của người hiển máu ngay cả khi cụm máy chủ trực trung gian xảy ra sự cố đột ngột hoặc thực hiện khởi động lại hệ thống (Restart dịch vụ).	
7	Mã nguồn & Bảo hành chuyển giao	- Nhà thầu phải bàn giao đầy đủ 100% Mã nguồn (Source Code) đạt tiêu chuẩn chất lượng mã nguồn (Quality Gate). Nhà thầu phải cấu hình và chạy kiểm tra mã nguồn tự động thông qua công cụ phân tích tĩnh SonarQube (hoặc tương đương) trước khi bàn giao. - Nhà thầu phải bàn giao tài khoản quản trị cao nhất (Root/Super Admin) của toàn bộ các dịch vụ hạ tầng, máy chủ đám mây và các kho mã nguồn (Repository); đồng thời ký biên bản chuyển giao 100% quyền sở hữu trí tuệ đối với mã nguồn viết riêng cho Viện. - Chỉ số định lượng bắt buộc để nghiệm thu: + Tỷ lệ bao phủ kiểm thử đơn vị (Unit Test Coverage) $\geq 80\%$ cho toàn bộ mã nguồn tầng nghiệp vụ lõi (Core Business Logic).	Đạt/Không đạt

		+ Không còn lỗi bảo mật nghiêm trọng (Zero Blockers & Critical Vulnerabilities). + Tỷ lệ mã trùng lặp (Code Duplication) < 3%. - Nhà thầu phải bàn giao đầy đủ tài liệu đặc tả yêu cầu (SRS), tài liệu thiết kế cơ sở dữ liệu (ERD), tài liệu kiến trúc hệ thống và tài liệu/video hướng dẫn sử dụng. - Thời gian bảo hành hệ thống tối thiểu 01 năm đối với toàn bộ các lỗi phát sinh do quá trình triển khai sai lệch so với thiết kế. Cam kết khắc phục lỗi nghiêm trọng (P0 Critical) với thời gian phản hồi ≤ 4 giờ và hoàn thành sửa lỗi ≤ 24 giờ. - Toàn bộ các thư viện, framework, nền tảng mã nguồn mở hoặc công nghệ trung gian do nhà thầu sử dụng để xây dựng hệ thống (gồm phân hệ lưu trữ log, giám sát metric, kiểm tra mã nguồn, container hóa) bắt buộc phải thuộc nhóm giấy phép mở thương mại tự do (như MIT, Apache 2.0, BSD hoặc tương đương). Nghiêm cấm sử dụng các mã nguồn có giấy phép ràng buộc gây rủi ro an ninh mạng hoặc ép buộc công khai mã nguồn đóng của Viện. Nhà thầu phải bàn giao danh mục kiểm toán bản quyền (Software Bill of Materials - SBOM) kèm theo tài khoản gốc cao nhất (Super Admin/Root Keys) của toàn bộ các dịch vụ khi bàn giao hệ thống.	
--	--	---	--

PHẦN II: DANH MỤC THÔNG SỐ KỸ THUẬT HẠ TẦNG

STT	Tên Hạng mục Hạ tầng	Cấu hình kỹ thuật tiêu chuẩn (Hoặc tương đương)	Số lượng	Tiêu chí đánh giá
1	Quản lý Khóa & Bảo mật (Vault)	Hệ thống Quản lý khóa và Tham số bảo mật tập trung (HashiCorp Vault HA hoặc tương đương), đáp ứng tiêu chuẩn mã hóa dữ liệu	01	Đạt/Không đạt

		FIPS 140-2, hỗ trợ tự động xoay vòng khóa (Key rotation) mà không làm gián đoạn ứng dụng Production.		
2	Công cụ CI/CD & Giám sát	- Công cụ tự động hóa đường ống CI/CD (GitHub Actions, GitLab CI hoặc tương đương); Hệ thống Docker Registry nội bộ (dung lượng ≥ 100 GB tích hợp quét mã độc tự động); - Giải pháp Giám sát hiệu năng và Cảnh báo tự động tập trung (Prometheus + Grafana + Alert Manager hoặc tương đương), hỗ trợ thu thập metric chuỗi thời gian (Time-series data), cấu hình biểu đồ trực quan động và định tuyến cảnh báo đa kênh (Email, SMS, Telegram/Webhook API); - Giải pháp quản lý log tập trung (ELK, Loki hoặc tương đương).	01 bộ	Đạt/Không đạt
3	Cổng Kết nối Dịch vụ ngoài	Sẵn sàng tích hợp kỹ thuật với hệ thống định danh điện tử VNeID (đáp ứng Nghị định 13/2023/NĐ-CP), tài khoản nhà phát triển Google/Apple, Google Maps Platform API, Firebase Cloud Messaging (FCM), Apple Push Notification service (APNs) và cổng dịch vụ gửi SMS Brand-name / SMTP relay.	01 bộ	Đạt/Không đạt
4	Phân tách môi trường mạng	Triển khai biệt lập hoàn toàn 03 môi trường mạng: Môi trường Phát triển (Dev ~25% tài nguyên), Môi trường Thử nghiệm (Staging ~50% tài nguyên) và Môi trường Vận hành chính thức (Production chạy full cấu hình High Availability và Auto-scaling).	03 bộ	Đạt/Không đạt

PHẦN III: YÊU CẦU KỸ THUẬT PHÂN HỆ TÍCH HỢP VÀ KẾT NỐI API SẴN CÓ

STT	Thành phần kết nối / Nghệp vụ API	Yêu cầu kỹ thuật chi tiết trong E-HSMT	Tiêu chí đánh giá
1	Xác thực mã thông báo đa tầng (Secure Authentication Integration)	- Hệ thống của nhà thầu phải tích hợp và xử lý chính xác luồng xác thực từ cấu trúc API sẵn có: + Đối với đăng nhập bên thứ ba: Tiếp nhận, mã hóa và truyền tải Identity Token (JWT) từ cấu phần Google/Apple ID về API Gateway để đối soát tính hợp lệ. + Đối với phiên làm việc: Xử lý đồng thời cấu trúc Header Authorization gồm hai tầng khóa: Basic {{Token}} (Mã hóa định danh ứng dụng) và Member-Authorization (Mã thông báo phiên làm việc của người hiển máu). - Cam kết vô hiệu hóa chuỗi token cục bộ trên thiết bị ngay lập tức khi API phản hồi mã lỗi xác thực hệ thống (HTTP Status 401 Unauthorized).	Đạt / Không đạt
2	Đồng bộ luồng dữ liệu Tin tức và Tương tác (News & Comment Engine)	- Mã nguồn ứng dụng phải tối ưu hóa các phương thức gọi API (POST / GET) đối với phân hệ Tin tức và Bình luận theo đúng cấu trúc payload dữ liệu thô (Raw JSON Payload) quy định trong Postman Collection.	Đạt / Không đạt

		- Chỉ số kiểm soát bằng thông: Luồng tải danh sách tin tức bắt buộc phải áp dụng kỹ thuật phân trang dữ liệu (Pagination via API parameters). - Độ trễ hiển thị bài viết mới và nội dung bình luận từ lúc máy chủ ghi nhận đến khi hiển thị mượt mà trên App di động phải đạt chỉ số thời gian ≤ 03 giây trong điều kiện mạng thông thường.	
3	Tích hợp hệ thống lõi LIS/HIS nội bộ của Viện	- Nhà thầu bắt buộc phải cấu hình trực kết nối API bảo mật (sử dụng giao thức mã hóa đường truyền mTLS hoặc API Key) để tiếp nhận tự động kết quả dữ liệu từ hệ thống quản lý phòng xét nghiệm (LIS) và thông tin bệnh viện (HIS). - Dữ liệu trả về (gồm nhóm máu, thể tích, chỉ số sàng lọc y sinh) phải được bóc tách từ các định dạng file cấu trúc y tế chuẩn hóa HL7 hoặc XML/JSON và ánh xạ (Mapping) chính xác 100% vào hồ sơ lịch sử của người dùng trên App di động. - Thời gian đồng bộ tự động kể từ khi bác sĩ phòng Lab bấm phê duyệt trên hệ thống nội bộ đến khi App phát thông báo đẩy (Push) cho người dùng không được quá ≤ 05 phút.	Đạt / Không đạt
4	Cơ chế xử lý lỗi đường truyền và Chống treo nghẽn (Fault Tolerance)	- Nhà thầu bắt buộc phải thiết lập thuật toán xử lý lỗi kết nối ngầm tại Client (Retry & Timeout Policy) khi tương tác với API Gateway của Viện:	Đạt / Không đạt

		+ Thời gian ngắt kết nối tối đa (Connection Timeout) cấu hình cố định là 10 giây. + Khi xảy ra lỗi mạng (HTTP Status 5xx hoặc mất kết nối), hệ thống tự động gọi lại API tối đa 03 lần theo thuật toán lũy tiến thời gian (Exponential Backoff). - Trường hợp quá 03 lần thất bại, ứng dụng phải hiển thị giao diện thông báo lỗi thân thiện (Friendly Error Handling State) và tự động ghi log lỗi vào vùng nhớ cục bộ để phục vụ đối soát, tuyệt đối không được phép gây treo ứng dụng (Freeze UI) hoặc tự động sập App (Crash).	
--	--	--	--

PHẦN IV: MA TRẬN YÊU CẦU KỸ THUẬT CHI TIẾT CỦA CÁC TÍNH NĂNG PHẦN MỀM

STT	Tên nhóm tính năng	Mô tả chi tiết yêu cầu kỹ thuật chuẩn hóa trong E-HSMT	Tiêu chí đánh giá
NHÓM 1 – ỨNG DỤNG DI ĐỘNG (Dành cho nền tảng Android & iOS)			
1	Đăng nhập	a) Đăng nhập qua Bên thứ ba (Social Login): - Tích hợp giải pháp đăng nhập một chạm sử dụng giao thức bảo mật OAuth 2.0 đối với tài khoản Google ID và Apple ID. - Token trả về từ Google/Apple phải được gửi về Backend API để xác thực tính hợp lệ trước khi cấp quyền truy cập hệ thống. - Đối với thiết bị iOS, bắt buộc phải tuân thủ chính sách App Store Review Guidelines về việc hiển thị nút "Sign in with Apple". b) Đăng nhập qua Số điện thoại (SĐT):	Đạt/Không đạt

	- Cho phép người dùng nhập SĐT để đăng nhập. Hệ thống phải tự động kiểm tra định dạng SĐT Việt Nam (đầu số hợp lệ, độ dài 10 chữ số). - Tích hợp hệ thống SMS Brand-name qua cổng kết nối trung gian để gửi mã OTP (One-Time Password) xác thực. - Thời gian hiệu lực của mã OTP tối đa là 120 giây. Hệ thống cấu hình chặn (Block) tạm thời SĐT trong 15 phút nếu nhập sai OTP quá 05 lần liên tiếp nhằm chống tấn công Brute-force. c) Sẵn sàng thực hiện đăng nhập qua VNeID khi đủ điều kiện kết nối với trung tâm dữ liệu quốc gia về dân cư: - Nhà thầu có trách nhiệm thiết kế sẵn sàng về mặt kiến trúc phần mềm, xây dựng các hàm tiếp nhận thông tin và giao diện App-to-App theo đúng tài liệu đặc tả kỹ thuật tiêu chuẩn của cổng VNeID. - Hệ thống tự động chuyển hướng (Redirect) hoặc gọi ứng dụng VNeID gốc trên thiết bị thông qua App-to-App login. - Trả về trạng thái đăng nhập thành công và đồng bộ các trường thông tin cơ bản được cấp phép (Họ tên, ngày sinh, số CCCD, SĐT liên kết VNeID). d) Phương án dự phòng (Fallback) khi VNeID gặp sự cố (hoặc chưa thể kết nối với VNeID): - Nhà thầu phải xây dựng giải pháp dự phòng độc lập, kích hoạt tự động hoặc bán tự động khi cổng kết nối VNeID bị gián đoạn hoặc không còn hỗ trợ đăng nhập.	
--	--	--

		- Giải pháp thay thế: Cho phép người dùng đăng nhập bằng SĐT + OTP kết hợp với yêu cầu xác thực tài khoản ở cấp độ cao bằng cách: Sử dụng camera gốc của điện thoại để quét mã QR trên thẻ Căn cước công dân (CCCD) hoặc chụp ảnh mặt trước/mặt sau thẻ CCCD. - Hệ thống Backend tích hợp công nghệ Công nghệ OCR bóc tách dữ liệu CCCD đạt Độ chính xác $\geq 95\%$ áp dụng đối với tập mẫu thẻ CCCD đạt chuẩn đầu vào (Hình ảnh chụp rõ nét bằng camera gốc của thiết bị, không bị mờ chữ, không bị lóa sáng bóng đèn, không bị che góc, góc nghiêng không quá 10 độ) tại giai đoạn UAT. e) Luồng xử lý đồng bộ khi thay đổi SĐT: - Kịch bản người dùng thay đổi SĐT đăng ký trên hệ thống của Viện nhưng tài khoản VNeID vẫn dùng SĐT cũ (hoặc ngược lại): Hệ thống bắt buộc phải thiết lập một Luồng đối soát và đồng bộ dữ liệu (Data Reconciliation). - Khi có sự không trùng khớp, ứng dụng phải hiển thị thông báo yêu cầu xác thực bổ sung bằng mã QR/CCCD hoặc gửi OTP về SĐT đăng ký trên VNeID để xác nhận chính chủ trước khi cập nhật dữ liệu SĐT mới nhất vào hồ sơ người hiến máu của Viện. - Đảm bảo mã định danh duy nhất của công dân (Số CCCD) làm gốc để liên kết các SĐT thay đổi. f) Quản lý phiên và Bảo mật - Áp dụng cơ chế mã hóa phiên làm việc (Session Management) bằng JWT (JSON Web Token) + Refresh Token.	
--	--	--	--

		- Định lượng thời gian: Access Token tự động hết hạn và mất hiệu lực sau 15 phút; Refresh Token có thời hạn lưu trữ an toàn tối đa 07 ngày. - Cơ chế thu hồi phiên lập tức (Token Invalidation): + Hệ thống bắt buộc phải triển khai mô hình Hủy token lưu đệm (Token Blacklisting) trên cụm bộ nhớ đệm trực trung gian. + Ngay khi xảy ra sự kiện: Người dùng bấm Đăng xuất, Người dùng thực hiện Đổi mật khẩu thành công hoặc Tài khoản bị CMS khóa quyền quyền, thời gian xử lý tại máy chủ Backend (Server-side processing latency) để cập nhật trạng thái hủy token vào cụm bộ nhớ đệm Redis phải đạt < 100ms. - Toàn bộ gói tin truyền lên máy chủ trong quá trình đăng nhập bắt buộc phải đi qua lớp bảo mật mạng truyền tải TLS 1.3.	
2	Điều khoản sử dụng	Hiển thị nội dung pháp lý: - Cho phép người dùng xem toàn bộ điều khoản sử dụng, chính sách bảo mật dữ liệu cá nhân của Viện trực tiếp trên ứng dụng trước và sau khi đăng nhập. - Nội dung văn bản được cấu hình động từ hệ thống quản trị (CMS Admin), hỗ trợ định dạng Rich Text (đậm, nghiêng, gạch chân, chèn link liên kết) giúp cập nhật văn bản pháp luật tức thời mà không cần phát hành lại ứng dụng nâng cấp.	Đạt/Không đạt
3	Trang chủ (Dashboard)	a) Banner Slide & Cá nhân hóa tác động tâm lý - Khu vực đầu trang chủ bố trí biểu ngữ dạng trượt (Banner Slide) tự động chuyển động hoặc cho phép vuốt tay (Swipe).	Đạt/Không đạt

	- Tích hợp bộ đếm cá nhân hóa 100% theo thời gian thực (Real-time data rendering): Hiển thị thông điệp truyền cảm hứng dựa trên công thức quy đổi nghiệp vụ (Ví dụ: "<i>1 lần hiến máu cứu 3 người</i>"). Hệ thống tự động truy xuất dữ liệu hồ sơ để hiển thị chính xác: "<i>Bạn đã hiến [aa] lần, đã cứu [aaa] người</i>". b) Thanh trạng thái sức khỏe (Dynamic Status Bar) - Bổ sung thanh trạng thái trực quan ngay phía dưới phần thông tin cá nhân để người dùng biết ngay điều kiện tham gia hiến máu hiện tại. - Logic hiển thị theo màu sắc: Nếu người dùng Đủ điều kiện hiến máu (đã qua thời gian tối thiểu giữa các lần hiến theo quy định y tế), thanh trạng thái bắt buộc phải hiển thị Màu Xanh lá cây. - Nếu chưa đủ điều kiện, hệ thống tự động tính toán số ngày còn lại và hiển thị trạng thái màu xám/đỏ kèm dòng chữ đếm ngược: "Bạn có thể hiến máu tiếp theo sau [X] ngày nữa". c) Tình trạng Kho máu (Blood Inventory Widget) - Hiển thị biểu đồ hoặc sơ đồ trạng thái động về lượng máu dự trữ hiện tại của Viện Huyết học – Truyền máu Trung ương giúp điều hướng người hiến. - Nguyên tắc bảo mật số liệu: Hệ thống chỉ hiển thị trạng thái định tính (Thiếu / Đầy đủ) cho từng nhóm máu (A, B, O, AB) để người dùng biết Viện đang cần nhóm máu nào, tuyệt đối không hiển thị số liệu số lượng thô (đơn vị thể tích/bản ghi dữ liệu gốc) ra ứng dụng cộng đồng.	
--	--	--

	- Dữ liệu trạng thái này bắt buộc phải kết nối tự động thông qua trục kết nối API bảo mật do hệ thống thông tin của Viện cung cấp, độ trễ cập nhật < 30 giây. d) Mã QR Cá nhân hóa truy cập nhanh (Quick QR Check-in) - Tích hợp và hiển thị một mã QR Code định danh duy nhất của người dùng ngay tại màn hình Trang chủ (bố trí góc trên hoặc nút nổi tiện ích). - Mục đích: Khi người hiến máu đến trực tiếp các điểm hiến hoặc xe hiến lưu động của Viện, chỉ cần mở màn hình Trang chủ là có thể đưa mã QR này vào thiết bị quét tại bàn tiếp đón để tự động đối chiếu, xác thực thông tin và check-in vào hệ thống tức thì mà không cần qua nhiều bước tìm kiếm sâu. e) Khối Vinh danh & Trò chơi hóa (Gamification Block) - Hiển thị thông tin nhóm máu, số lần hiến máu của người dùng tại khu vực dễ nhìn thấy nhất. - Thiết kế không gian hiển thị thông minh, gọn gàng (Sử dụng dạng lưới cuộn ngang hoặc danh sách thu gọn) cho mục Huân chương thành tích và Bảng xếp hạng (Ranking) bạn bè/hệ thống. - Đảm bảo không làm loãng không gian hiển thị chính của trang chủ nhưng vẫn đủ kích thích, thúc đẩy tinh thần tương tác của người dùng. f) Khối nội dung Giáo dục (Donor Education Section) - Thiết lập riêng một phân vùng nội dung trên Trang chủ dành cho đối tượng người mới tham gia hiến máu lần đầu hoặc người dùng đã lâu chưa đi hiến máu lại.	
--	---	--

		- Nội dung hiển thị tập trung giải đáp ngắn gọn các câu hỏi cốt lõi: "Điều kiện để được hiến máu là gì?", "Quy trình hiến máu gồm những bước nào?", "Cần chuẩn bị gì trước và sau khi hiến máu?" để giảm tải tâm lý e ngại cho người hiến.	
4	Đặt lịch	a) Phân loại và Điều hướng hình thức hiến máu - Hệ thống phân tách rõ ràng 2 loại hình thức hiến ngay từ bước khởi tạo: Hiến máu toàn phần và Hiến tiểu cầu. - Logic cấu hình địa điểm: Hình thức "Hiến máu toàn phần" được áp dụng cho tất cả các điểm hiến lưu động và cố định. Riêng hình thức "Hiến tiểu cầu" chỉ được hiển thị và cho phép lựa chọn khi người dùng chọn địa điểm là Viện Huyết học – Truyền máu Trung ương. b) Màn hình Trạng thái Đặt lịch (Khởi tạo) - Hệ thống tự động truy xuất dữ liệu lịch hẹn từ API Backend. Nếu người dùng không có lịch hẹn nào sắp diễn ra, hiển thị giao diện trạng thái trống (Empty State) phối hợp đồ họa tối giản và thông điệp truyền thông thân thiện . - Nút hành động "ĐẶT LỊCH" kích thước lớn (chiếm toàn bộ chiều ngang vùng an toàn hiển thị), thiết kế nổi bật (Sticky Bottom) cố định tại chân màn hình. Cung cấp 3 nút tùy chọn độc lập: "Đặt lịch hiến Máu", "Đặt lịch hiến Tiểu cầu" và nút "Hủy"	Đạt/Không đạt
5	Đặt lịch hiến tiểu cầu	a) Bộ chọn Ngày	Đạt/Không đạt

	- Giao diện lịch tích hợp (Calendar View): Hiển thị dạng lưới đầy đủ các ngày trong tháng (Ví dụ: May 2026), cho phép người dùng chuyển đổi linh hoạt giữa tháng trước và tháng sau. - Kiểm tra điều kiện thời gian: Hệ thống tự động vô hiệu hóa (Disable, hiển thị mờ và khóa tương tác) đối với toàn bộ các ngày trong quá khứ và ngày hiện tại nếu đã quá khung giờ phục vụ. - Chọn địa điểm: Chỉ hiển thị các điểm hiến có hạ tầng máy tách tiểu cầu khả dụng (mặc định là Viện Huyết học – Truyền máu Trung ương). - Nút "Tiếp tục" ở trạng thái mờ (Disabled), chỉ sáng lên (Enabled) sau khi người dùng lựa chọn đồng thời 01 ngày và 01 địa điểm hợp lệ. b) Bộ chọn Khung giờ - Giao diện hiển thị ma trận danh sách các khối giờ cố định trong ngày, phân tách rõ ràng thành các Block 02 giờ và 01 giờ cuối ngày: 7h00 - 9h00, 9h00 - 11h00, 11h00 - 13h00, 13h00 - 15h00, 15h00 - 16h00, 16h00 - 17h00. - Quản lý trạng thái khối giờ (State Management): + Khối giờ còn chỗ trống: Hiển thị màu nền xanh lá hoặc xanh dương. + Khối giờ được chọn: Hiển thị biểu tượng dấu tích (Checked) ở góc phải. + Khối giờ hết chỗ hoặc đã quá giờ: Tự động chuyển màu xám, khóa tương tác và ẩn nút chọn. - Nút "Tiếp tục" chỉ kích hoạt khi người dùng hoàn tất chọn 01 khung giờ khả dụng. c) Bản khai Sàng lọc Sức khỏe điện tử (Các trang câu hỏi)	
--	---	--

	Hệ thống hiển thị bằng câu hỏi trắc nghiệm tiền sàng lọc y tế bắt buộc (Gồm tối thiểu 19 câu hỏi nghiệp vụ chuyên sâu chia theo các danh mục mốc thời gian: Lịch sử hiện, Tiền sử bệnh lý nền, Sút cân trong 6 tháng, Châm cứu/xăm mình, Hành vi nguy cơ trong 2 tuần, Sử dụng thuốc kháng sinh trong 1 tuần, Tình trạng khuyết tật). - Mỗi câu hỏi bắt buộc cấu hình 02 nút lựa chọn độc quyền (Radio Button) tương ứng với nhãn "Có" và "Không". - Ứng dụng bắt buộc thực hiện cơ chế cuộn mượt mà (Smooth scrolling) với tốc độ phản hồi giao diện đạt 60 FPS ổn định trên các thiết bị tầm trung. - Người dùng bắt buộc phải trả lời 100% các câu hỏi. Hệ thống tự động kiểm tra, nếu phát hiện câu hỏi bị bỏ sót, sẽ tự động cuộn màn hình đến vị trí câu hỏi đó và hiển thị cảnh báo viền đỏ. d) Màn hình Cam kết & Hoàn tất Đăng ký - Cuối danh sách bảng khai, hệ thống bố trí ô tích chọn xác nhận trách nhiệm pháp lý bắt buộc (Checkbox): "Tôi đồng ý chịu hoàn toàn trách nhiệm với những câu trả lời trên". - Nút hành động cuối cùng "Đăng ký" (Màu đỏ) mặc định bị khóa; chỉ được kích hoạt mở khóa sau khi người dùng đã tích chọn đồng ý vào ô Checkbox cam kết. - Sau khi bấm "Đăng ký", hệ thống hiển thị màn hình thông báo Đăng ký thành công kèm mã lịch hẹn, mã QR định danh và tự động kích hoạt đẩy thông báo (Push Notification) về thiết bị	
--	---	--

6	Đặt lịch hiến máu	a) Khởi tạo và Chọn Ngày - Giao diện lịch tích hợp (Calendar View) tương tự mục 5a. - Người dùng chọn ngày → Hiển thị danh sách các điểm hiến máu cố định và lưu động cùng ngày. b) Danh sách Địa điểm đặt lịch - Hiển thị danh sách các điểm hiến máu cố định và lưu động dưới dạng thẻ (Card UI). Mỗi thẻ bao gồm: Tên địa điểm, địa chỉ chi tiết, khung giờ phục vụ, ngày tổ chức. - Tích hợp khả năng sắp xếp danh sách theo khoảng cách địa lý (từ gần nhất đến xa nhất) dựa trên định vị Geolocation của thiết bị người dùng. c) Xác nhận lựa chọn & Đăng ký nhắc lịch - Khi người dùng chọn xong địa điểm, ứng dụng tự động quay trở lại màn hình Lịch và điền text thông tin địa điểm đã chọn vào trường dữ liệu. - Ngày được chọn sẽ chuyển sang trạng thái kích hoạt: Đổi màu nền sang Màu Đỏ đậm, chữ trắng để người dùng nhận diện trực quan. - Nút "ĐẶT LỊCH" ở chân màn hình tự động chuyển từ trạng thái mờ (Disabled) sang trạng thái kích hoạt (Enabled - màu đỏ hiển thị rõ) để sẵn sàng gửi lệnh. - Khi bấm "ĐẶT LỊCH", hệ thống bắt buộc hiển thị một hộp thoại thông báo (Dialog Popup) đè lên giao diện chính nhằm xác nhận lại thông tin ngày hiến. - Tính năng Opt-in thông minh: Popup tích hợp câu hỏi đồng ý nhận thông báo nhắc nhở khi gần đến ngày hiến máu.	Đạt/Không đạt
---	--------------------------	--	---------------

		- Cung cấp 2 nút bấm rõ ràng: "Hủy bỏ" (đóng popup, giữ nguyên trạng thái) và "Xác nhận" (gửi lệnh tạo lịch hẹn và đăng ký token nhận push notification). - Hiện thị màn hình đồ họa thông báo trạng thái thành công hoàn toàn sau khi API Backend trả về mã phản hồi 200 OK. Bao gồm đoạn text truyền cảm hứng dẫn dò giữ gìn sức khỏe. - Nút sticky button "Xác nhận" ở cuối trang khi bấm sẽ điều hướng người dùng quay trở lại màn hình quản lý danh sách lịch hẹn cá nhân. d) Quản lý danh sách Lịch hẹn - Màn hình hiển thị danh sách các lịch hiến máu đã đăng ký và sắp diễn ra dưới dạng danh sách cuộn dọc. - Cử chỉ thông minh (Swipe-to-Action): Hỗ trợ hành vi vuốt thẻ lịch hẹn sang bên trái (Swipe Left). Khi vuốt, hệ thống tự động lộ ra nút "Thùng rác" (Màu đỏ) ở cạnh phải thẻ. - Khi người dùng nhấn vào nút Thùng rác này, hệ thống sẽ kích hoạt luồng hủy lịch hẹn, giải phóng slot và đồng bộ trạng thái về máy chủ tức thì.	
7	Lịch sử hiến máu	a) Màn hình Danh sách lịch sử - Hiện thị danh sách cuộn dọc toàn bộ các lần hiến máu thành công, sắp xếp theo thứ tự thời gian giảm dần. - Mỗi bản ghi hiển thị cấu trúc tiêu chuẩn: Chỉ số thứ tự lần hiến (Ví dụ: Lần 25, Lần 24), Ngày hiến (DD/MM/YYYY), Thể tích máu (350 ml, 250 ml), Hình thức hiến (Toàn phần hoặc Tiểu cầu), và Tên địa điểm tiếp nhận. b) Màn hình Chi tiết	Đạt/Không đạt

		- Hiển thị thông số tổng quan của lần hiến được chọn: Số lần, Ngày hiến, Địa điểm chi tiết, Lượng máu, và Cân nặng của người hiến tại thời điểm đó. - Hành trình đơn vị máu (Blood Unit Lifecycle Timeline): Bắt buộc tích hợp dòng thời gian theo dõi trạng thái thực tế của đơn vị máu đã hiến qua 3 nút mốc (Node) nghiệp vụ: 1. Ngày hiến máu 2. Ngày máu được lưu trữ 3. Ngày đơn vị máu được sử dụng cho bệnh nhân tại [Tên Bệnh viện] c) Màn hình xem "Loại xét nghiệm" - Tích hợp nút chọn Xét nghiệm dạng hộp thoại (Modal Dropdown / Action Sheet) hiển thị 3 phân hệ: Xét nghiệm sàng lọc, Công thức máu, và Xét nghiệm sinh hóa. - Giao diện hiển thị danh sách dạng bảng gồm tên chỉ số và trạng thái kết quả: + Đối với Sàng lọc: Hiển thị trạng thái định tính (Ví dụ: "Không phản ứng") . + Đối với Công thức máu & Sinh hóa: Hiển thị chỉ số định lượng kèm con số cụ thể. - Mã màu cảnh báo tự động (Smart Color Coding): Hệ thống bắt buộc tự đổi chiều dài chỉ số an toàn sinh học. Các chỉ số bình thường hiển thị nhãn màu xám; các chỉ số vượt ngưỡng hoặc dưới ngưỡng an toàn (Ví dụ: Axit uric tăng) bắt buộc phải được bôi đỏ nổi bật để cảnh báo trực quan cho người dùng. d) Màn hình xem "Nhận định"	
--	--	---	--

		- Hiện thị nội dung văn bản nhận định chuyên môn, phân tích chuyên sâu và lời khuyên y tế từ đội ngũ Bác sĩ của Viện dựa trên kết quả xét nghiệm của lần hiến đó. - Giao diện hỗ trợ định dạng văn bản động (Rich Text), tự động nhận diện và chuyển đổi các chuỗi ký tự số điện thoại thành Liên kết tương tác (Click-to-Call Link). Người dùng có thể chạm trực tiếp vào số Tổng đài (Ví dụ: 0976990066) trên màn hình để thực hiện cuộc gọi tư vấn trực tiếp đến hotline của Viện mà không cần nhập lại số thủ công. e) Album ảnh & Gói quà tặng - Album ảnh kỷ niệm: Cho phép người dùng chụp hoặc tải lên từ thư viện tối đa ≤ 10 ảnh/lần hiến để lưu trữ khoảnh khắc cá nhân tại ngày hội hiến máu. - Bộ lọc An toàn Tập tin tải lên (Secure Media Upload Engine): + Hệ thống mã nguồn tại API Gateway bắt buộc tích hợp thư viện kiểm tra sâu cấu trúc tập tin (Deep File Inspection). Chỉ chấp nhận các tập tin có định dạng ảnh chuẩn hóa là .jpg, .jpeg, .png thông qua việc kiểm tra Mã ký tự đầu (Magic Bytes / File Signature), không kiểm tra phần mở rộng đuôi file thô sơ. + Tự động chạy tiến trình loại bỏ hoàn toàn dữ liệu vị trí ẩn vĩ độ/kinh độ (Strip EXIF Metadata) của bức ảnh trước khi đẩy vào kho Object Storage nhằm bảo vệ quyền riêng tư vị trí của người hiến máu theo Nghị định 13/2023/NĐ-CP.	
--	--	--	--

		- Thông tin gói quà: Hiện thị rõ tên gói quà tặng xét nghiệm tương đương mà người dùng đã đăng ký nhận khi tham gia hiến máu để đảm bảo tính công khai, minh bạch về quyền lợi. f) Cấp Giấy chứng nhận điện tử tích hợp - Cho phép người dùng xem trực tuyến và tải xuống Giấy chứng nhận hiến máu điện tử định dạng tệp tin PDF bảo mật trực tiếp từ màn hình thành tích. - File PDF chứng nhận xuất bản phải tích hợp Chữ ký số (Digital Signature) của Viện để đảm bảo tính pháp lý và chống làm giả dữ liệu. - Trên phôi giấy chứng nhận phải tự động sinh một Mã QR mã hóa tĩnh chứa chuỗi ký tự kiểm tra (Hash string); khi quét mã QR này, hệ thống điều hướng về trang xác thực công khai của Viện để xác minh tính hợp lệ của văn bản.	
8	Bảng xếp hạng & huy hiệu số	a) Hệ thống phân hạng Thành tích (Gamification Tiers) - Hệ thống tự động tính toán tổng số lần hiến máu thành công từ dữ liệu lõi để xếp hạng người dùng theo các cấp bậc vinh danh lũy tiến: Đồng → Bạc → Vàng → Titan → Kim cương,... (Hạn mức số lần đạt phân hạng được cấu hình động từ CMS Admin). - Tại mỗi thẻ tài khoản trên bảng xếp hạng, bắt buộc phải hiển thị đồ họa thiết kế dạng Huân/Huy chương số (Digital Badge Icon) tương ứng với cấp bậc hiện tại của người dùng để tăng tính trực quan. b) Bảng xếp hạng tổng thể (Global & Regional Leaderboard) - Hiện thị danh sách top người hiến máu xuất sắc nhất theo dạng cuộn mượt mà đạt hiệu năng tối thiểu 60 FPS.	Đạt/Không đạt

		- Cung cấp bộ lọc phân loại đa chiều: Bảng xếp hạng Toàn quốc; Bảng xếp hạng theo Tỉnh/Thành phố; và Bảng xếp hạng theo Tháng/Năm/Tổng thời gian. - Mỗi dòng kết quả bao gồm: Vị trí thứ hạng (Rank), Ảnh đại diện (Avatar), Tên hiển thị, Biểu tượng huy chương cấp bậc và Tổng số lần hiển máu công khai. c) Cấp và Quản lý Huy hiệu số (Digital Badge System) - Thiết lập kho huy hiệu số với tối thiểu 10+ loại huy hiệu tương ứng với các cột mốc thành tích và hoạt động (Ví dụ: Huy hiệu "Hiển máu lần đầu", Huy hiệu "Mốc 10 lần", Huy hiệu "Người lan tỏa cộng đồng" khi mời thành công 5 bạn bè...). - Các huy hiệu chưa đạt được sẽ hiển thị màu xám mờ. Khi đạt điều kiện, hệ thống tự động kích hoạt (Unlock) chuyển sang phiên bản màu sắc rực rỡ và đẩy thông báo vinh danh real-time về App. - Tích hợp Share API của hệ điều hành cho phép người dùng chia sẻ trực tiếp hình ảnh huy chương đạt được lên mạng xã hội (Facebook, Zalo, Instagram) kèm link liên kết tải App. d) Cơ chế ẩn danh bảo mật dữ liệu cá nhân - Để tuân thủ Nghị định 13/2023/NĐ-CP, hệ thống bắt buộc tích hợp nút cấu hình quyền riêng tư cho người dùng. - Nếu người dùng bật chế độ ẩn danh, khi họ lọt vào Top của Bảng xếp hạng công khai, hệ thống sẽ tự động che tên thật và đổi thành "Người hiển máu ẩn	
--	--	--	--

		danh", đồng thời thay thế ảnh đại diện bằng avatar mặc định của hệ thống để bảo vệ danh tính.	
9	Bạn bè & Social Ranking	a) Màn hình Danh sách bạn bè & Bảng xếp hạng nội bộ - Hiện thị danh sách toàn bộ tài khoản người dùng đã kết bạn thành công theo dạng danh sách cuộn mượt mà (60 FPS). - Với mỗi người bạn trong danh sách, hệ thống phải trích xuất động các thông số: Tên hiển thị (Display Name), Ảnh đại diện (Avatar), Vị trí xếp hạng hệ thống (Rank), và Tổng số lần hiển máu thành công. - Cho phép sắp xếp danh sách bạn bè theo 2 bộ lọc: Theo thứ tự bảng chữ cái (A-Z) hoặc Theo số lần hiển máu giảm dần (Social Leaderboard) để kích thích tinh thần thi đua. b) Tính năng Tìm kiếm bạn bè (Search Engine) - Cung cấp thanh tìm kiếm thông minh thời gian thực. Hệ thống chỉ cho phép tìm kiếm tài khoản khác thông qua Mã định danh duy nhất (Username/Mã người hiển) hoặc Tên hiển thị (Display Name). - Nguyên tắc bảo mật thông tin (PII) : Nghiêm cấm việc cho phép tìm kiếm hoặc hiển thị công khai thông tin bạn bè bằng Số điện thoại hoặc Số CCCD trên thanh tìm kiếm chung để ngăn chặn hành vi khai thác, thu thập thông tin cá nhân bất hợp pháp. c) Quản lý Lời mời kết bạn & Gợi ý kết bạn	Đạt/Không đạt

		- Lời mời kết bạn: Hiển thị danh sách các yêu cầu kết bạn đang chờ xử lý. Cung cấp 2 nút tương tác nhanh: "Đồng ý" (Chuyển trạng thái sang Bạn bè) và "Từ chối" (Xóa yêu cầu khỏi danh sách). - Gợi ý kết bạn (Recommendation Engine): Hệ thống tự động gợi ý danh sách người dùng khác dựa trên thuật toán logic ngầm: Những người dùng có cùng điểm hiển máu thường xuyên hoặc những người dùng được mời tham gia chung thông qua mã liên kết (Social Invite Deep Link) từ luồng đặt lịch. d) Cấu hình Quyền riêng tư (Privacy Toggle) - Bắt buộc phải tích hợp cấu hình quyền riêng tư cho từng tài khoản tại màn hình "Cài đặt cá nhân": "Cho phép người khác tìm kiếm và xem thành tích hiển máu của tôi" (Bật/Tắt). - Nếu người dùng tắt cấu hình này, tài khoản của họ sẽ tự động ẩn hoàn toàn khỏi thanh tìm kiếm chung, danh sách gợi ý kết bạn và bảng xếp hạng chung của toàn hệ thống (Tuân thủ nghiêm ngặt quyền được kiểm soát dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP).	
10	Chatbot AI tư vấn	a) Giao diện hội thoại & Trợ lý ảo (Conversational UI) - Thiết kế giao diện bong bóng chat (Chat bubble) quen thuộc, hỗ trợ cuộn mượt mà đạt hiệu năng ổn định 60 FPS. - Tích hợp các trạng thái hiển thị động: Đang gõ chữ (Typing indicator), thời gian gửi tin nhắn, và lịch sử cuộc trò chuyện gần nhất. - Tích hợp linh vật độc quyền: Tại giao diện cổng vào Chatbot và góc biểu tượng trợ lý ảo, bắt buộc phải hiển thị Biểu tượng Gà hiển máu sinh động.	Đạt/Không đạt

	b) Công nghệ Animation linh vật Gà hiến máu - Biểu tượng linh vật Gà hiến máu bắt buộc phải sử dụng công nghệ xử lý hoạt họa vector dạng Lottie (JSON) hoặc Rive animation, không sử dụng ảnh GIF động truyền thống để tránh giảm hiệu năng thiết bị. - Thông số kỹ thuật hoạt họa: + Tốc độ khung hình: Đạt chuẩn 60 FPS mượt mà, không giật lag. + Dung lượng tệp tin: Tối ưu dưới 500 KB/file cấu hình. + Cơ chế tương tác (Interactive states): Biểu tượng Gà hiến máu có các hành động thay đổi linh hoạt theo ngữ cảnh trò chuyện (Ví dụ: Chào mừng khi mở chat, suy nghĩ khi chờ kết quả AI, gật đầu đồng ý hoặc giờ tay cổ vũ). c) Tư vấn Điều kiện & Nghiệp vụ hiến máu 24/7 - Chatbot hoạt động tự động liên tục 24/7. - Xử lý ngôn ngữ tự nhiên thông minh phục vụ giải đáp tức thì các câu hỏi về: Điều kiện tham gia hiến máu/tiểu cầu, quy trình chuẩn bị sức khỏe trước và sau khi hiến, chế độ quyền lợi, bảo hiểm và bồi hoàn. - Dữ liệu phản hồi dạng text kết hợp định dạng Rich Text (Đậm, nghiêng, xuống dòng) giúp người dùng dễ đọc. d) Gợi ý Địa điểm & Tích hợp liên kết đặt lịch hẹn - Khi người dùng hỏi về địa điểm hiến máu, Chatbot tự động phân tích ngữ cảnh, kết hợp dữ liệu định vị vị trí (Geolocation) của thiết bị để gợi ý danh sách các điểm hiến máu gần nhất của Viện.	
--	---	--

		- Trong câu trả lời của Chatbot, hệ thống bắt buộc phải nhúng kèm Nút hành động (Call-to-Action Button) trực quan (Ví dụ: "Đặt lịch ngay"). Khi người dùng nhấn nút này, ứng dụng sẽ tự động chuyển hướng sâu (Deep-link) thẳng sang mô-đun Đặt lịch hiển máu/tiểu cầu tương ứng mà không cần thoát ra màn hình chính. e) Cơ chế chuyển mạch dự phòng (Fallback Engine) - Hệ thống bắt buộc triển khai cơ chế tự động hiển thị cấu phần nút bấm chuyển mạch dự phòng (Nút kết nối trực tiếp đến Tổng đài CSKH hoặc số hotline của Viện: 0976990066) ngay trong luồng hội thoại của bong bóng chat khi thỏa mãn một trong hai điều kiện định lượng sau: + Điều kiện logic hệ thống (Client-side Trigger): Người dùng nhấn vào nút phản hồi biểu tượng "Câu trả lời không hữu ích" (Thao tác đánh giá tiêu cực) tối đa 02 lần liên tiếp trong cùng một phiên hỏi đáp (Session). + Điều kiện cấu trúc dữ liệu (API-side Trigger): Trường dữ liệu điểm số tin cậy (nhãn "confidence_score" hoặc tương đương trong tệp tin phản hồi JSON của API Chatbot) trả về giá trị nhỏ hơn ngưỡng tham số thiết lập. Tham số ngưỡng này bắt buộc phải cấu hình động được từ màn hình CMS Admin Web (ngưỡng mặc định ban đầu thiết lập là 70% hoặc 0.7), cho phép cán bộ Viện tự điều chỉnh tùy biến theo tình hình vận hành thực tế mà không cần can thiệp mã nguồn ứng dụng. - Quy chuẩn hiển thị giao diện: Nút bấm hotline phải tự động xuất hiện ở vị trí dưới cùng của khung chat (Sticky Bottom Action Component) với kích thước	
--	--	--	--

		vùng chạm tối thiểu $\geq 48 \times 48$ dp, sử dụng màu sắc chủ đạo nhận diện của Viện (Mã Hex #ED1C24) để người dùng dễ dàng nhận biết và thực hiện cuộc gọi một chạm (Click-to-Call) trực tiếp từ ứng dụng. f) Chiến lược Quản lý Ngữ cảnh (Context Window & Cache Eviction) - Hệ thống xử lý AI bắt buộc phải tích hợp giải pháp Bộ nhớ đệm nhúng ngữ nghĩa (Semantic Vector Caching) tại tầng trực trung gian. Đối với các câu hỏi có độ tương đồng ngữ nghĩa $\geq 95\%$, hệ thống lấy câu trả lời trực tiếp từ cache mà không cần chạy lại mô hình sinh LLM, tiết kiệm tài nguyên tính toán. - Thiết lập giới hạn kích thước ngữ cảnh hội thoại tối đa không quá 5 lượt chat liên tiếp/phiên làm việc (Context Window Management) để tránh tràn bộ nhớ RAM của Server Specialized.	
11	Quản lý thông báo	a) Danh sách thông báo (Notification Inbox) - Hiển thị danh sách cuộn mượt mà (60 FPS) phân tách rõ ràng theo các tab định dạng khác nhau: Thông báo hệ thống, Thông báo cá nhân, Tin tức khuyến mãi/sự kiện. - Mỗi thẻ thông báo hiển thị cấu trúc gồm: Tiêu đề (Bold), đoạn trích nội dung ngắn, ảnh thu nhỏ (Thumbnail), nhãn thời gian nhận (Ví dụ: 5 phút trước) và chấm xanh biểu thị trạng thái "Chưa đọc". - Hỗ trợ tính năng phân trang (Pagination) hoặc tải chậm (Lazy Loading) để tối ưu hiệu năng thiết bị. b) Hiển thị nổi bật trên Màn hình chính (In-App Shopeee-style Widgets)	Đạt/Không đạt

		- Hộp thoại nổi tương tác (In-App Popup/Banner Canvas): Khi người dùng vừa mở ứng dụng, hệ thống tự động kiểm tra và hiển thị các thông báo khẩn cấp hoặc chiến dịch hiển máu đột xuất dưới dạng Popup/Banner lớn đè lên màn hình chính với hiệu ứng mờ nền (Overlay Blur). - Cơ chế điều khiển thông minh (Smart Suppress & Frequency Cap): Hệ thống bắt buộc phải tích hợp luật chặn spam. Đối với các popup quảng bá sự kiện, hệ thống phải tự động ẩn đi sau khi người dùng đã xem qua hoặc nhấn nút tắt đóng lại, giới hạn tần suất hiển thị không quá 01 lần/user/ngày để tránh gây phiền hà. - Hộp thông tin nổi (Floating Widget/Badge): Thiết kế biểu tượng chuông thông báo hiển thị nổi bật ở thanh tiêu đề màn hình chính, tích hợp bộ đếm số lượng tin chưa đọc (Red Badge Counter) cập nhật thời gian thực. c) Cá nhân hóa theo sự kiện hành vi (Behavioral & Event Triggers) - Hệ thống tự động thiết lập các kịch bản kích hoạt thông báo tự động (Automated Behavioral Triggers) dựa trên thời gian thực của máy chủ kết hợp thông tin hồ sơ của từng cá nhân: + Ngày sinh nhật: Tự động gửi thông điệp chúc mừng sinh nhật cá nhân hóa kèm huy hiệu vinh danh độc quyền. + Kỷ niệm hiển máu: Gửi thông báo tri ân nhân ngày kỷ niệm, mốc hiển máu lần đầu hoặc mốc đặc biệt.	
--	--	--	--

		+ Chu kỳ đủ điều kiện: Hệ thống tự động tính toán lịch đếm ngược, gửi thông báo nhắc nhở ngay khi người dùng vừa chạm mốc đủ điều kiện khoảng cách ngày an toàn cho lần hiển máu/tiểu cầu tiếp theo. d) Chi tiết thông báo Đa phương tiện sinh động (Rich Media Context) - Khi người dùng bấm click vào một thông báo (từ danh sách inbox hoặc từ thanh thông báo trạng thái của hệ điều hành), ứng dụng mở ra màn hình chi tiết thông báo với định dạng đa phương tiện (Rich Media Layout). - Hỗ trợ định dạng nhúng nâng cao: Màn hình chi tiết bắt buộc phải hỗ trợ nhúng hình ảnh độ phân giải cao, trình phát video nội bộ (Native Video Player) phát các clip truyền thông hiển máu sinh động với tốc độ tải mượt mà, và bố trí các Nút kêu gọi hành động (CTA Button) (Ví dụ: Nút "Đặt lịch ngay" kết nối Deep-link trực tiếp sang mô-đun đặt lịch hiển tiểu cầu/máu toàn phần). e) Quản lý trạng thái và Xóa thông báo - Cung cấp cơ chế tương tác thông minh cho phép người dùng quản lý hộp thư thông báo: + Xóa từng thông báo: Hỗ trợ cử chỉ vuốt thẻ tin nhắn sang trái để lộ nút Xóa (Thùng rác) hoặc bấm icon menu tùy chọn để xóa. + Xóa hàng loạt / Đánh dấu đã đọc: Bố trí nút "Đọc tất cả" hoặc "Xóa tất cả" ở góc màn hình để dọn sạch hộp thư thông báo cá nhân. - Trạng thái xóa phải được đồng bộ ngay lập tức về cơ sở dữ liệu hệ thống.	
12	Quản lý tài khoản và Xác thực tài khoản	a) Cập nhật thông tin cá nhân & Xác thực 2 mức	Đạt/Không đạt

		- Xác nhận thông tin qua Camera ảnh CCCD: Tích hợp với cấu phần Camera gốc (Native Camera App) trên thiết bị di động để chụp ảnh thẻ Căn cước công dân (CCCD) mặt trước/mặt sau. - Tài khoản xác thực Mức 1 (Level 1): Trạng thái tài khoản cơ bản sau khi người dùng hoàn tất xác thực số điện thoại qua cổng SMS OTP hoặc liên kết qua Google/Apple ID thành công. Quyền hạn mức 1: Cho phép xem Trang chủ, tin tức truyền thông, và sử dụng Chatbot AI tư vấn . - Tài khoản xác thực Mức 2 (Level 2 - Định danh y tế): Trạng thái tài khoản cao cấp nhất, được kích hoạt tự động ngay sau khi luồng xác thực qua cổng VNeID trả về kết quả khớp 100% hoặc luồng chụp ảnh CCCD qua OCR đối soát thành công với cơ sở dữ liệu người hiến máu hiện hữu của Viện. Quyền hạn mức 2: Mở khóa các tính năng cốt lõi bắt buộc gồm Đặt lịch hiến tiểu cầu/máu , Xem chi tiết kết quả xét nghiệm , và Tái giấy chứng nhận điện tử ký số. - Cập nhật thông tin cá nhân: Cho phép chỉnh sửa các trường dữ liệu động: Ảnh đại diện, địa chỉ liên hệ, email nhận báo cáo, và số điện thoại khẩn cấp. Riêng thông tin cốt lõi (Họ tên, ngày sinh, số CCCD, nhóm máu) sau khi đã xác thực Mức 2 sẽ bị khóa chỉnh sửa ở giao diện App người dùng, chỉ được cập nhật qua nghiệp vụ đối soát tại quầy của Viện. b) Xóa tài khoản (Right to Erasure) - Quy trình Xác nhận xóa tài khoản: Thiết kế luồng xác nhận đa bước bảo mật cao nhằm tránh thao tác nhầm lẫn. Khi người dùng nhấn nút "Xóa tài khoản",	
--	--	---	--

		hệ thống hiển thị Popup cảnh báo hệ quả pháp lý (mất toàn bộ lịch sử thành tích, huy hiệu, và chứng nhận điện tử). Người dùng phải thực hiện nhập mật khẩu/Mã OTP xác nhận chính chủ lần cuối. - Thời gian xử lý dữ liệu cứng (Retention Window): Tuân thủ nghiêm ngặt chính sách GDPR và Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân. Hệ thống Backend tự động kích hoạt tiến trình xóa sạch toàn bộ thông tin định danh (PII), phiên đăng nhập, lịch sử kết nối của tài khoản trên App trong vòng ≤ 30 ngày kể từ ngày nhận yêu cầu. c) Đăng xuất (Logout) - Hủy bỏ phiên làm việc lập tức (Instant Token Revocation): Khi người dùng bấm "Đăng xuất khỏi hệ thống", ứng dụng gửi lệnh API đồng thời lên máy chủ, thực hiện xóa bỏ và vô hiệu hóa hoàn toàn cặp chuỗi khóa xác thực JWT (Access Token & Refresh Token) ra khỏi hệ thống quản lý bộ nhớ đệm Redis Cache tập trung ngay lập tức (độ trễ $< 100\text{ms}$) để phòng chống triệt để các cuộc tấn công phát lại phiên (Replay Attack). - Xóa dữ liệu vùng nhớ đệm cục bộ (Secure Memory Wipe): Ứng dụng di động tự động giải phóng toàn bộ các biến dữ liệu tạm thời, thông tin PII, ảnh kỷ niệm đang lưu đệm trên bộ nhớ RAM của thiết bị. Điều hướng màn hình quay trở lại trạng thái màn hình Đăng nhập ban đầu.	
13	Cài đặt ứng dụng	a) Cài đặt thông báo (Push, Email Preferences) - Cung cấp giao diện cấu hình cho phép người dùng chủ động Bật/Tắt (Toggle Switch) nhận thông báo theo từng danh mục nội dung độc lập: Thông báo lịch	Đạt/Không đạt

		hiển máu, Thông báo kết quả xét nghiệm nhảy cảm, Tin tức sự kiện truyền thông. - Hỗ trợ cấu hình đa kênh phân phối: Cho phép lựa chọn nhận qua ứng dụng (Push Notification) hoặc qua hộp thư điện tử (Email). - Khi người dùng thay đổi cấu hình, ứng dụng di động phải gọi API đồng thời để cập nhật trạng thái tùy chọn vào cơ sở dữ liệu hệ thống ngay lập tức (độ trễ phản hồi P95 < 200ms). b) Xác thực Sinh trắc học (Biometric Auth - Tối ưu bổ sung) - Tích hợp phân hệ cài đặt cho phép người dùng Bật/Tắt tính năng đăng nhập nhanh bằng sinh trắc học cá nhân có sẵn trên phần cứng thiết bị: Vân tay (TouchID / Biometric) hoặc Nhận diện khuôn mặt (FaceID). - Tính năng này đóng vai trò là giải pháp xác thực bổ sung song hành cùng phương thức đăng nhập OTP/VNeID truyền thống để tăng tốc độ truy cập ứng dụng của người dùng.	
NHÓM 2 – HỆ THỐNG QUẢN TRỊ (CMS Admin Web)			
14	Dashboard & Thống Kê	- Màn hình tổng quan cập nhật dữ liệu tự động với độ trễ < 30 giây (không cần tải lại trang): Tổng số lượng người dùng, tổng số ca hiển máu, danh sách lịch hẹn sắp tới. - Tích hợp hệ thống biểu đồ phân tích đa chiều (Line, Bar, Pie, Heat Map) theo mốc thời gian Ngày/Tháng/Quý/Năm.	Đạt/Không đạt

		- Tính năng Drill-down chuyên sâu: Cho phép bấm trực tiếp vào số liệu tổng hợp trên biểu đồ để chuyển hướng xem danh sách chi tiết các bản ghi cấu thành con số đó. - Thiết lập tính năng tự động lập lịch (Scheduled report) gửi báo cáo định kỳ qua email admin dưới dạng file đính kèm.	
15	Quản Lý Lịch Hiện	- Cung cấp linh hoạt hai chế độ hiển thị danh sách đăng ký đặt lịch: Chế độ lịch biểu (Calendar view) và Chế độ danh sách (List view). - Hỗ trợ tính năng xử lý hàng loạt (Bulk approve/reject): Cho phép tích chọn phê duyệt hoặc từ chối nhiều lịch đặt cùng một lúc. - Tiến trình xử lý hàng loạt bắt buộc phải được thiết kế chạy ngầm dưới dạng Background Thread, không được gây nghẽn hoặc khóa (Freeze) giao diện trình duyệt Web của nhân viên vận hành. - Biểu mẫu y tế (Medical Form) nhập kết quả xét nghiệm bắt buộc phải tích hợp thư viện kiểm tra dữ liệu đầu vào (Client-side validation) tự động đối chiếu dải chỉ số an toàn sinh học của Viện. - Hệ thống phải có khả năng tích hợp, đồng bộ hai chiều kết quả xét nghiệm với Hệ thống thông tin xét nghiệm (LIS) của Viện thông qua chuẩn kết nối HL7/ASTM hoặc API tiêu chuẩn tương đương, bảo đảm kết quả xét nghiệm được cập nhật tự động, không nhập tay trùng lặp. - Sau khi lưu trạng thái phê duyệt/hủy, hệ thống tự động kích hoạt Push Notification thông báo kết quả ngay lập tức tới thiết bị của người dùng.	Đạt/Không đạt

16	Phân Quyền RBAC	- Hệ thống phân quyền dựa trên vai trò kiểm soát đa tầng (Role-Based Access Control): Phân quyền độc lập tới từng module chức năng (tối thiểu 20+ module riêng biệt) và chi tiết đến từng nút bấm thao tác (Thêm, Sửa, Xóa, Xem). - Ghi nhật ký vận hành quản trị viên (Audit trail) chi tiết 100%: Lưu vết chính xác nhãn thời gian (Timestamp), tài khoản thực hiện và nội dung chi tiết hành động. - Tích hợp tính năng thiết lập danh sách địa chỉ IP được phép truy cập (IP Whitelist) dành riêng cho các nhóm tài khoản Quản trị viên cấp cao.	Đạt/Không đạt
17	Báo Cáo & Xuất Dữ Liệu	- Cung cấp sẵn tối thiểu 10 mẫu (Template) báo cáo nghiệp vụ y tế phổ biến, cho phép thiết lập bộ lọc đa điều kiện và tùy chỉnh khoảng thời gian linh hoạt. - Định dạng tệp tin kết xuất đầu ra bắt buộc: File Excel phải giữ nguyên cấu trúc định dạng bảng dữ liệu động (Pivot table), file PDF phải đạt chuẩn trình bày văn bản chuyên nghiệp. - Hỗ trợ cơ chế tự động kết xuất và gửi báo cáo định kỳ hàng tháng qua email theo cấu hình thời gian lập sẵn (Scheduled auto-export).	Đạt/Không đạt
NHÓM 3 – BẢO MẬT & BẢO VỆ DỮ LIỆU CÁ NHÂN (PII)			
18	Bảo Vệ Dữ Liệu Cá Nhân	- Áp dụng thuật toán mã hóa đối xứng mạnh AES-256 mã hóa lưu trữ (at-rest) cho toàn bộ các trường dữ liệu định danh cá nhân (PII) như Họ tên, CCCD, Số điện thoại, Địa chỉ, Nhóm máu trong DB. - Sử dụng giao thức bảo mật lớp truyền tải TLS 1.3 cho toàn bộ luồng dữ liệu di chuyển (in-transit).	Đạt/Không đạt

		- Quy định nghiêm cấm sử dụng dữ liệu thật của bệnh nhân trên môi trường Test/Staging; bắt buộc phải có tập lệnh tự động tạo dữ liệu giả lập đã được che giấu thông tin (Anonymized test data script). - Lưu vết riêng biệt lịch sử truy cập dữ liệu PII (Ghi nhận rõ ai đã xem thông tin của người hiến máu nào, vào lúc nào). - Đáp ứng quyền được xóa dữ liệu (GDPR right-to-erasure): Hệ thống tự động triển khai quy trình xóa sạch dữ liệu tài khoản theo yêu cầu của người dùng trong vòng ≤ 30 ngày.	
19	Bảo Mật Ứng Dụng Web	- Nhà thầu phải cam kết: Trước khi đưa hệ thống vào vận hành chính thức (Go-Live), toàn bộ sản phẩm (Mobile App và Web CMS) phải được quét lỗ hổng và kiểm thử xâm nhập (Penetration Testing) bởi một Đơn vị chuyên trách An ninh mạng độc lập (Có chứng nhận đạt chuẩn an toàn không còn lỗi nghiêm trọng P0, P1 theo danh mục OWASP Top 10). - Hệ thống phải được thiết kế, xây dựng và vận hành đáp ứng yêu cầu bảo đảm an toàn hệ thống thông tin tối thiểu Cấp độ 3 theo Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT (do hệ thống xử lý dữ liệu cá nhân và thông tin sức khỏe của người hiến máu). - Nhật ký truy cập dữ liệu cá nhân (PII Access Log) của người hiến máu bắt buộc phải ghi nhận rõ cơ chế: Ai đã xem, xem thông tin của ai, vào mốc thời gian nào; dữ liệu log này không được phép sửa/xóa và lưu trữ tập trung tối thiểu 12 tháng.	Đạt/Không đạt

		- Phòng chống lỗi XSS bằng cơ chế mã hóa đầu ra (Output encoding) phối hợp cấu hình chặt chẽ tiêu đề Content Security Policy (CSP) trên Web Server. - Phòng chống lỗi CSRF bằng cơ chế tự động luân chuyển mã token bảo mật theo từng yêu cầu (Token rotation per-request). - Ngăn chặn lỗi SQL Injection tuyệt đối bằng cách bắt buộc sử dụng truy vấn tham số hóa (Parameterized Queries / ORM) và không viết mã lệnh bằng chuỗi SQL thô (Raw SQL). - Quản lý phiên làm việc Web Admin an toàn: Sử dụng chuỗi muối ngẫu nhiên (Random salt), thiết lập thuộc tính bảo mật HttpOnly, Secure và SameSite cho Cookie hệ thống. - Hệ thống bắt buộc phải được quét lỗi, kiểm thử xâm nhập tự động (Automated Penetration Testing) trước mỗi đợt phát hành lên môi trường Production.	
20	Bảo Mật Ứng Dụng Mobile	- Nghiêm cấm lưu trữ trực tiếp các thông tin nhạy cảm và dữ liệu PII dưới dạng file thô trên bộ nhớ cục bộ của điện thoại. Toàn bộ thông tin khóa xác thực bắt buộc phải được mã hóa lưu trữ trong Keychain (iOS) hoặc KeyStore (Android). - Triển khai công nghệ SSL Certificate Pinning trên ứng dụng di động để ngăn chặn triệt để các cuộc tấn công nghe lén, giả mạo chứng chỉ ở giữa (Man-In-The-Middle attack).	Đạt/Không đạt

		- Mã hóa và làm xáo trộn mã nguồn ứng dụng trước khi đóng gói phát hành bằng công cụ chuyên dụng (ProGuard/R8 cho Android và thực hiện Bitcode stripped cho iOS) nhằm chống đảo ngược mã nguồn (Reverse engineering). - Tích hợp tính năng tự động phát hiện thiết bị bẻ khóa (Jailbreak/Root detection) và thực hiện khóa ứng dụng, từ chối quyền truy cập ngay lập tức nếu phát hiện thiết bị không an toàn. - Bắt buộc thực thi chính sách bảo mật truyền tải dữ liệu App Transport Security (ATS) trên nền tảng iOS.	
NHÓM 4 – HẠ TẦNG, API & KHẢ NĂNG MỞ RỘNG			
21	Hệ thống API Backend	- Toàn bộ các tương tác nghiệp vụ giữa Mobile App, CMS và máy chủ bắt buộc thực hiện qua hệ thống trực RESTful API xây dựng theo tiêu chuẩn mở OpenAPI 3.0 (Tự động biên dịch tài liệu Swagger UI từ mã nguồn). - Triển khai cơ chế phân tách phiên bản API (API Versioning như v1, v2) đảm bảo các cập nhật tính năng mới không làm gián đoạn, hỏng hóc các phiên bản ứng dụng cũ đang cài đặt trên máy người dùng. - Thiết lập quy định quản lý vòng đời API nghiêm ngặt: Hệ thống trực Gateway bắt buộc hỗ trợ cấu hình nhãn tiêu đề phản hồi X-API-Deprecated và X-API-Sunset cho các phiên bản API cũ. - Khi Viện ban hành phiên bản mới, các API cũ chỉ được phép duy trì hoạt động tối đa không quá 06 tháng (hoặc qua 02 phiên bản cập nhật lớn). Ứng dụng di động của người dùng chạy bản cũ bắt buộc phải nhận được thông báo điều hướng tự động, yêu cầu cập nhật App lên phiên bản mới nhất từ Store thì	Đạt/Không đạt

		mới được phép tiếp tục gọi API, bảo vệ an toàn cho toàn bộ hạ tầng lõi của Viện. - Cấu hình giới hạn tần suất gọi API (Rate limiting) ở mức tối đa 1.000 requests/phút/user để chống tấn công từ chối dịch vụ phá hoại hệ thống.	
22	Hạ Tầng & Công cụ CI/CD	- Quy trình đóng gói và triển khai ứng dụng phải được tự động hóa 100% qua đường ống CI/CD pipeline sử dụng GitHub Actions, GitLab CI hoặc tương đương. Hệ thống đường ống CI/CD bắt buộc phải tích hợp cầu phần Quét mã độc và lỗ hổng bảo mật tự động cho Docker Image (Container Image Scanning) trước khi đẩy lên Private Registry. - Toàn bộ dịch vụ ứng dụng chạy trên kiến trúc microservices được quản lý bằng Helm Chart trên nền tảng K8s, hỗ trợ cập nhật hệ thống chỉ bằng 1 lệnh duy nhất. - Quy trình phát hành phiên bản mới (Release) bắt buộc đáp ứng mô hình Blue-Green Deployment (Không có thời gian chết hệ thống - Zero-downtime). Cơ chế tự động khôi phục về phiên bản an toàn cũ (Rollback) khi xảy ra lỗi nghiêm trọng phải hoàn thành trong thời gian ≤ 5 phút.	Đạt/Không đạt
23	Hiệu Năng & SLA cam kết	- Hệ thống xử lý mượt mà, phân phối tải cân bằng đạt chỉ số thời gian phản hồi API ở mức P95 < 200ms dưới điều kiện tải kiểm thử thực tế. Các chỉ số hiệu năng nêu tại mục này bắt buộc phải được đo kiểm, chứng minh bằng công cụ kiểm thử tải tiêu chuẩn (JMeter, k6, Gatling hoặc tương đương) và nhà thầu phải bàn giao báo cáo kết quả kiểm thử tải (Load/Stress Test Report) cho Viện trong giai đoạn nghiệm thu.	Đạt/Không đạt

		- Cam kết bằng điều khoản hợp đồng tỷ lệ sẵn sàng dịch vụ SLA Uptime toàn hệ thống đạt mức $\geq 99,5\%$. - Tích hợp dịch vụ CDN mạng lưới phân phối nội dung, đảm bảo thời gian tải các tài sản tĩnh (Hình ảnh banner, giao diện đồ họa) đạt tốc độ dưới 0,5 giây. - Quy trình tối ưu hóa truy vấn cơ sở dữ liệu (Database Query Optimization) và đánh giá kế hoạch thực thi câu lệnh (Execution Plan Review) phải được thực hiện bắt buộc trước mỗi đợt release.	
24	Hỗ Trợ & Bảo Hành phần mềm	- Cung cấp kênh tổng đài Hotline hỗ trợ kỹ thuật liên tục từ thứ Hai đến thứ Sáu hàng tuần. - Bàn giao bộ tài liệu quản lý, cẩm nang người dùng cuối và hệ thống video đào tạo trực tuyến (Đóng gói qua nền tảng Zoom / Loom hoặc tương đương). - Cam kết quy trình xử lý sự cố phần mềm nghiêm ngặt theo biên bản thỏa thuận mức dịch vụ (SLA Bug fix): Tiếp nhận phản hồi lỗi nguy cấp P0 trong vòng ≤ 4 giờ và hoàn thành sửa lỗi triệt để trong vòng ≤ 24 giờ. - Định kỳ hàng tháng, nhà thầu phải xuất và gửi báo cáo đánh giá sức khỏe hệ thống (Monthly health check report) một cách minh bạch cho Chủ đầu tư.	Đạt/Không đạt

PHẦN V: YÊU CẦU UI/UX

STT	Thành phần bàn giao / Tiêu chuẩn thiết kế	Yêu cầu kỹ thuật chi tiết trong E-HSMT (Định lượng, Minh bạch & Kiểm thử được)	Tiêu chí đánh giá
-----	---	--	-------------------

1	Tính đa dạng và độc lập của Phương án thiết kế (UI Concepts)	- Nhà thầu bắt buộc phải cung cấp tối thiểu 03 phương án thiết kế giao diện đồ họa (High-fidelity UI Concept) độc lập và khác biệt hoàn toàn về phong cách phối màu phụ, cách bố trí bố cục các Widget và trải nghiệm luồng tương tác tại màn hình Trang chủ (Dashboard). - Mỗi phương án thiết kế bắt buộc phải thể hiện trọn vẹn sự đồng bộ nhận diện thương hiệu với màu chủ đạo của Viện (Mã màu Hex #ED1C24) và thể hiện đầy đủ cấu trúc các khối tính năng: Thanh trạng thái sức khỏe (Dynamic Status Bar), Widget Kho máu định tính, Mã QR truy cập nhanh và Khối vinh danh/Huy hiệu số. - Các phương án phải được trình bày dưới dạng bản vẽ độ phân giải cao, mô phỏng chính xác trên 2 kích thước màn hình di động tiêu chuẩn (Tỷ lệ 19.5:9 cho iOS và 20:9 cho Android).	Đạt / Không đạt
2	Bản mẫu tương tác và Công cụ cộng tác (Interactive Prototype)	- Toàn bộ 03 phương án thiết kế giao diện phải được xây dựng trên công cụ thiết kế chuyên nghiệp dựa trên nền tảng đám mây phổ biến (Figma, Adobe XD, Sketch hoặc tương đương). - Nhà thầu bắt buộc phải cấu hình liên kết chuyển động trung gian giữa các màn hình để tạo thành các Bản mẫu tương tác (Interactive Prototype / Wireframe click-through), cho phép người dùng thử nghiệm có thể bấm, vuốt, chuyển trang, mở popup bán khai y tế giống như ứng dụng thực tế để làm cơ sở cho Viện đánh giá, lựa chọn trước khi lập trình.	Đạt / Không đạt

3	Bộ thư viện thiết kế chuẩn hóa (Design System / UI Kit)	- Nhà thầu phải cung cấp bộ tài liệu phân cấp kiểu chữ (Typography Scale), bảng biểu tượng đồ họa hệ thống (Iconography dạng Vector .svg) và Hệ thống thiết kế (Design System UI Kit) chuẩn hóa. - Định lượng trạng thái phần tử: 100% các thành phần giao diện tương tác (Nút Đặt lịch, ô tích chọn Checkbox bản khai y tế, các nút câu hỏi Có/Không) bắt buộc phải được thiết kế đầy đủ các trạng thái hiển thị: Mặc định (Default), Đang tương tác (Hover/Pressed), Đã chọn (Selected) và Khóa chức năng (Disabled). - Kích thước vùng chạm tương tác (Touch Target Size) trên di động bắt buộc phải đạt tối thiểu $\geq 48 \times 48$ dp để chống bấm nhầm cho người dùng.	Đạt / Không đạt
4	Quy trình kiểm thử Trải nghiệm người dùng định lượng (SUS Score)	- Để chứng minh giao diện được tối ưu khoa học cho giới trẻ, nhà thầu phải phối hợp cùng Viện tổ chức một đợt kiểm thử trải nghiệm người dùng độc lập (User Acceptance Testing - UAT cho bản vẽ UI) trên một nhóm mẫu thử nghiệm tối thiểu 30 người thuộc độ tuổi thanh niên (18 - 35 tuổi). - Phương án thiết kế được lựa chọn đưa vào giai đoạn lập trình bắt buộc phải đạt điểm số đánh giá trung bình ≥ 75 điểm trên Thang đo tính khả dụng hệ thống chuẩn quốc tế (System Usability Scale - SUS Score).	Đạt / Không đạt
5	SLA Hỗ trợ chỉnh sửa và Bàn giao quyền sở hữu	- SLA Chỉnh sửa: Nhà thầu cam kết hỗ trợ tối thiểu 03 vòng hiệu chỉnh toàn diện (Revision Rounds) cho phương án được chọn dựa trên biên bản góp ý chuyên môn của Viện. Thời gian hoàn thành cập nhật bản vẽ cho mỗi vòng không quá ≤ 03 ngày làm việc.	Đạt / Không đạt

		- Quy chuẩn bàn giao: Sau khi Viện chốt phương án cuối cùng, nhà thầu phải bàn giao 100% quyền sở hữu, link gốc sản phẩm thiết kế và file source code thiết kế định dạng vector sạch, phân lớp (Layered) rõ ràng, sẵn sàng cho tính năng xuất bản mã nguồn tự động dành cho lập trình viên (Developer Handoff).	
--	--	---	--

PHẦN VI: YÊU CẦU NĂNG LỰC NHÂN SỰ CHỦ CHỐT

STT	Vị trí nhân sự	Số lượng	Yêu cầu về trình độ, năng lực và kinh nghiệm nghiệp vụ	Hồ sơ, tài liệu bắt buộc phải nộp để chứng minh
1	Trưởng nhóm triển khai (Project Manager)	01 người	- Trình độ: Tốt nghiệp Đại học trở lên chuyên ngành CNTT, Tin học y tế hoặc các ngành tương đương. - Có ≥ 10 năm kinh nghiệm làm việc trong lĩnh vực CNTT. - Đã từng làm Giám đốc dự án hoặc Trưởng nhóm triển khai cho tối thiểu 01 dự án phần mềm y tế hoặc ứng dụng di động có giá trị tương đương gói thầu đang xét.	- Bằng tốt nghiệp Đại học/Thạc sĩ/Tiến sĩ. - Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Biên bản nghiệm thu hoặc xác nhận của Chủ đầu tư dự án tương tự trước đó.
2	Chuyên viên phân tích nghiệp vụ (BA)	01 người	- Trình độ: Đại học trở lên chuyên ngành CNTT hoặc Quản lý y tế. - Có ≥ 5 năm kinh nghiệm phân tích nghiệp vụ phần mềm (BA) trong lĩnh vực y tế.	- Bằng tốt nghiệp Đại học. - Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu.

			- Thành thạo kỹ năng khảo sát nghiệp vụ và viết tài liệu đặc tả yêu cầu hệ thống (SRS).	- Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Bản sao tối thiểu 01 tài liệu đặc tả SRS phần mềm do nhân sự này thực hiện (đã che thông tin nhạy cảm).
3	Lập trình viên Mobile Flutter	02 người	- Trình độ: Đại học hoặc Cao đẳng chuyên ngành CNTT. - Có ≥ 5 năm kinh nghiệm lập trình ứng dụng di động sử dụng Flutter/Dart. - Đã trực tiếp phát triển và đưa thành công ≥ 2 ứng dụng lên các chợ ứng dụng (Google Play và Apple App Store).	- Bằng tốt nghiệp/Chứng chỉ chuyên ngành. - Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Đường link (URL) kèm ảnh chụp minh chứng 02 ứng dụng đang hoạt động trên Store.
4	Lập trình viên Backend	02 người	- Trình độ: Đại học trở lên chuyên ngành CNTT. - Có ≥ 5 năm kinh nghiệm lập trình Backend sử dụng nền tảng Node.js hoặc .NET Core. - Có kinh nghiệm thiết kế RESTful API, xây dựng cấu trúc cơ sở dữ liệu và xử lý logic nghiệp vụ hệ thống.	- Bằng tốt nghiệp Đại học. - Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH).

				- Tài liệu minh chứng đã tham gia thiết kế/xây dựng hệ thống API cho tối thiểu 01 dự án tương tự.
5	Chuyên viên thiết kế UI/UX	01 người	- Có ≥ 5 năm kinh nghiệm thiết kế giao diện ứng dụng di động và hệ thống quản trị Web. - Thành thạo công cụ thiết kế chuyên nghiệp Figma.	- Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Portfolio/Hồ sơ năng lực thiết kế (Đường link Figma hoặc tệp PDF sản phẩm giao diện đã thiết kế).
6	Kỹ sư kiểm thử phần mềm (Tester/QA)	01 người	- Có ≥ 3 năm kinh nghiệm kiểm thử chất lượng phần mềm. - Sở hữu chứng chỉ quốc tế ISTQB Foundation Level hoặc có tối thiểu 05 năm kinh nghiệm kiểm thử chất lượng các hệ thống phần mềm y tế, ứng dụng di động cấp doanh nghiệp. - Thành thạo kiểm thử chức năng, hiệu năng, bảo mật và sử dụng công cụ kiểm thử tự động (như Appium).	- Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Bản sao công chứng chứng chỉ quốc tế ISTQB Foundation Level hoặc Advanced Level (nếu có); Hoặc các giấy tờ chứng minh kinh nghiệm kiểm thử tương đương (Hợp

				đồng, biên bản nghiệm thu dự án cũ) trong trường hợp nhân sự áp dụng tiêu chuẩn 5 năm kinh nghiệm. - Báo cáo kết quả kiểm thử (Test Report) của một dự án cũ làm minh chứng năng lực.
7	Kỹ sư hạ tầng & Vận hành (DevOps)	01 người	- Có ≥ 5 năm kinh nghiệm quản trị hệ thống Linux, Docker, đường ống CI/CD. - Có kinh nghiệm thực tế triển khai, giám sát hệ thống trên các nền tảng đám mây lớn (AWS/GCP/Azure) và quản trị Kubernetes Cluster.	- Sơ yếu lý lịch (CV) có xác nhận. - Hợp đồng lao động chính thức (Thời hạn ≥ 01 năm hoặc không xác định thời hạn) ký với nhà thầu dự thầu. - Bản sao trích xuất dữ liệu đóng Bảo hiểm xã hội (BHXH). - Các chứng chỉ hạ tầng đi kèm (nếu có - như AWS, CKA...) hoặc tài liệu minh chứng đã thiết lập hệ thống K8s cho dự án thực tế.