HL7 (Health Level Seven) Security

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

Xinlei Lin
Jiabo Wang

Índice

1. Introducción

- Health Level 7 (HL7)
- HL7: conjunto de estándares que han sido adoptados a nivel mundial com base para el intercambio estructurado de dato médicos.
- A medida que se incrementa la cantidad de datos sensibles transmitidos, surge una preocupación creciente por los riesgos asociados a su seguridad
- FHIR: surge como opción para asegurar la seguridad en el intercambio de datos

2. Objetivos

Analizar los mecanismos de seguridad definidos por el estándar FHIR en el contexto de HL7

- Identificar/describir los principales componentes de seguridad: autenticación, autorización y cifrado
- Analizar la correspondencia entre las medidas de seguridad de FHIR y los requisitos establecidos por normativas como GDPR, HIPAA o ISO/IEC 27001
- Proponer posibles mejoras o recomendaciones para fortalecer la seguridad en implementaciones futuras
- Evaluar los desafíos más relevantes en la adopción de las políticas de seguridad de FHIR en sistemas reales

3. FHIR

Los estándares HL7 más importantes son HL7 v2, HL7 v3, CDA, HL7 FHIR y CCOW. Entre los cuales, destaca FHIR por ser el estándar más moderno, flexible y orientado a tecnologías web.

Fast Healthcare Interoperability Resources (FHIR) utiliza formatos como JSON y XML, se apoya en protocolos seguros como HTTPS, e integra mecanismos de autenticación y control de acceso como OAuth 2.0 y OpenID Connect.

También define un conjunto de “recursos” que representan conceptos clínicos granulares.

Esto lo convierte en el estándar preferido para nuevos desarrollos en salud digital, impulsando la transformación digital del sector sanitario.

3.1 FHIR - Autenticación / autorización

Objetivo: Autenticar correctamente a los usuarios y sistemas para prevenir accesos no autorizados.

FHIR no implementa autenticación directamente, pero **está diseñado para integrarse fácilmente con estándares modernos**, especialmente:

- **OAuth 2.0**: mecanismo de autorización para sistemas REST, ampliamente soportado por FHIR. Permite emitir *access tokens* seguros y con expiración.
- **OpenID Connect**: se usa para autenticar usuarios finales (pacientes, médicos) sobre OAuth 2.0, proporcionando información de identidad de forma segura.
- **SMART on FHIR**: es un estándar que permite crear aplicaciones de salud que se integran fácilmente con sistema historiales médicos electrónicos (EHR), usando OAuth 2.0 y OpenId Connect.

3.2 FHIR - Control de acceso y autorización

Objetivo: Permitir definir quién puede hacer qué dentro del sistema de salud (leer, escribir, modificar, eliminar datos).

Una vez autenticado el usuario, FHIR permite definir políticas de autorización basadas en:

- **Scopes de OAuth2**: controlan qué recursos puede acceder una app.
- **Access Control Lists (ACLs)** en el servidor FHIR.
- **Attribute-Based Access Control (ABAC)** y **Role-Based Access Control (RBAC)**, definidos a través de perfiles personalizados o motores externos.

FHIR también trabaja en **Consent Resources** y **Provenance** para definir explícitamente qué datos pueden compartirse y bajo qué condiciones.

3.3 FHIR - Cifrado y Seguridad en la transmisión

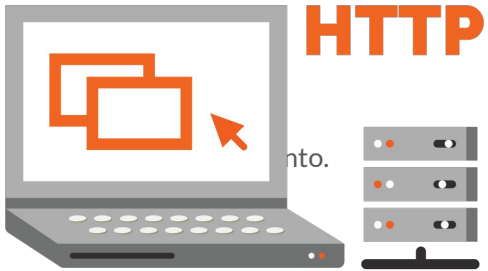
Objetivo: Proteger la información médica durante el envío entre sistemas, evitando espionaje o ataques de intermediarios.

FHIR utiliza el protocolo **HTTPS (TLS 1.2 o superior)** como requisito mínimo para cualquier implementación segura:

- Previene ataques de intermediario (Man-in-the-Middle).
- Asegura que los datos transmitidos estén **cifrados en tránsito**.

En tránsito:

- **HTTPS + TLS 1.2/1.3** son obligatorios para proteger la comunicación entre clientes y servidores.



En reposo:

- **Cifrado con AES-256 o RSA** en bases de datos nto.
- **Uso de HSMs (Hardware Security Modules)** para protección de claves en entornos críticos.

Esto previene la exposición de datos sensibles en caso de pérdida o robo de dispositivos o acceso a disco.

3.4 FHIR - Integridad de datos

Objetivo: Asegurar que la información no haya sido alterada intencional o accidentalmente.

FHIR permite mantener la integridad de los datos mediante:

- **Firmas digitales** (digital signatures), mediante el recurso `Signature`, que puede usarse para firmar recursos o transacciones.

- **Estrategias de hashing** para comprobar que los datos no han sido alterados entre origen y destino.

- Uso de **versionado de recursos**, que ayuda a rastrear cambios e identificar modificaciones no autorizadas.

3.5 FHIR - Gestión de identidad

Objetivo: Los sistemas de salud deben identificar correctamente a pacientes, usuarios, profesionales y dispositivos para evitar errores o fraudes.

- Se integran **Identity Providers (IdP)** a través de OpenID Connect para asegurar qué usuarios estén verificados.

- FHIR permite interoperar con sistemas de gestión de identidad de pacientes, profesionales y dispositivos.

- **Identifier Systems** se utilizan en los recursos (ej. identificadores de recursos o de pacientes) para garantizar unicidad y trazabilidad.

3.6 FHIR - Recursos

1. **Patient**: Representa la **información demográfica y administrativa** de un paciente. Contiene:
    - Nombre, dirección, género, fecha de nacimiento.
    - Identificadores únicos (DNI, número de historia clínica).
    - Información de contacto (teléfono, correo).
    - Relación con familiares/responsables.
    -
2. **Practitioner**: Representa a un **profesional de la salud** (médico, enfermero, técnico, etc.). Contiene:
    - Identificadores (registro colegial, NIF).
    - Nombre y datos de contacto.
    - Especialidades médicas.
    - Afiliación a organizaciones.

```
{
  "resourceType": "Patient",
  "id": "12345",
  "identifier": [
    {
      "system": "http://example.org/mrns",
      "value": "123456"
    }
  ],
  "name": [
    {
      "use": "official",
      "family": "Doe",
      "given": ["John"]
    }
  ],
  "gender": "male",
  "birthDate": "1970-01-01",
  "address": [
    {
      "use": "home",
      "line": ["123 Main St"],
      "city": "Anytown",
      "state": "WA",
      "postalCode": "12345",
      "country": "USA"
    }
  ]
}
```

3.6 FHIR - Recursos

3. **Encounter**: Describe una **interacción entre paciente y sistema de salud**, como una consulta, hospitalización o telemedicina.

- Fecha y duración del encuentro.
- Tipo de encuentro (ambulatorio, urgencia, internación).
- Lugar y organización.
- Participantes (paciente, médico, enfermero)

4. **Condition**: Representa un **diagnóstico, problema clínico o condición médica** del paciente. Contiene:

- Código clínico (ICD-10, SNOMED CT).
- Estado clínico (activo, resuelto).
- Fecha de inicio y resolución.
- Observaciones y notas clínicas.

3.6 FHIR - Recursos

5. Observation: Registra **datos clínicos u observaciones médicas**, como signos vitales, resultados de laboratorio, medidas físicas, etc.

- Tipo de observación (por ejemplo, presión arterial, glucosa).
- Valor cuantitativo o cualitativo.
- Fecha y unidad de medida.
- Relación con paciente y encuentro.

4. Quién se dedica a desarrollar HL7

Health Level Seven International (HL7.org) - organización sin fines de lucro fundada en EE. UU. que lidera el desarrollo de estándares HL7

Estructura de HL7: Internacionales y regionales - HL7 España, HL7 Argentina, HL7 México, HL7 Europe y HL7 Brazil, entre otros

Organizaciones aliadas - IHE, SNOMED, También trabaja con gobiernos y agencias como el Reino Unido/NHS, EE. UU./ONC, Canadá/Infoway, así como con la OMS, ISO y la FDA, entre otros.

Comunidad de desarrolladores y proyectos open source - Existe una amplia comunidad de desarrolladores que contribuyen a proyectos de código abierto para implementar FHIR, como HAPI FHIR (Java), Firely .NET SDK, Google FHIR Engine, FHIR.js y fhirpath.js.

Empresas tecnológicas y de salud - Grandes empresas del sector salud y tecnología, como Epic, Cerner (Oracle Health), Siemens Healthineers, Meditech, Google, Microsoft, Amazon y Apple

HL7 International

IHE INTERNATIONAL

SNOMED International

HAPI FHIR

5. Uso en el mercado

HL7 FHIR: El nuevo paradigma de interoperabilidad - Actualmente, FHIR se ha posicionado como el estándar preferido para nuevos desarrollos en interoperabilidad. Su adopción se ha extendido rápidamente en aplicaciones móviles, portales de pacientes y registros de salud personales (PHRs). Las principales plataformas en la nube, incluyendo Google Cloud Healthcare API, Microsoft Azure API for FHIR y Amazon HealthLake, lo han incorporado como estándar base.

5. Uso en el mercado

HL7 v2.x: El estándar histórico predominante - Este formato mantiene una presencia dominante en hospitales, laboratorios y clínicas, siendo utilizado principalmente para el intercambio de información crítica como admisiones, altas, transferencias, resultados de laboratorio y órdenes médicas.

HL7 v3 y CDA: Una adopción selectiva - La versión 3 de HL7 tuvo una implementación más restringida, limitándose principalmente a grandes iniciativas nacionales como Canadá Health Infoway, el sistema UK NHS Spine en su versión original, y algunos servicios de salud autonómicos en España.

6. Problemas y limitaciones

🔧 Variabilidad en implementaciones

Diferentes perfiles/extensiones

↓

Dificultad de compatibilidad

🏥 Infraestructura obsoleta

Sistemas legados no preparados para APIs modernas

⚖️ Gobernanza y regulación difusa

Incertidumbre legal sobre acceso, consentimiento y usos secundarios

🔐 Riesgos de seguridad

Falta de implementación robusta de OAuth2/OpenID

👨‍💻 Déficit de formación técnica

Poca experiencia en REST, JSON, modelado clínico

7. Futuro

Arquitectura moderna(FHIR)

APIs RESTful, JSON, OAuth2

Soporte para móviles, nube , IoT

Adopcion global

Google, Amazon, Microsoft

Ecosistema abierto y colaborativo

Migracion progresiva

Conectores v2 => FHIR

Apoyo normativo: 21st Century Cures Act y European Health Data Space (EHDS)

21st Century Cures

EHDS
HealthData@EU Pilot

Vision futura

FHIR R5, IA y análisis clínico => SNOMED, LOINC

Seguridad avanzada (ABAC, GDPR)

8. Discusión

- **Migración de HL7 v2 a FHIR**

  ¿Deberían los sistemas de salud migrar completamente a FHIR o mantener una coexistencia con HL7 v2?

8. Discusión

- **Seguridad y Privacidad en HL7 FHIR**

  ¿Las especificaciones actuales de FHIR son suficientes para garantizar la privacidad y seguridad de los datos clínicos?

¿Las especificaciones actuales de FHIR son suficientes para garantizar la privacidad y seguridad de los datos clínicos?

Transporte seguro	HTTPS + TLS 1.2/1.3
Almacenamiento seguro	AES-256, RSA, HSM
Autenticación	OpenID Connect, SSO
Autorización	Scopes, Roles, OAuth 2.0, SMART on FHIR
Privacidad	Consentimiento, anonimización
Auditoría	Logs de acceso y acciones
Cumplimiento legal	GDPR, HIPAA, normativas locales

8. Discusión

- **Adopción en Sistemas Públicos y Privados**

  ¿Qué estrategias son más efectivas para lograr la adopción masiva de FHIR en sistemas de salud públicos y privados?

8. Discusión

- **Gobernanza y Control de Datos Clínicos**

  ¿Quién debería tener el control final sobre los datos clínicos: el paciente, el proveedor de salud o el Estado?