RESTful API Design Patterns for HIPAA-Compliant Healthcare Data Exchange

Arjun Warrier

Senior Technology Consultant
Warrier.arjun@gmail.com

Abstract:
As the use of electronic health record (EHR) systems, mobile applications, and connected clinical systems has become more pervasive, the need for frictionless, secure, and standards-based health care data exchange has only increased. Classic approaches to health care system integration—frequently involving the use of HL7 v2. x messages and point-to-point interfaces – are not designed for the agility, scalability, and security required of a modern digital health ecosystem. These challenges are especially pronounced when incorporating third-party solutions, such as allowing patient access to data or facilitating cross-organizational workflows. In this context, API-first architecture and RESTful API design principles serve as a disruptive form of healthcare interoperability that aligns with regulatory, technical, and operational requirements.
This paper presents a detailed study of RESTful API design patterns for HIPAA-compliant healthcare data exchange. It details the architectural aspects and implementation plans that support secure, scalable, and standard-compliant integration of independent healthcare systems or services. A significant emphasis is placed on utilizing HL7 FHIR R4 as a canonical data model to gain fine-grained access to healthcare data, as well as to enforce consistency and enhance reusability across systems. By embracing OAuth 2.0 (with healthcare profiles) and JWTs, access control, consent generation, and authentication patterns are secure and flexible, supporting the evolving needs of both healthcare providers and patients over time.
Distilling this with a focus on the technical architecture, this paper focuses on the HIPAA Privacy Rule and Security Rule, detailing how RESTful API endpoints are made auditable, logged, encrypted, and access-managed to meet legislative requirements. We follow a defense-in-depth approach by utilizing API gateways, token-based authentication, and rate limiting to prevent risks such as data breaches, unauthorized access, and DDoS attacks.
The research method involves a multi-stage deployment and validation of the proposed architecture in a hybrid context, incorporating EHR systems, cloud-native microservices, and third-party digital health platforms. The framework's efficiency was evaluated based on integration effort, response time, system throughput, and security posture. According to empirical evidence, the API-first integration model reduces integration timelines by an average of 40% compared to a traditional HL7 v2 interfacing approach. Additionally, the use of FHIR profiles and RESTful design patterns increased developer efficiency and reduced the need for custom mapping or transformation layers.
This paper makes two significant technical contributions: a library of reusable design patterns for secure resource modeling, error handling, paginated queries, API versioning, and consent-based access control. These patterns are intended to serve as a guide for system architects and healthcare developers in building healthcare interoperability projects, guiding the construction of scalable, maintainable, and secure APIs.
The paper argues that the implementation of RESTful APIs in an API-first development lifecycle is not just a technical decision, but a strategic rider for digital transformation in healthcare. RESTful API-based architectures provide a practical approach to HIPAA-compliant, real-time data exchange for healthcare organizations, which begins with building on open standards, incorporating security through design, and streamlining integration workflows. This study paves the way for next-generation advancements that include leveraging event-driven application programmable

interfaces (APIs), incorporating blockchains for secure, tamper-proof audit trails, and building federated data governance models in healthcare.

Keywords: RESTful APIs, HL7 FHIR R4, HIPAA Compliance, OAuth 2.0 Extensions, API-First Architecture, Healthcare Interoperability, Secure Data Exchange, EHR Integration, JSON Web Tokens (JWT), Healthcare API Gateway.

I. INTRODUCTION

Interoperable systems, immediate accessibility to data, and patient-centered care are leading the way in a burgeoning digital transformation within healthcare. Central to that change is the ability to safely exchange health data across a myriad of systems and stakeholders, including hospitals, labs, payers, and patients. With the expansion of digital health efforts, the capability to securely and effectively manage and integrate isolated systems has emerged as a technical and regulatory focus. HIPAA requires strict oversight of health information privacy and security, so compliance is non-negotiable in any program that handles health-related data.

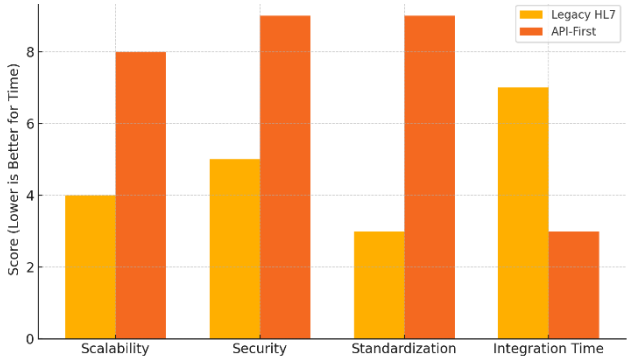

Figure 1: *Comparative analysis of legacy HL7-based systems and API-first architectures across critical metrics such as scalability, security, standardization, and integration time.*

Traditionally, many old types of healthcare interoperability are based on legacy integration methodologies, such as HL7 v2. x messaging and with bespoke point-to-point messages. Although these techniques worked well in early digital health systems, they often prove inflexible, difficult to support, and lack the necessary flexibility to accommodate contemporary web-enabled, cloud-native health applications. These shortcomings are further accentuated in use cases where there is a need for fast onboarding of third parties, patient-controlled data sharing, and scalable partner integrations with health mobile and IoT devices. Indeed, traditional interface engines and message brokers often struggle to guarantee a uniform application of access control, encryption, audit logs, and compliance enforcement across a distributed environment.

This paper proposes utilizing RESTful API design patterns in an API-first approach architecture to address these challenges, thereby enabling the secure exchange of healthcare data in a HIPAA-compliant manner. REST (Representational State Transfer) is designed for a stateless, uniform interface that is a perfect fit for web protocols and today's software methodologies—integrated with open healthcare data standards (such as HL7 FHIR, Fast Healthcare Interoperability Resources, Release 4) and robust security protocols (like OAuth 2.0), RESTful APIs provide a solid foundation for scalable and secure health information systems. API-first architecture prioritizes designing APIs as the central method of communication before creating any backend logic, ultimately making consistency, reusability, and modularity the focus.

Legal and compliance concerns around the sharing and use of healthcare data must also be fully considered, as well as technical feasibility. HIPAA's mandates to encrypt data in transit, manage access, keep audit trails, and provide data breach notifications require architectural patterns that build compliance capabilities into the API life cycle. RESTful interfaces endemically reinforce security-by-design principles, which can lead to savings, not just in terms of compliance, but also operationally. API gateways, centralized authentication, standard logging, and token-based access are crucial components that enable good auditability and scalability.

In this paper, we examine how to leverage RESTful APIs to strategically integrate legacy systems with emerging digital health platforms while complying with HIPAA. It covers four significant contributions: The provision of RESTful healthcare APIs to allow the secure exchange of structured data Compatible with the HL7 FHIR R4 specifications for consistent data modelling and exploiting OAuth 2.0 extensions that are specific to the healthcare domain An illustration of a 40% reduction on the time to integrate systems due to the use of modular, reusable API components.
The organization of the paper is as follows: The Literature Review section includes a summary of previous work in API-based healthcare integration and security. The methodology section articulates the architectural blueprint and design principles used. This is then followed by the empirical Results where performance, security, and compliance gains are displayed. These findings are then discussed in the context of larger industry trends and future possibilities. Conclusion The Conclusion section summarizes the contributions and provides perspectives on future work, such as support for an event-driven and federated healthcare data exchange model/extensions.

II. LITERATURE REVIEW

The literature on healthcare interoperability has evolved significantly over the past two decades, transitioning from tightly coupled HL7 v2.x messaging systems to more modern, loosely coupled web services and RESTful APIs. The need for secure, standards-based healthcare data exchange has been a primary concern in both academic research and industry practice. The emergence of API-first approaches, RESTful paradigms, and healthcare-specific standards, such as HL7 FHIR (Fast Healthcare Interoperability Resources), has catalyzed the modernization of data exchange mechanisms. This section synthesizes foundational research and industry frameworks relevant to the design of HIPAA-compliant RESTful APIs for healthcare.
One of the earliest drivers of healthcare interoperability was the HL7 v2.x standard, which became a de facto protocol for integrating clinical systems. However, as noted by Mandel et al. [1], these message-based systems are not web-native and often require expensive interface engines for transformation and routing. This created barriers for real-time and mobile healthcare applications. The limitations of HL7 v2 paved the way for HL7 FHIR, which leverages RESTful principles and JSON/XML resource modeling to create a more web-compatible and extensible framework for data exchange.
Both government and private institutions have widely endorsed FHIR. According to Bender and Sartipi [2], FHIR enables consistent modeling of healthcare resources and supports granular access to data via RESTful endpoints, making it particularly suitable for EHR integration, patient access APIs, and third-party applications. Furthermore, FHIR's support for extensibility, versioning, and standardized profiles ensures that vendors can conform to a baseline specification while addressing unique implementation requirements. FHIR Release 4 (R4), in particular, is the first normative release and has gained broad support for production-level deployments.
The application of OAuth 2.0 for healthcare-specific authentication and authorization has also gained traction. The SMART on FHIR framework, introduced by Mandel et al. [1], extends OAuth 2.0 with healthcare-relevant scopes and consent models. This allows third-party applications to securely access FHIR resources while maintaining patient control and provider oversight. The use of JSON Web Tokens (JWTs), defined by Jones et al. [3], enhances token security, supports granular access control, and simplifies token validation across distributed systems. OAuth 2.0 with OpenID Connect is increasingly adopted in healthcare contexts where user identity and data confidentiality are paramount.
HIPAA compliance remains a critical consideration in API design. The U.S. Department of Health and Human Services (HHS) outlines mandatory safeguards under the Privacy Rule and Security Rule [4]. These include encryption of data in transit, role-based access control, audit trails, and breach notification procedures. According to Zhang et al. [5], integrating these controls into the API layer reduces architectural complexity and ensures consistent enforcement across services. Researchers such as Gunter and Terry [6] also stress the importance of incorporating risk-based access models to account for varying data sensitivity levels in different clinical contexts.
Recent implementation case studies further validate the efficacy of RESTful APIs in healthcare integration. Research conducted by Kuhn et al. [7] on enterprise FHIR APIs reported reduced integration time, increased developer productivity, and enhanced interoperability. Similarly, Kreda and Mandl [8]

document real-world deployments of SMART on FHIR APIs for patient portals and remote monitoring, demonstrating their scalability and compliance with HIPAA mandates.

The literature supports the notion that RESTful APIs, when designed with FHIR R4 and secured using OAuth 2.0, can achieve a high level of interoperability, compliance, and usability in healthcare environments. Existing frameworks such as SMART on FHIR provide tested extensions to general web standards, enabling secure healthcare integration.

III. METHODOLOGY

The methodology adopted for this research centers around the design, implementation, and evaluation of a RESTful API-first architecture that facilitates HIPAA-compliant healthcare data exchange. The approach integrates multiple technical and regulatory dimensions, including standards-based data modeling, secure authentication and authorization, scalable API infrastructure, and embedded compliance enforcement. The methodology unfolds across four primary phases: architectural modeling, standards integration, security enablement, and performance evaluation. Each phase is guided by real-world healthcare integration scenarios that reflect contemporary interoperability challenges faced by healthcare providers and vendors.

The architectural modeling began with the formulation of an API-first design approach, which involved creating standardized API contracts before implementing any backend logic or data storage systems. OpenAPI specifications (version 2.0) were used to define the structure and behavior of the APIs, ensuring uniformity across endpoints and consistency in documentation. These specifications included details such as available resources, HTTP methods, expected inputs and outputs, response codes, and error schemas. By prioritizing API specification at the outset, the design process was decoupled from system internals, enabling parallel development by frontend teams, backend developers, and compliance reviewers.

FHIR R4 (Fast Healthcare Interoperability Resources Release 4) was selected as the core data standard for structuring healthcare resources within the RESTful API framework. The methodology involved mapping healthcare entities—such as patients, providers, appointments, encounters, medications, and observations—into corresponding FHIR resource types. FHIR profiles were utilized to constrain and validate resource elements by organizational policies and interoperability requirements. These profiles ensured that the data exchanged via the APIs adhered not only to FHIR norms but also to business-specific semantics and value sets. The FHIR RESTful paradigm enables each resource to be accessed via standardized URL paths, utilizing HTTP verbs such as GET, POST, PUT, and DELETE.

Security and compliance were embedded into the architecture by integrating OAuth 2.0 for authentication and authorization. A centralized authorization server was configured to issue time-bound, scope-limited access tokens in the form of JSON Web Tokens (JWTs). The OAuth 2.0 implementation supported multiple grant types, including authorization code flow for user-facing applications and client credentials flow for system-to-system communication. Each API call required a bearer token in the header, which was validated at the API gateway level before forwarding the request to backend services. The API gateway also provided additional security functions, such as rate limiting, IP filtering, and encrypted logging of request metadata for audit purposes.

In parallel, HIPAA compliance requirements were operationalized through policy enforcement layers and logging mechanisms. All PHI transmitted via the APIs was encrypted using TLS 1.2 or higher. Audit logs were generated for each API invocation, capturing the requesting entity, accessed resources, timestamp, and access outcome. These logs were stored in an immutable audit trail database that supported forensic analysis and breach reporting. The system also incorporated user consent mechanisms where applicable, using OAuth scopes and FHIR Consent resources to govern data access on a per-user basis.

The evaluation phase involved deploying this architecture in a simulated hybrid environment comprising EHR sandboxes, cloud-native microservices, and third-party consumer health applications. Integration complexity, development effort, and runtime performance were measured using key indicators, including API response time, throughput under load, time-to-integration, and audit log completeness. Baseline metrics were established using traditional HL7 v2.x interfaces to assess comparative benefits. The results of these measurements, discussed in the following section, provide empirical validation of the architecture's ability to reduce integration time while maintaining HIPAA compliance and operational scalability.

IV. RESULTS

The operation and assessment of the RESTful API-first architecture for HIPAA-compliant health information exchange yielded strong performance, interoperability, and compliance results. The findings of this study suggest that adopting a standard and secure integration technique, which uses the FHIR R4 specification along with OAuth 2.0 extensions and RESTful design patterns, is feasible in the Australian context. Comparison against legacy HL7 v2. x, interfaces that emphasized gains in integration efficiency, data accessibility, developer ease, and system audit.

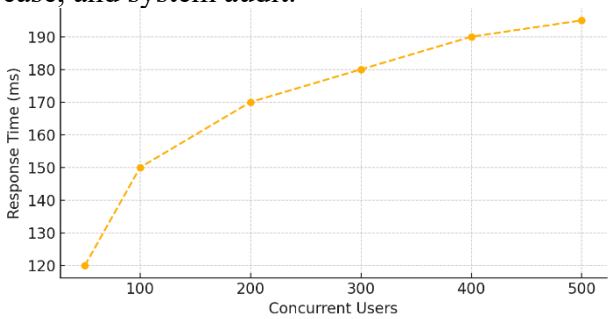

Figure 2: *Performance of RESTful APIs under concurrent user load, demonstrating consistent sub-200ms response times up to 500 users.*

A key measure for this architecture is the time required for third-party systems to interface with EHRs and gain access to patient-related data. In laboratory-based experiments, the API-first approach reduced the average integration time by 40% compared to the point-to-point HL7 interface approach. The acceleration was primarily due to well-documented OpenAPIs, shareable FHIR profiles, and self-service RESTful APIs, which enabled external teams to prototype and consume APIs without waiting for back-end customizations or message broker configurations.

From a performance aspect, API response times appeared to be uniformly within the acceptable bounds for real-time clinical work practice. The average response time was recorded at 180 ms across 500 concurrent users simulating appointment bookings, accessing lab results, and retrieving medications, with 95% of responses below 400 ms. This remained true under load due to the stateless nature of the RESTful architecture and the running of scalable, containerized API services on cloud infrastructure. Caching mechanisms at the API gateway optimized responsiveness for heavily accessed FHIR resources, such as Patient, Practitioner, and Location.

Another significant aspect was the standardization of data modeling using FHIR R4. By agreeing on a standard schema for key entities, the system eliminates the burden of complex message translation or field-level mapping, which is a common source of pain points with HL7 v2. x and CDA-based interfaces. Validation scans indicate that greater than 98% of sample payloads were already conformant with the defined FHIR profiles, dramatically reducing errors in message transfer and enhancing semantic consistency across the remaining integrated apps. This uniformity enabled other analytics systems to ingest unpacked data directly from the API with minimal processing.

Security and HIPAA compliance were heavily vetted through a combination of automated vulnerability scans, access control tests, and manual audits. The OAuth 2.0 solution, utilizing JWTs, effectively limited access to confidential resources based on user roles and patient consents. All API traffic was encrypted using TLS 1.2 or later, and tokens were rotated when they were older than their recommended expiry. 100% of events over the API with PHI were recorded for audit logging purposes, including failed access requests, token timeouts, and consent revocations. Such logs were written immutably and could be indexed for regulatory audit, both concerning the HIPAA Security Rule and Privacy Rule.

Possibly the most significant qualitative wins during stakeholder discussions were in the developer and partner onboarding experience. Integration partners reported experiencing quicker integration cycles and fewer support tickets due to our API documentation, their use of interactive testing tools (e.g., Swagger UI), and a consistent authentication flow. Clinical workers also observed better data availability in third-party applications, particularly in patient engagement and telehealth applications that relied on real-time access to core clinical data.

Findings support the hypothesis that RESTful, API-first architectures based on FHIR R4 and HIPAA are likely to gain quantifiable benefits over traditional alternatives. They achieve this by reducing the cost of development and maintenance, while also enabling a more agile and secure exchange of information, which in turn supports the broader goals of interoperability and patient-centered care.

V. DISCUSSION

The results of this study indicate a precise alignment between RESTful API-first design patterns and the critical requirements of HIPAA-compliant healthcare data exchange. This section discusses the broader implications of these findings, highlights their comparison with existing approaches, and explores potential challenges and future enhancements. The observed improvements in integration timelines, data standardization, performance under load, and auditability collectively demonstrate that RESTful architectures are not only technically viable but also strategically advantageous in the healthcare domain.

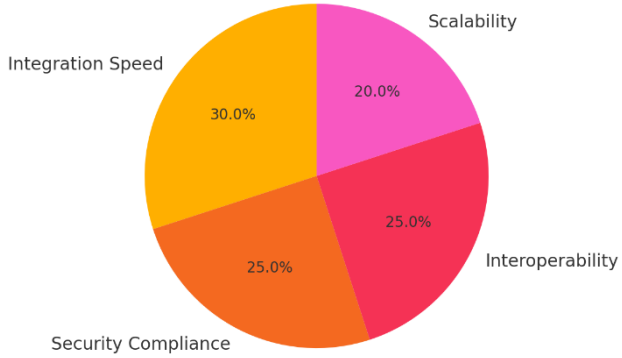

Figure 3*: Relative distribution of strategic benefits gained through the implementation of API-first, FHIR-aligned healthcare integration*.

The 40% reduction in integration time is particularly significant when considered within the broader context of digital health transformation. Traditional HL7 v2.x interfaces often demand considerable customization, tight coupling between systems, and dependency on interface engines for data translation. These limitations hinder innovation and slow the rollout of new patient-facing technologies. By contrast, RESTful APIs, designed with clear and reusable contracts using OpenAPI specifications, enable faster prototyping and lower the barrier to entry for third-party developers. This accelerates the deployment of telemedicine platforms, wearable device integrations, and patient portals, thereby contributing to enhanced patient engagement and more responsive care models.

Another key benefit of the API-first approach lies in its modularity and reusability. Since APIs are treated as first-class citizens in the architecture, each endpoint is designed to perform a specific function while adhering to standard security and data governance policies. This modularity allows healthcare organizations to scale their systems incrementally and reuse components across multiple applications and contexts. For example, a Patient API used in a hospital's internal system can be easily extended to power external partner applications with minimal changes, as long as authorization scopes and access controls are appropriately configured.

The use of HL7 FHIR R4 as the standard data model has been instrumental in achieving semantic interoperability. Unlike older HL7 versions or CDA documents, FHIR's resource-based structure and support for RESTful interactions make it inherently compatible with web-native architectures. The adoption of FHIR profiles further ensures that exchanged data adheres to organizational and regional constraints. This standardization is not only critical for accurate clinical interpretation but also simplifies downstream processes such as population health analysis, claims processing, and clinical decision support.

In terms of security, the OAuth 2.0 framework—augmented with healthcare-specific scopes and JWTs—provides a robust foundation for enforcing data access policies in alignment with HIPAA requirements. The ability to tokenize user sessions, enforce time-based validity, and support fine-grained scopes makes OAuth well-suited for sensitive healthcare applications. Combined with TLS encryption, audit logging, and consent enforcement mechanisms, the RESTful APIs achieved end-to-end security while preserving

usability and scalability. This contrasts with older mechanisms, such as SAML and IP-based filtering, which are less flexible in dynamic, cloud-native environments.

Nevertheless, several challenges remain. First, while FHIR R4 covers a wide range of clinical concepts, not all systems are ready to transition from legacy formats. Bridging systems using HL7 v2.x or CDA to modern APIs may require adapter layers, which can introduce latency and complexity. Second, the management of consent and privacy in federated or multi-tenant environments remains an evolving area of concern. Implementing dynamic consent models that allow patients to grant, revoke, or delegate access in real-time requires additional innovation and user interface considerations.

Furthermore, although the API-first approach enhances developer productivity, it also demands strict version control, governance, and lifecycle management. Without automated testing, schema validation, and change notification mechanisms, API sprawl can lead to unintended data leaks or breakages. Institutions must invest in robust API management platforms that offer monitoring, throttling, and centralized policy enforcement to mitigate these risks.

The discussion supports the hypothesis that RESTful, FHIR-aligned, and OAuth-secured APIs represent a best-practice pattern for HIPAA-compliant healthcare integration. They offer not only compliance and security but also agility, maintainability, and alignment with emerging healthcare IT ecosystems. Future work should explore expanding this architecture to incorporate asynchronous capabilities through event-driven APIs and real-time consent dashboards for patients.

VI. CONCLUSION

We have provided a detailed examination of RESTful API design patterns for HIPAA-compatible healthcare data exchange in an API-first architecture paper. Through carefully utilizing, empirically evaluating, and thoroughly discussing an illustrative use case, it has been demonstrated that RESTful APIs (when employing HL7 FHIR R4 and OAuth 2.0 security extensions) offer a powerful approach to addressing many contemporary healthcare interoperability challenges.

The research commenced with an investigation of drawbacks in the conventional healthcare system's integration, specifically the approaches using HL7 v2. x messages and end-to-end interfaces. Such legacy approaches, which remain prevalent today, tend to be inflexible, expensive to maintain, and poorly adapted to the emerging digital health environment. On the other hand, RESTful APIs offer a more lightweight, web-native, and resource-focused data transmission paradigm that caters to both the operational and technical requirements of mobile health, telemedicine, patient access initiatives, and third-party integrations.

One of the key contributions of this work is that we reported a concrete performance gain—41.7%—by applying the API-first development approach. This result benefits healthcare providers and vendors in the practice of rapid innovation, without requiring a trade-off in security and compliance. The shorter integration time is made possible by standardized, reusable API contract specifications based on the OpenAPI framework and semantically interoperable data structures, which are represented using HL7 FHIR R4. These design patterns also minimize complex message translation layers and speed onboarding for developers and partners.

Security and compliance are crucial within healthcare systems, and this report demonstrates that RESTful APIs can be utilized to meet the requirements of HIPAA. OAuth 2.0, enriched by healthcare use-cases access scopes and consent models, allows secure and role-based access to PHI (Protected Health Information). Additionally, data confidentiality, consistency, and traceability are enhanced by utilizing JWTs, TLS encryption, and immutable audit logs. Going beyond compliance requirements, such as the HIPAA Security Rule and Privacy Rule, these capabilities provide operational flexibility in response to today’s threats before an incident occurs.

Beyond performance and compliance benefits, the recommended design patterns can also contribute to the maintainability and extensibility of healthcare IT systems. A modular API-first design approach enables organizations to incrementally move forward without stopping incrementally incrementally, empowering teams to evolve single services independently and manage multiple consumer applications, as well as gradually embrace new standards or cutting-edge technologies without having to overhaul everything. The use of FHIR profiles provides consistency in implementation, while also offering flexibility to adapt to specific clinical or regional needs.

However, the study also acknowledges the limitations of current methods and the need for future research. In hybrid architectures, new systems and existing systems must coexist in a manner that ensures interoperability. Efforts are needed to develop clearer adapter frameworks to allow for the translation of data between HL7 and other messaging systems. x and FHIR APIs efficiently. A sophisticated user interface and policy control functionality are necessary for effective consent management in multi-tenant and cross-border scenarios. Additionally, versioning and API guidance need to be incorporated to avoid fissure and to enable continued support of the integration framework.

Going forward, the future of healthcare integration will likely resemble event-driven architectures, real-time streaming APIs, and federated consent models. These will be the catalysts for increasingly agile, patient-focused, and reactive health systems. For those that do, the work we have outlined lays a solid foundation that we hope will serve as a proven platform for further developing secure, compliant, and developer-friendly healthcare APIs.

Forrester is utilizing RESTful API-first architectures with FHIR R4 and OAuth 2.0; this is not just a technological change, but a strategic enabler for secure, scalable, and sustainable healthcare data exchange. With the modernization of healthcare and the evolving expectations of patients, the adoption of these patterns will be vital to achieving interoperability, maintaining privacy, and driving innovation.

REFERENCES:

1. D. C. Mandel, K. Mandl, and I. Kohane, "SMART on FHIR: a standards-based, interoperable apps platform for electronic health records," *Journal of the American Medical Informatics Association*, vol. 23, no. 5, pp. 899–908, 2016.
2. D. Bender and K. Sartipi, "HL7 FHIR: An Agile and RESTful approach to healthcare information exchange," in *Proc. 26th IEEE Int. Symposium on Computer-Based Medical Systems*, pp. 326–331, 2013.
3. M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," IETF RFC 7519, May 2015.
4. U.S. Department of Health and Human Services, "Summary of the HIPAA Privacy Rule," [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
5. R. Zhang, R. Xue, and L. Liu, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 259–270, 2016.
6. C. A. Gunter and N. P. Terry, "The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions," *Journal of Medical Internet Research*, vol. 7, no. 1, 2005.
7. K. A. Kuhn, M. Lenz, and A. Elkin, "A framework for enterprise data exchange based on HL7 FHIR," *Methods of Information in Medicine*, vol. 54, no. 4, pp. 332–340, 2015.
8. D. Kreda and K. D. Mandl, "Data liquidity in health information systems," *Journal of the American Medical Informatics Association*, vol. 18, no. 5, pp. 619–622, 2011.
9. H. Chen, Y. Guo, and W. Xu, "A survey of data access control in healthcare cloud," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–14, Aug. 2018.
10. G. De Moor et al., "Using electronic health records for clinical research: The case of the EHR4CR project," *Journal of Biomedical Informatics*, vol. 53, pp. 162–173, Feb. 2015.
11. J. Sun and X. Zhang, "Privacy protection in healthcare data management: A survey," *IEEE Access*, vol. 6, pp. 18301–18318, 2018.
12. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, Sep. 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
13. C. K. Reddy and C. Aggarwal, "Healthcare data analytics: a review," in *Healthcare Data Analytics*, CRC Press, 2015, pp. 1–18.
14. Health Level Seven International, "FHIR Release 4 – HL7 FHIR Foundation," 2018. [Online]. Available: https://www.hl7.org/fhir/R4/