Welcome to the National Cybersecurity Center of Excellence

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Thursday, May 19, 2022, 1:00 PM – 3:30 PM (EDT)

We will begin shortly.

This meeting will be recorded.

NIST National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Ron Pulivarti, NIST NCCoE

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Robel Worku
Montgomery County Economic Development Corporation

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Priming the County's Economic Engine

Presented by Robel Worku
Economic Development Specialist

Montgomery County Economic Development Corporation

May 18th, 2022

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

About MCEDC

The **official public-private economic development organization** representing Montgomery County, MD

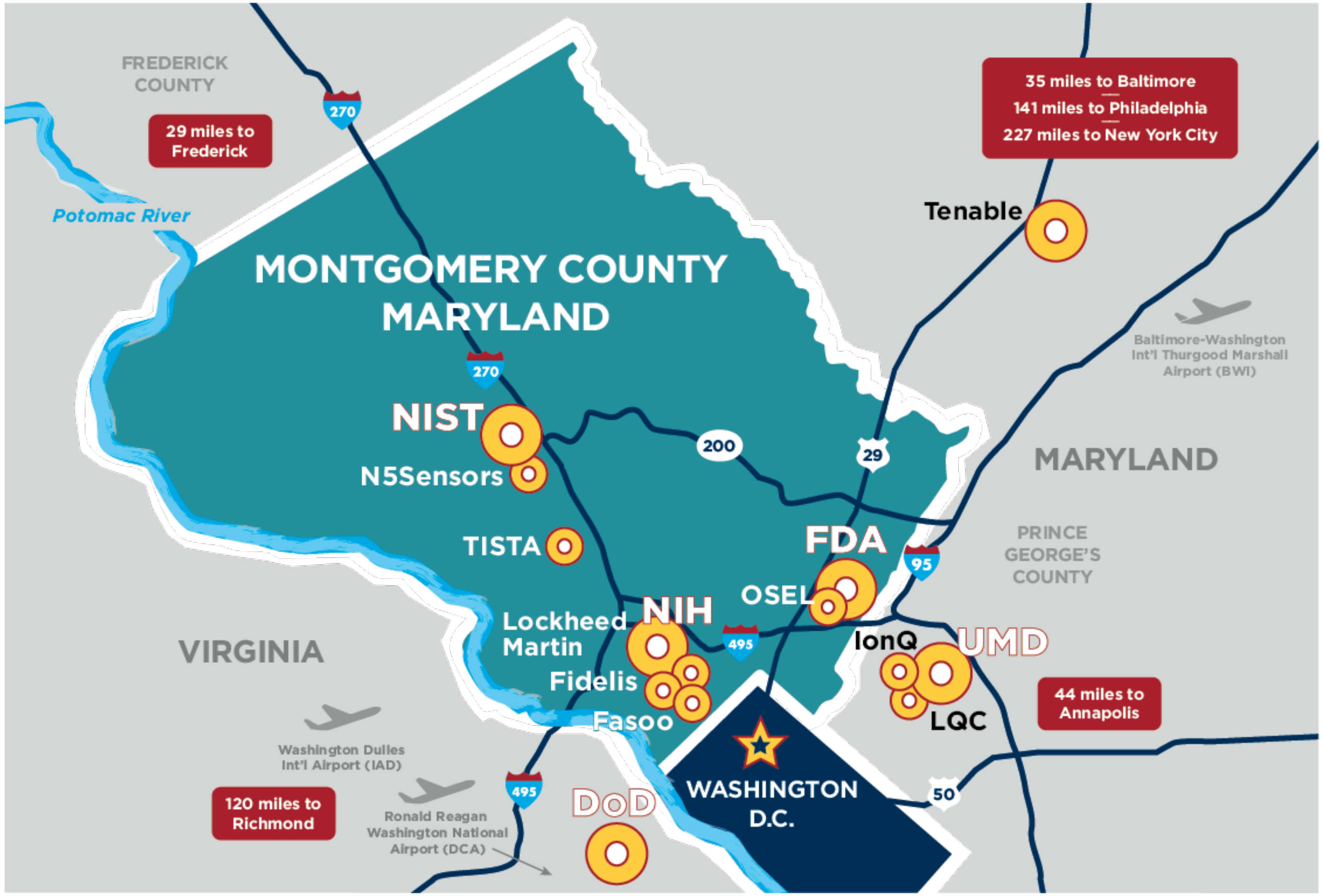
Led by a board of directors, our mission is to **help businesses start and grow in the county, or help companies relocate here**

How does MCEDC help?
We help make connections to:

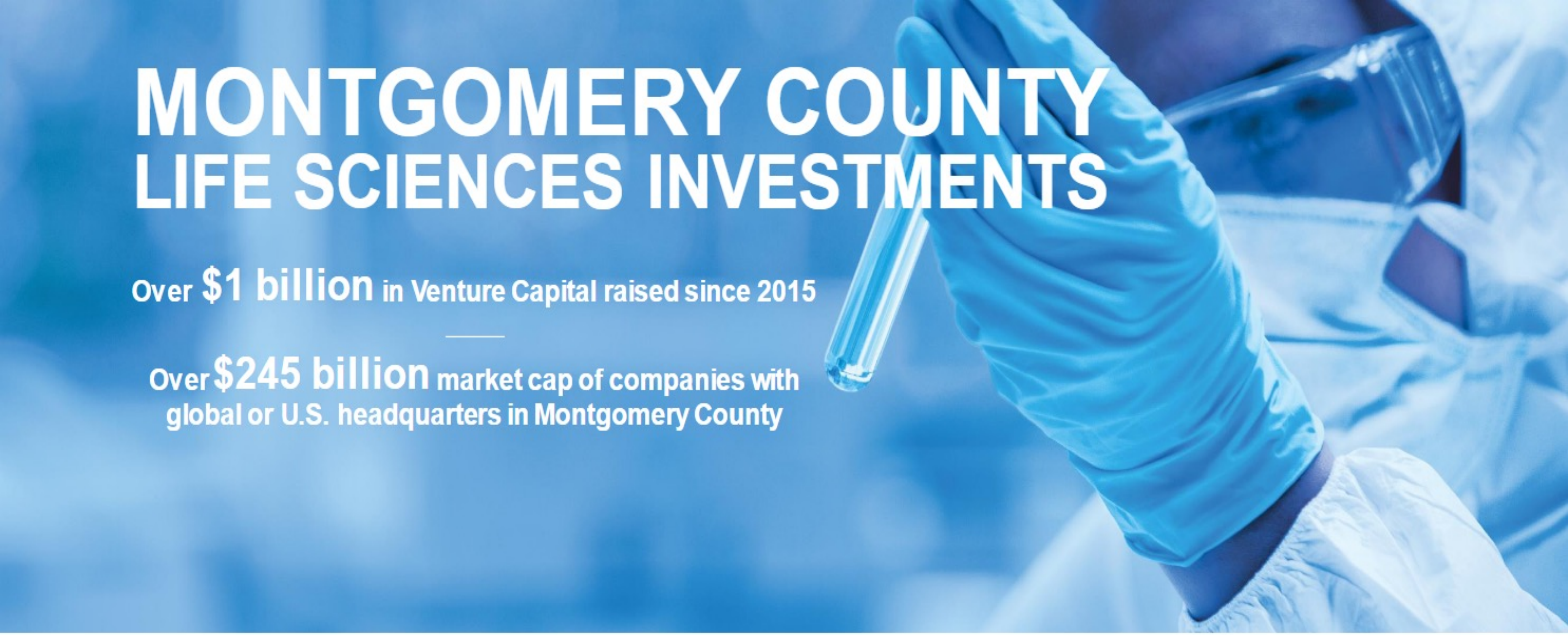
- Gain market intelligence
- Link business owners to aligned partnerships
- Find the ideal business address
- Explore available incentives
- Attract talent and help with workforce training
- Help companies relocate here

Big Data Capital Next to the Nation’s Capital

Partial list of federal assets and local companies



MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND



MONTGOMERY COUNTY
LIFE SCIENCES INVESTMENTS

Over **$1 billion** in Venture Capital raised since 2015

Over **$245 billion** market cap of companies with global or U.S. headquarters in Montgomery County

gsk GlaxoSmithKline QIAGEN AstraZeneca PRECIGEN ADVANCING MEDICINE WITH PRECISION ADAPTIVE PHAGE THERAPEUTICS Janssen PHARMACEUTICAL COMPANIES OF Johnson&Johnson INSILICO MEDICINE United Therapeutics BeneVir NEURALY

VIELABIO CERECOR Senseonics emergent biosolutions Vigene Biosciences Excellence in Gene Delivery REGENXBIO ARCELLX sirnaomics Advancing RNAi Therapeutics Supernus Pharmaceuticals

Major Industries

thinkmoco.com/key-industries

BioHealth and Life Sciences

Cybersecurity

Tech & Quantum Computing

Advanced Manufacturing

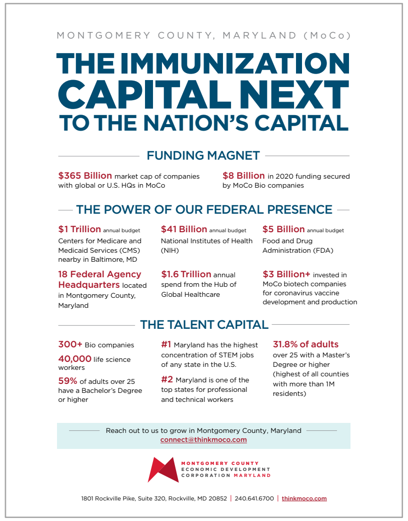
Hospitality & Tourism

Financial Services

Agribusiness

Nonprofits

Click on images to download



MONTGOMERY COUNTY, MARYLAND (MoCo)

THE IMMUNIZATION CAPITAL NEXT TO THE NATION'S CAPITAL

FUNDING MAGNET

$365 Billion market cap of companies with global or U.S. HQs in MoCo

$8 Billion in 2020 funding secured by MoCo Bio companies

THE POWER OF OUR FEDERAL PRESENCE

$1 Trillion annual budget Centers for Medicare and Medicaid Services (CMS) nearby in Baltimore, MD

18 Federal Agency Headquarters located in Montgomery County, Maryland

$41 Billion annual budget National Institutes of Health (NIH)

$1.6 Trillion annual spend from the Hub of Global Healthcare

$5 Billion annual budget Food and Drug Administration (FDA)

$3 Billion+ invested in MoCo biotech companies for coronavirus vaccine development and production

THE TALENT CAPITAL

300+ Bio companies

40,000 life science workers

59% of adults over 25 have a Bachelor's Degree or higher

#1 Maryland has the highest concentration of STEM jobs of any state in the U.S.

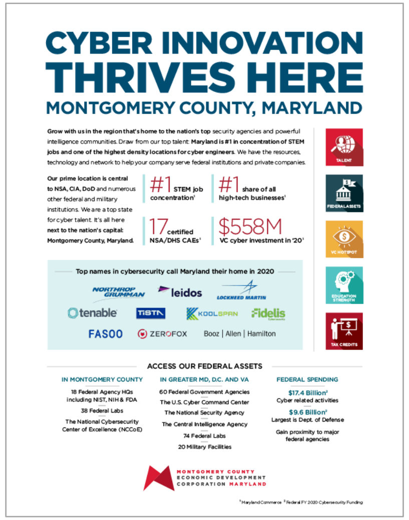
#2 Maryland is one of the top states for professional and technical workers

31.8% of adults over 25 with a Master's Degree or higher (highest of all counties with more than 1M residents)

Reach out to us to grow in Montgomery County, Maryland
connect@thinkmoco.com

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

1801 Rockville Pike, Suite 320, Rockville, MD 20852 | 240.641.6700 | thinkmoco.com



CYBER INNOVATION THRIVES HERE

MONTGOMERY COUNTY, MARYLAND

Grow with us in the region that's home to the nation's top security agencies and powerful intelligence communities. Draw from our top talent: **Maryland is #1 in concentration of STEM jobs and one of the highest density locations for cyber engineers.** We have the resources, technology and network to help your company serve federal institutions and private companies.

Our prime location is central to NSA, CIA, DoD and numerous other federal and military institutions. We are a top state for cyber talent. It's all here **next to the nation's capital: Montgomery County, Maryland.**

#1 STEM job concentration[1]

#1 share of all high-tech businesses[1]

17 certified NSA/DHS CAEs[1]

$558M VC cyber investment in '20[1]

Top names in cybersecurity call Maryland their home in 2020

NORTHROP GRUMMAN
leidos
LOCKHEED MARTIN
tenable
TISTA
KOOLSPAN
Fidelis Cybersecurity
FASOO
ZEROFOX
Booz | Allen | Hamilton

ACCESS OUR FEDERAL ASSETS

IN MONTGOMERY COUNTY

18 Federal Agency HQs including NIST, NIH & FDA

38 Federal Labs

The National Cybersecurity Center of Excellence (NCCoE)

IN GREATER MD, D.C. AND VA

60 Federal Government Agencies

The U.S. Cyber Command Center

The National Security Agency

The Central Intelligence Agency

74 Federal Labs

20 Military Facilities

FEDERAL SPENDING

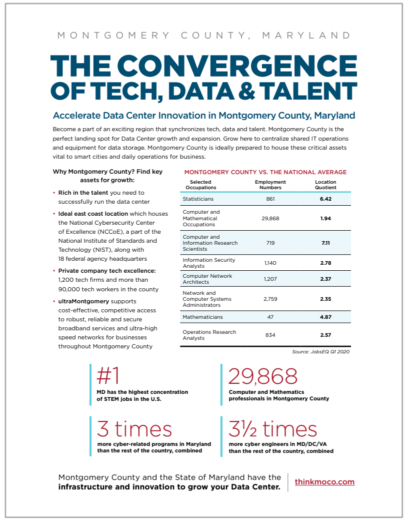
$17.4 Billion[2] Cyber related activities

$9.6 Billion[2] Largest is Dept. of Defense

Gain proximity to major federal agencies

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

[1] Maryland Commerce [2] Federal FY 2020 Cybersecurity Funding



MONTGOMERY COUNTY, MARYLAND

THE CONVERGENCE OF TECH, DATA & TALENT

Accelerate Data Center Innovation in Montgomery County, Maryland

Become a part of an exciting region that synchronizes tech, data and talent. Montgomery County is the perfect landing spot for Data Center growth and expansion. Grow here to centralize shared IT operations and equipment for data storage. Montgomery County is ideally prepared to house these critical assets vital to smart cities and daily operations for business.

Why Montgomery County? Find key assets for growth:

- **Rich in the talent** you need to successfully run the data center
- **Ideal east coast location** which houses the National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), along with 18 federal agency headquarters
- **Private company tech excellence:** 1,200 tech firms and more than 90,000 tech workers in the county
- **ultraMontgomery** supports cost-effective, competitive access to robust, reliable and secure broadband services and ultra-high speed networks for businesses throughout Montgomery County

MONTGOMERY COUNTY VS. THE NATIONAL AVERAGE

Selected Occupations	Employment Numbers	Location Quotient
Statisticians	861	**6.42**
Computer and Mathematical Occupations	29,868	**1.94**
Computer and Information Research Scientists	719	**7.11**
Information Security Analysts	1,140	**2.78**
Computer Network Architects	1,207	**2.37**
Network and Computer Systems Administrators	2,759	**2.35**
Mathematicians	47	**4.87**
Operations Research Analysts	834	**2.57**

Source: JobsEQ Q1 2020

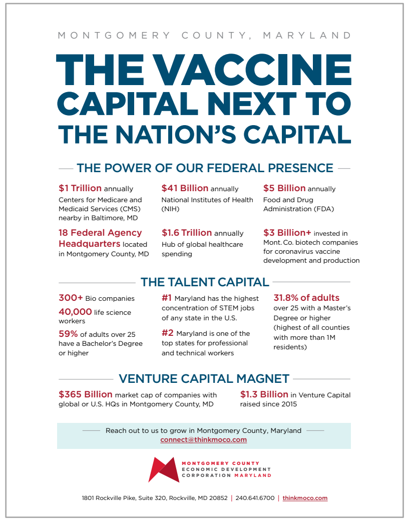
#1 **MD has the highest concentration of STEM jobs in the U.S.**

29,868 **Computer and Mathematics professionals in Montgomery County**

3 times **more cyber-related programs in Maryland than the rest of the country, combined**

3½ times **more cyber engineers in MD/DC/VA than the rest of the country, combined**

Montgomery County and the State of Maryland have the **infrastructure and innovation to grow your Data Center.** | thinkmoco.com



MONTGOMERY COUNTY, MARYLAND

THE VACCINE CAPITAL NEXT TO THE NATION'S CAPITAL

THE POWER OF OUR FEDERAL PRESENCE

$1 Trillion annually Centers for Medicare and Medicaid Services (CMS) nearby in Baltimore, MD

18 Federal Agency Headquarters located in Montgomery County, MD

$41 Billion annually National Institutes of Health (NIH)

$1.6 Trillion annually Hub of global healthcare spending

$5 Billion annually Food and Drug Administration (FDA)

$3 Billion+ invested in Mont. Co. biotech companies for coronavirus vaccine development and production

THE TALENT CAPITAL

300+ Bio companies

40,000 life science workers

59% of adults over 25 have a Bachelor's Degree or higher

#1 Maryland has the highest concentration of STEM jobs of any state in the U.S.

#2 Maryland is one of the top states for professional and technical workers

31.8% of adults over 25 with a Master's Degree or higher (highest of all counties with more than 1M residents)

VENTURE CAPITAL MAGNET

$365 Billion market cap of companies with global or U.S. HQs in Montgomery County, MD

$1.3 Billion in Venture Capital raised since 2015

Reach out to us to grow in Montgomery County, Maryland
connect@thinkmoco.com

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

1801 Rockville Pike, Suite 320, Rockville, MD 20852 | 240.641.6700 | thinkmoco.com

MONTGOMERY COUNTY
ECONOMIC DEVELOPMENT
CORPORATION MARYLAND

THANK YOU

Visit us at thinkmoco.com

robel@thinkmoco.com

Sign up for our newsletter for ongoing business news and support
Send us your updates so we can help promote your business — email us at connect@thinkmoco.com

Workshop Overview

Ron Pulivarti, NIST NCCoE

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

AGENDA: MAY 19

Segment	*Time (EDT)*
Workshop Day 1 Reflections	1:00 PM – 1:10 PM
Session Three: Genomic Data Security Through Risk Management	1:10 PM – 2:10 PM
Break	2:10 PM – 2:25 PM
Session Four: Genomic Data Security in Electronic Health Records	2:25 PM – 3:25 PM
Wrap Up	3:25 PM – 3:30 PM

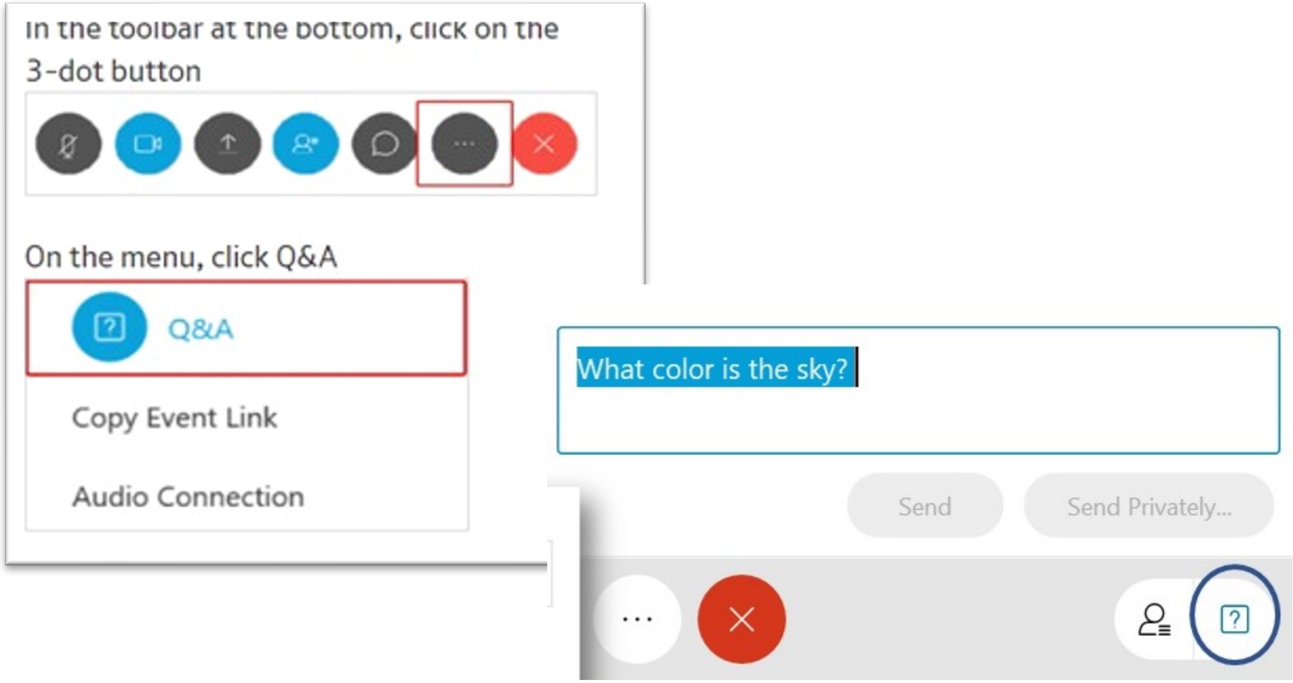
DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe a procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE.

Audience Engagement

Please use the Q&A window to enter your questions for today's workshop. We will do our best to answer the questions in real time.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type your question in the box, along with your name and organization.
3. Click **send**.
4. We will answer as many questions as we are able during Q&A sessions.



In the toolbar at the bottom, click on the 3-dot button

On the menu, click Q&A

What color is the sky?

Housekeeping

- We support the health and well being for all.
    - We are supporting virtual collaboration.
    - We have a 15-minute break planned for the day.

- We want audience engagement.
    - Please pose your questions for today's workshop using the Q&A window.

- We intend to share our learnings today.
    - We are recording this session for future post on the NCCoE Website.
    - We will post the speaker slides and recording on the NCCoE Website.

This meeting is being recorded.

Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Day One Recap

Fred Byers, NIST NCCoE

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Session Three: Genomic Data Security Through Risk Management

Victoria Yan Pillitteri (NIST)

David Bernick (Broad Institute)

NIST Risk Management Framework (RMF) Overview

National Institute of Standards and Technology
U.S. Department of Commerce

Victoria Yan Pillitteri
victoria.yan@nist.gov

Agenda – NIST RMF Overview

About the National Institute of Standards and Technology

Overview of the Federal Information Security Modernization Act (FISMA)

NIST SP 800-37, Rev. 2

Risk Management Framework for Information Systems & Organizations

Additional Resources

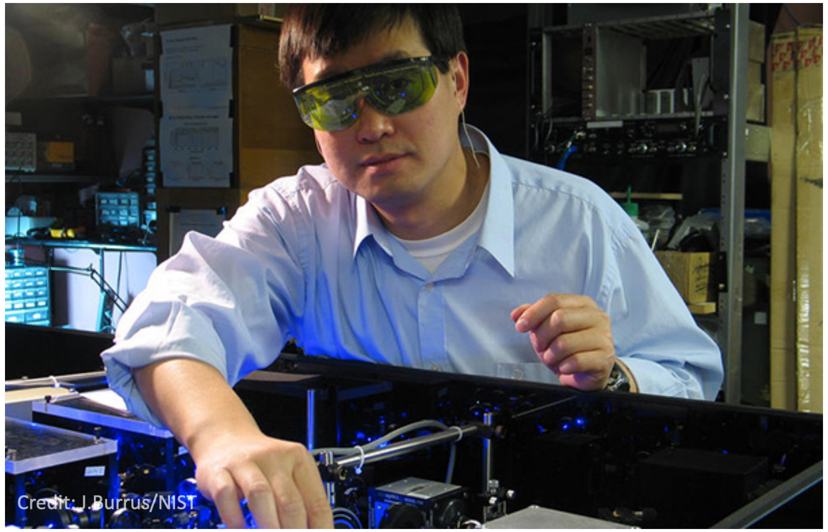
Questions

Contact Information

NIST Mission

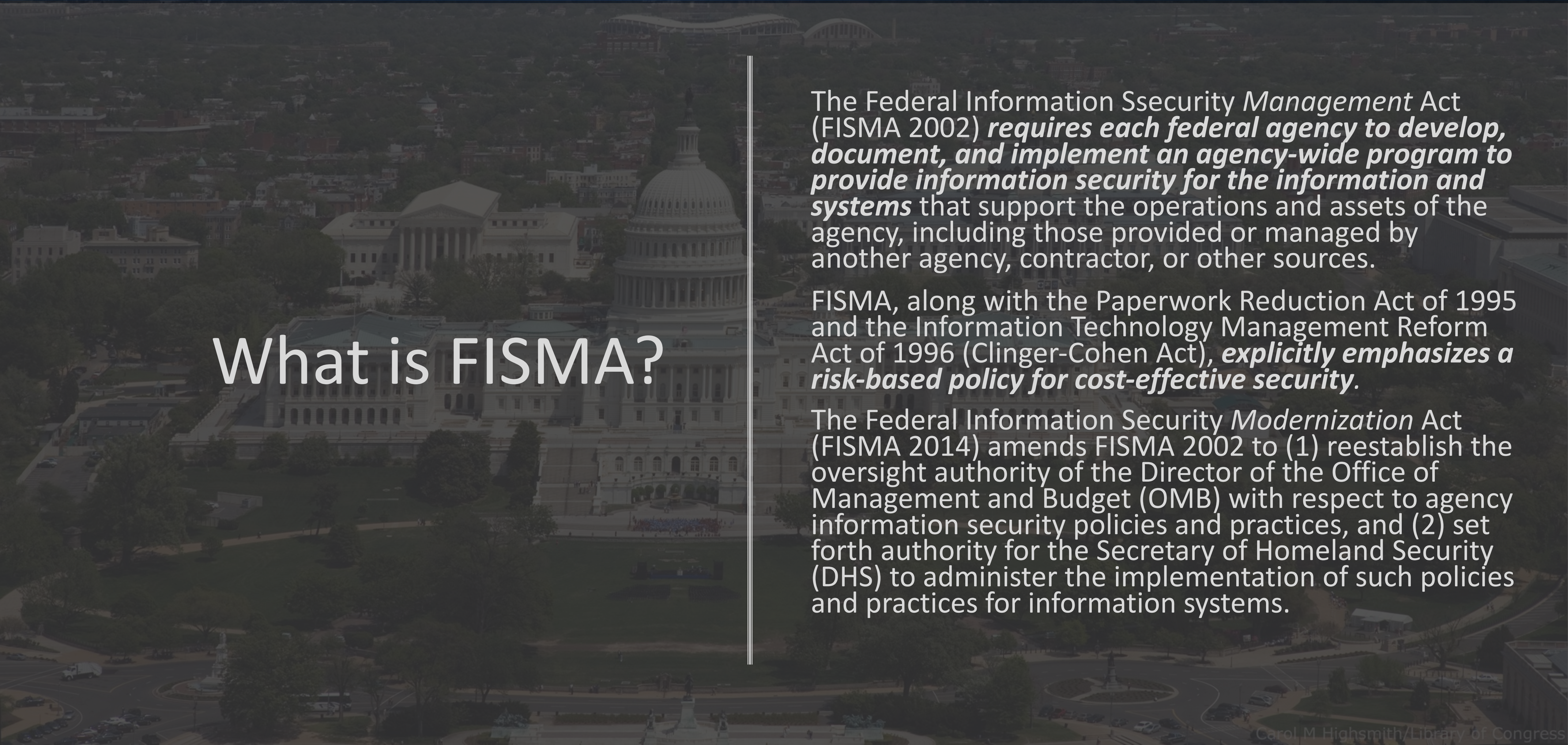
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

©Robert Rathe


Credit: J.Burrus/NIST

©Nicholas McIntosh Photography

Federal Information Security Modernization Act



Carol M Highsmith/Library of Congress

What is FISMA?

The Federal Information Ssecurity *Management* Act (FISMA 2002) ***requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems*** that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), ***explicitly emphasizes a risk-based policy for cost-effective security***.

The Federal Information Security *Modernization* Act (FISMA 2014) amends FISMA 2002 to (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

NIST Special Publication (SP) 800-37

Risk Management Framework (RMF) for Information Systems & Organizations

HOLLISTIC & FLEXIBLE
7 STEP PROCESS
TO MANAGE RISK

ADDRESSES
CYBERSECURITY & PRIVACY
RISK

APPLICABLE TO
ALL TYPES
OF SYSTEMS & ORGANIZATIONS

3 REVISIONS SINCE
2004

ROBUST FEDERAL IMPLEMENTATION OF THE
CYBERSECURITY FRAMEWORK

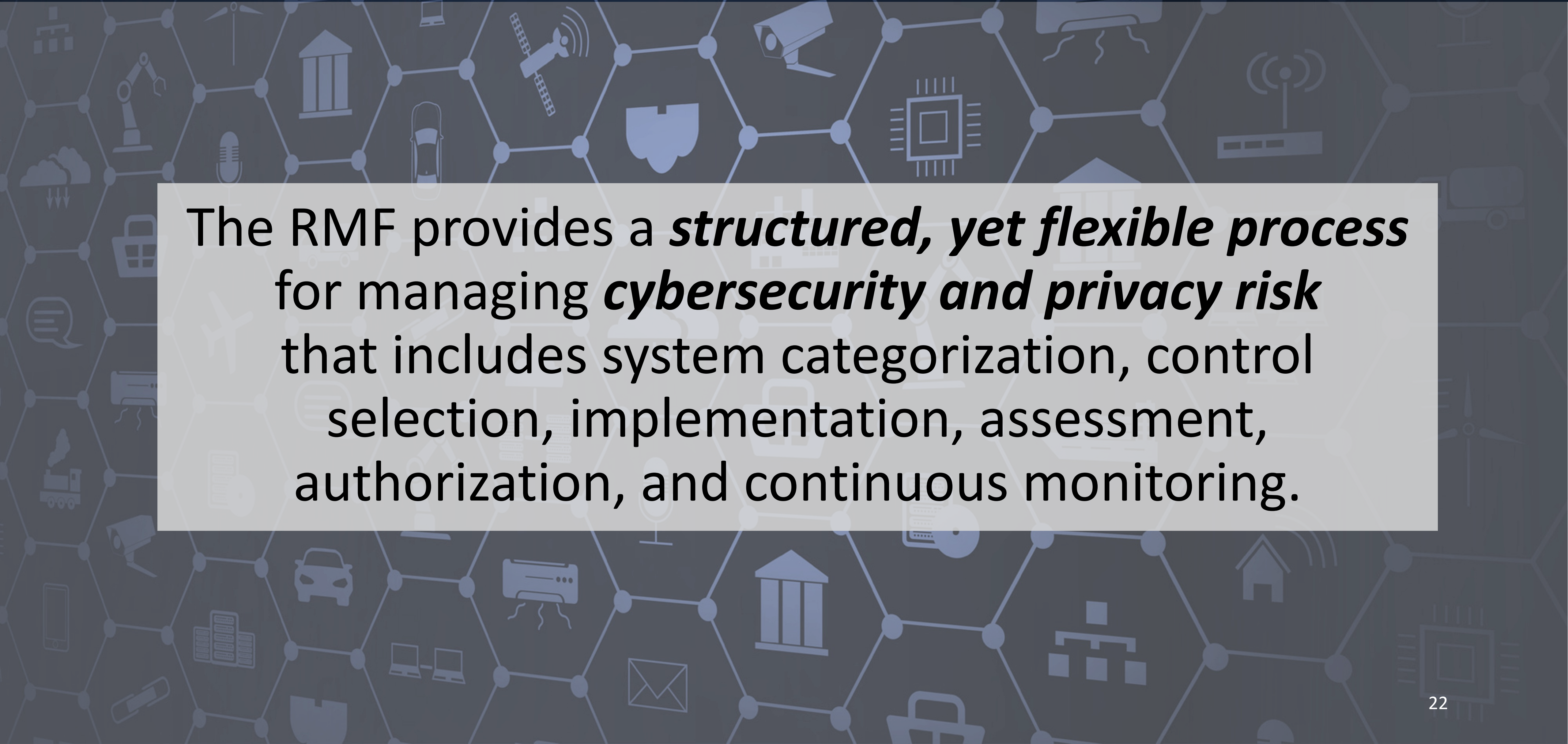
MANDATED BY
OMB A-130
FOR FEDERAL AGENCIES

SYSTEM & COMMON CONTROL
AUTHORIZATIONS

PROVIDES LINKS TO OTHER KEY
NIST PUBS

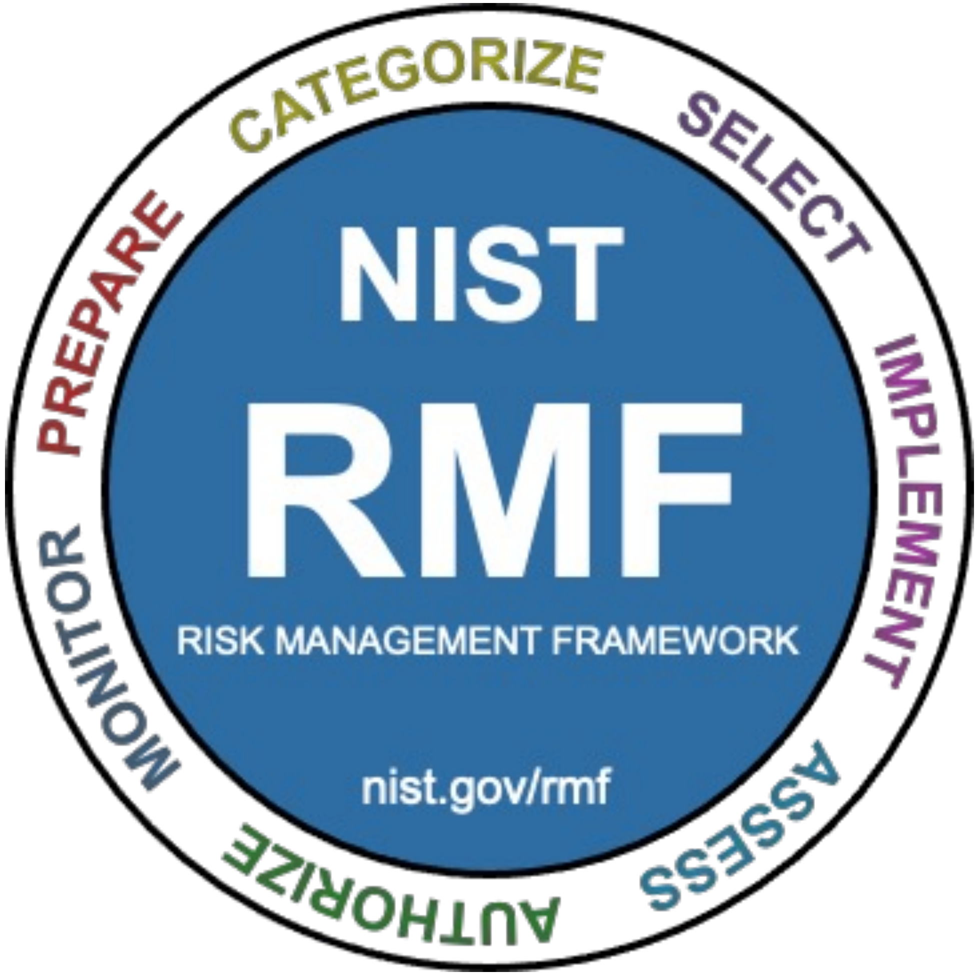
AUTHORIZATION
BOUNDARY
GUIDANCE

Risk Management Framework Overview



The RMF provides a ***structured, yet flexible process*** for managing ***cybersecurity and privacy risk*** that includes system categorization, control selection, implementation, assessment, authorization, and continuous monitoring.

Risk Management Framework Steps



Essential activities to **prepare** the organization to manage security and privacy risks

Categorize the system and information processed, stored, and transmitted based on an impact analysis

Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

Implement the controls and document how controls are deployed

Assess to determine if the controls are in place, operating as intended, and producing the desired results

Senior official makes a risk-based decision to **authorize** the system (to operate)

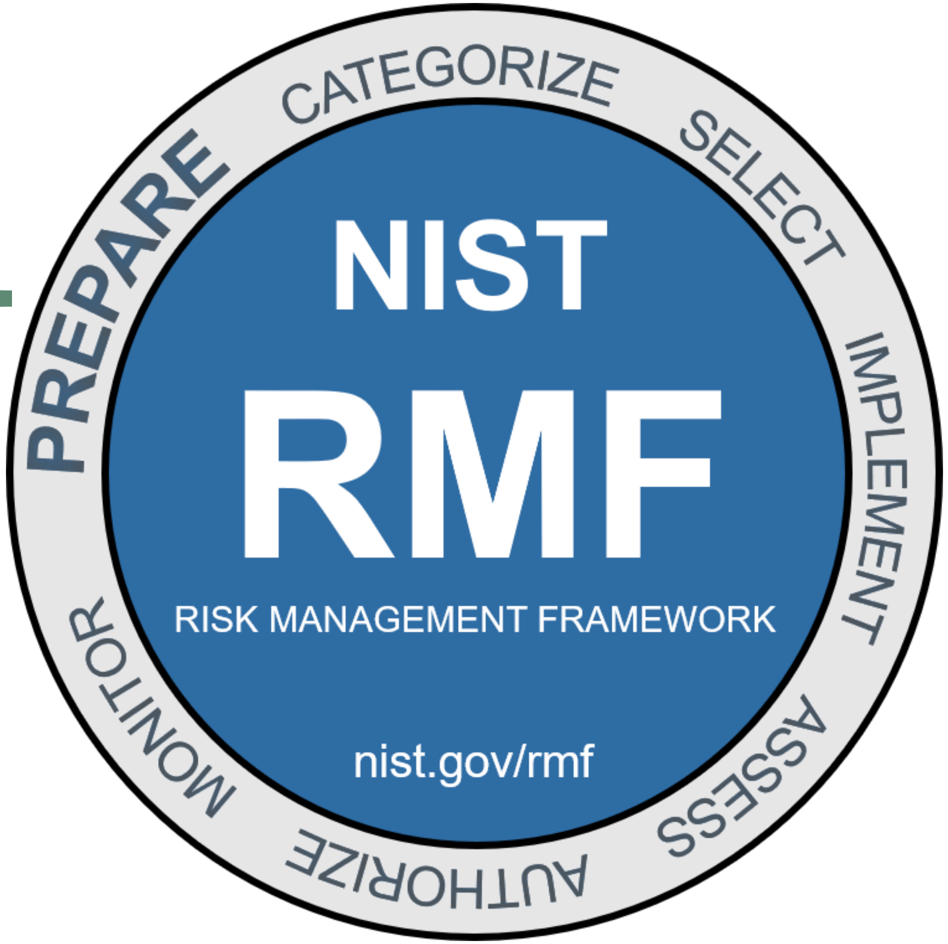
Continuously **monitor** control implementation and risks to the system

RMF Steps and Tasks: Considerations for Genomic Data

RMF Prepare Step

Genomic data is considered when developing/identifying the:

- Risk Management Strategy (Task P-2)
- Continuous Monitoring Strategy - Organization (Task P-7)
- Authorization Boundary (Task P-11)
- Information Types (Task P-12)
- Risk Assessment – System (Task P-14)
- Requirements Definition (Task P-15)



RMF Steps and Tasks: Considerations for Genomic Data

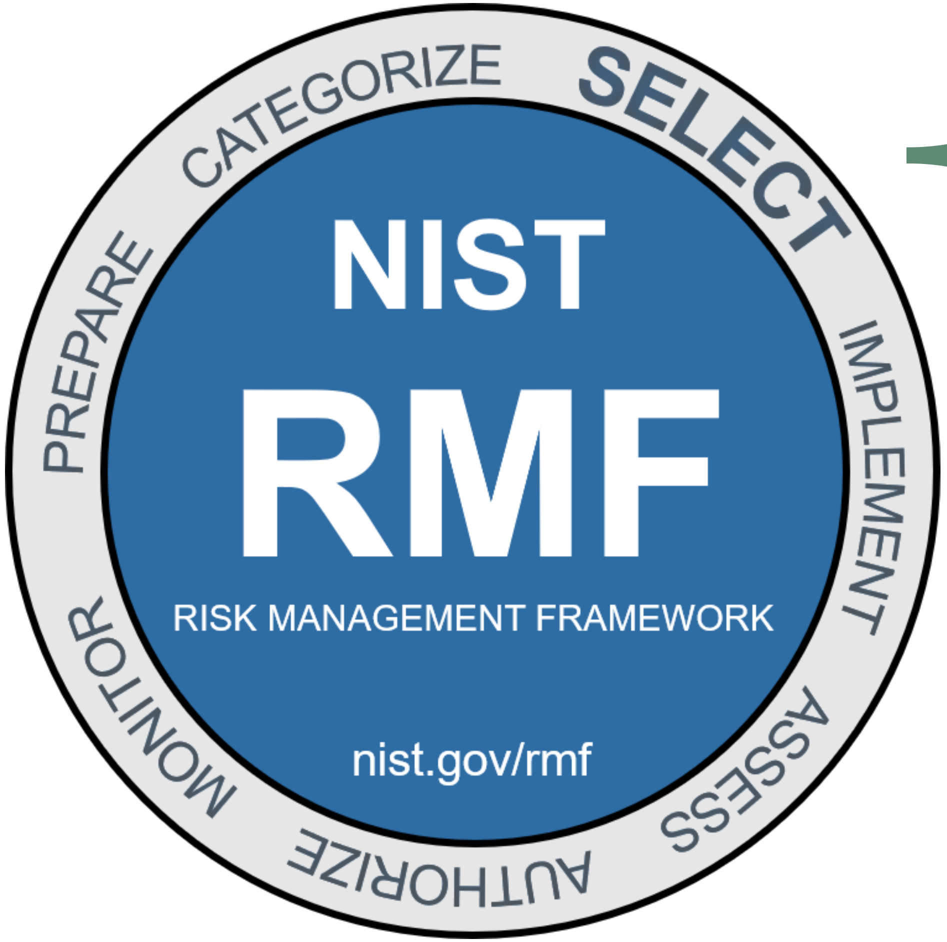
RMF Categorize Step

Genomic data is considered when developing the:

- Security Categorization (Task C-2)

CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
NIST
RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

RMF Steps and Tasks: Considerations for Genomic Data

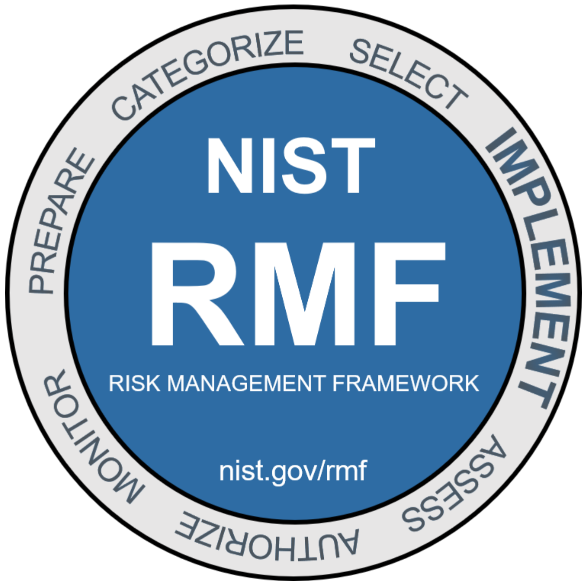


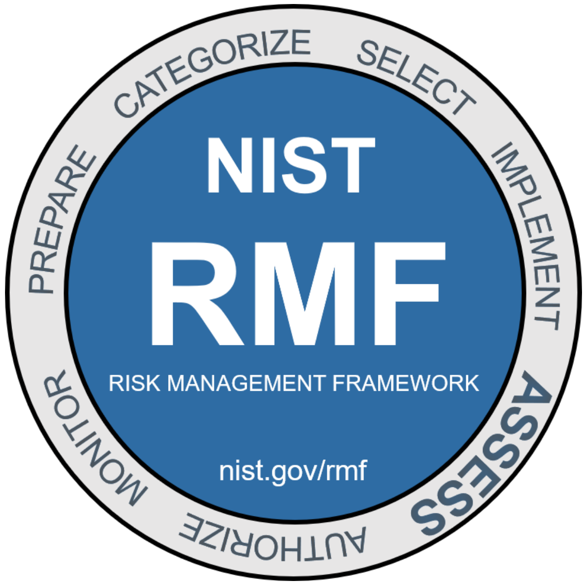
RMF Select Step

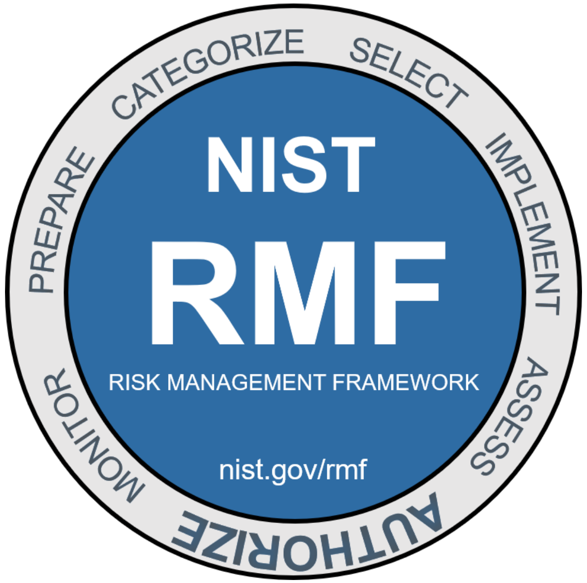
Genomic data is considered when developing/identifying the:

- Control Selection (Task S-1)
- Control Tailoring (Task S-2)
- Control Allocation (Task S-3)

RMF Steps and Tasks: Considerations for Genomic Data







RMF Steps and Tasks: Considerations for Genomic Data

RMF Monitor Step

Genomic data is considered during:

- System Disposal (Task M-7)

CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
PREPARE
NIST
RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

Additional Resources

Risk Management Framework

https://nist.gov/RMF

Program overview & links to additional resources, including ***Quick Start Guides***, **Roles & Responsibilities summary,** the Security Control Overlay Repository, and SP 800-53 Release Search

SP 800-37, Revision 2

https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

RMF for Information Systems and Organizations: A System Life Cycle Approach for Security & Privacy

RMF Online Course

https://csrc.nist.gov/Projects/risk-management/rmf-training

Free, 3 hour online introductory course on the RMF (SP 800-37, Revision 2) and LMS compatible formats

STAY IN TOUCH

CONTACT US

nist.gov/RMF

sec-cert@nist.gov

@NISTcyber

Academia Adventures in FedRAMP-land

(AKA no, no one has a diagram for that and there are no docs).

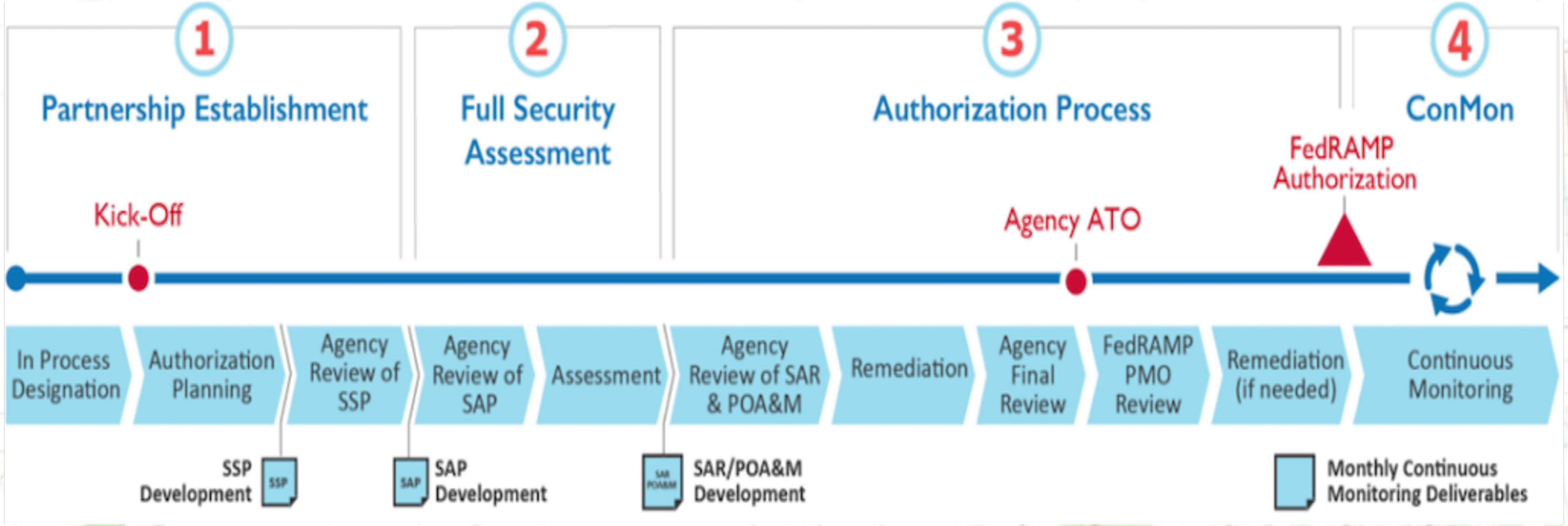
Frog put the cookies in a box. "There," he said. "Now we will not eat any more cookies."

"But we can open the box," said Toad.

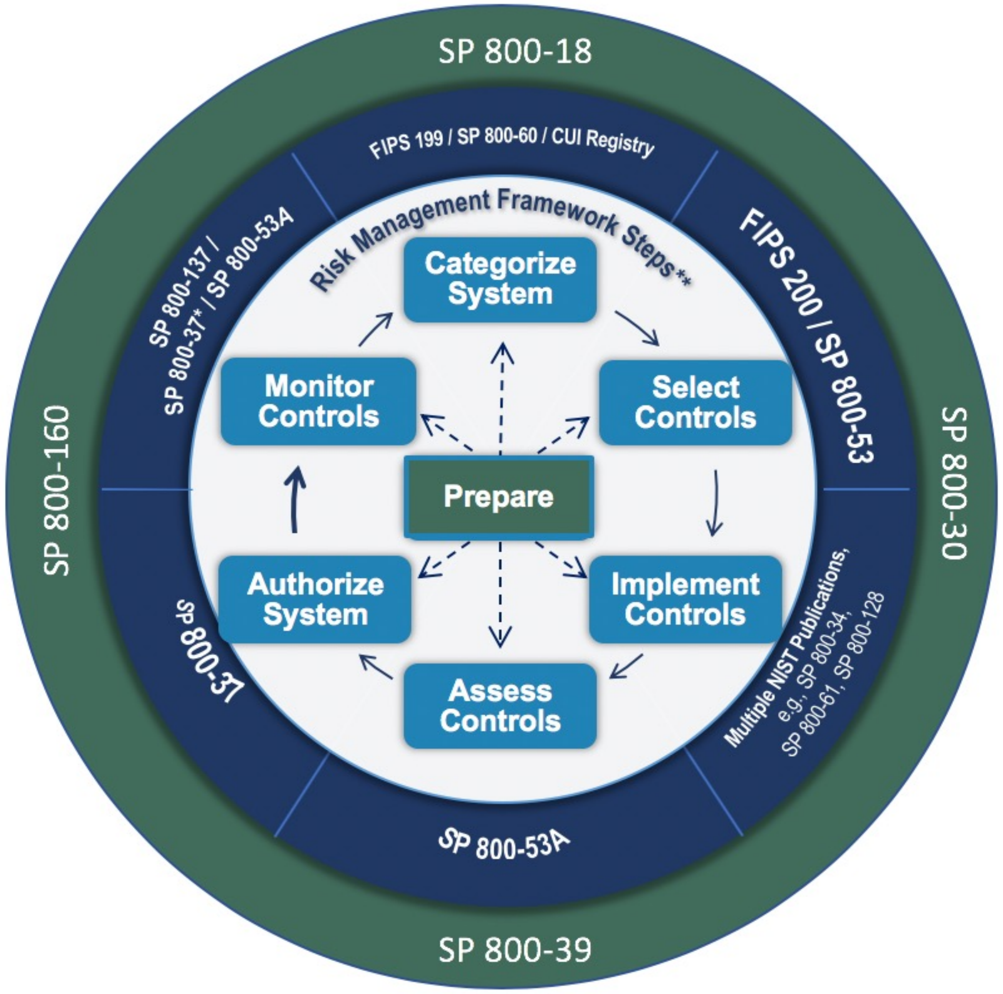
"That is true," said Frog.

David Bernick, Broad Institute
Chief Information Security Officer

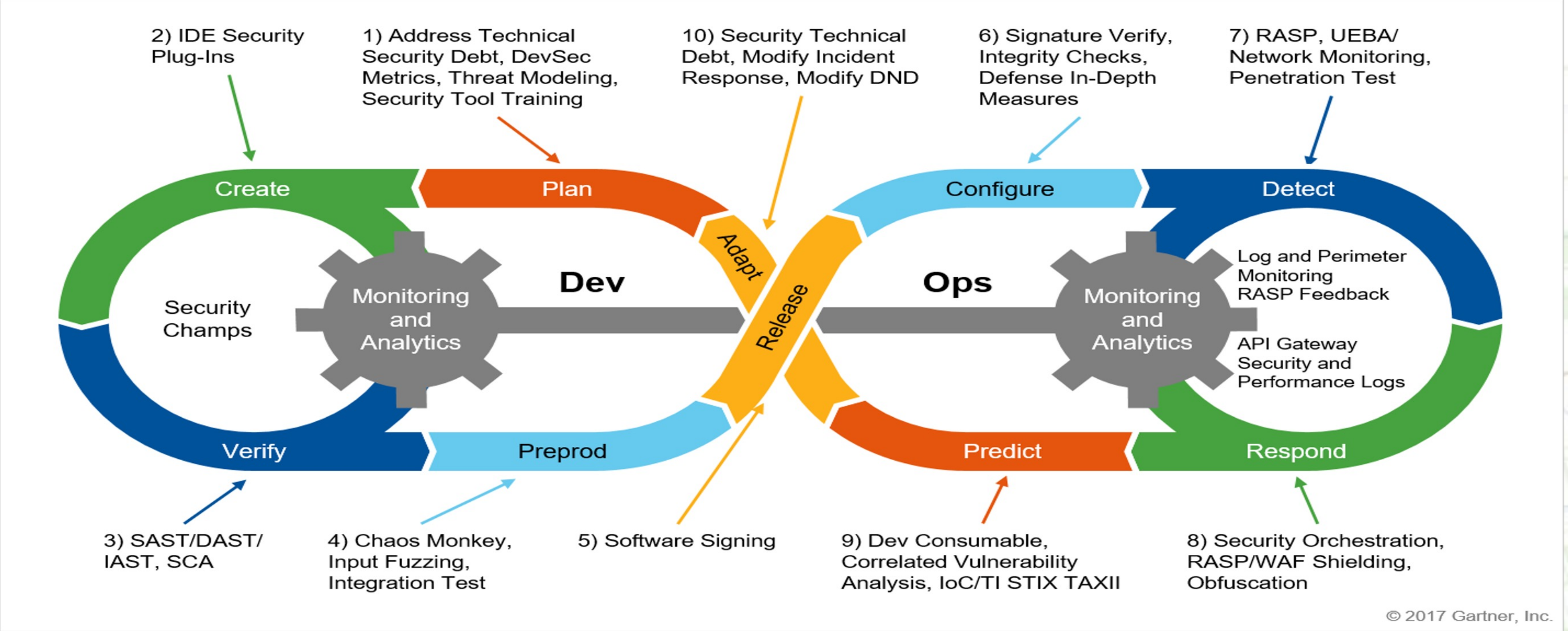
- Broad Institute concentrates on FedRAMP as a compliance.
    - It is highly prescriptive (NIST-800-53 r5 Moderate).
    - It is totally unforgiving and does not appreciate “hand wavy” explanations.
    - You get audited by auditors who in-turn are audited by GSA.



- We were already doing FISMA over and over for this same system.
    - FISMA also uses NIST-800-53 r5 Moderate and has the same auditors (in our case).
    - FedRAMP is about the System, FISMA is about the data. For us they were the same.



- What went great?
    - Culture!
        - Our compliance teams work closely with our Dev and Appsec and InfraSec teams.
        - Everyone knows this is important and product owners help allocate time. No “throw over the fence” culture.



2) IDE Security Plug-Ins
1) Address Technical Security Debt, DevSec Metrics, Threat Modeling, Security Tool Training
10) Security Technical Debt, Modify Incident Response, Modify DND
6) Signature Verify, Integrity Checks, Defense In-Depth Measures
7) RASP, UEBA/ Network Monitoring, Penetration Test
Create
Plan
Adapt
Configure
Detect
Security Champs
Monitoring and Analytics
Dev
Release
Ops
Monitoring and Analytics
Log and Perimeter Monitoring
RASP Feedback
API Gateway Security and Performance Logs
Verify
Preprod
Predict
Respond
3) SAST/DAST/ IAST, SCA
4) Chaos Monkey, Input Fuzzing, Integration Test
5) Software Signing
9) Dev Consumable, Correlated Vulnerability Analysis, IoC/TI STIX TAXII
8) Security Orchestration, RASP/WAF Shielding, Obfuscation
© 2017 Gartner, Inc.

- What wasn’t great?
  - Scanners are indisputable; If the scanner says it’s a HIGH, it’s a HIGH and you have 30 days to fix it.
    - That required us to clearly document EACH finding and EACH False Positive.
    - Couldn’t ignore things even if we KNEW they weren’t possibly exploitable.
    - We all know scanners aren’t that smart so it’s A LOT of extra stuff.
  - Change Management
    - If you’re letting devs release to prod without a security review of EACH change, you have to stop.
    - Most orgs with FedRAMP roll up changes for a weekly/bi-weekly release with security oversight.

Since this is a NIST talk, let's talk about NIST-800-53r4

The Good

- NIST-800-53 is a really good security framework.

The Bad

- Modern scanners don't know what to do with Dockers, but you're required to scan them.
    - Even stuff marketed at being Docker Scanners doesn't do great.
- Modern scanners don't know what to do with complex web-apps
    - But you have to scan anyhow and you'll never find anything meaningful.
- Annual Pentests are not meaningful in a modern, fast moving system.
    - Too complex for a 2 week engagement and they don't find anything.

The Ugly

- The Framework is more about traditional VM/Network/Web stacks and that doesn’t reflect a modern stack made up of various custom web-services (layer 7) and inherited cloud services that we don’t manage.
  - Example: Scanning OS of Dockers is a distraction as it’s nowhere near the security surface. But nothing about real Oauth security.
- Unprepared for an API-offering
  - A system that is primarily an API for use by users downstream means an ill-defined perimeter.
  - Scanning/protecting APIs is cutting-edge from vendors and not well vetted.

The Ugly

- Specifically for Life Sciences – Concepts like “timeouts” or “inactivity” are hard to define
  - Long running processes
  - Usually using refreshable tokens
  - What does it mean to “timeout” a user when the user’s running process lasts a week?
  - Auditors were unbending here and it took a lot of paperwork to accept a risk that is “normal” in our industry.

- Things we do beyond FedRAMP/NIST requirements
  - In-house red-teaming/SDLC enforcement/ongoing Pen-testing
  - IaaS security requirements – we adhere to CIS level 1 Benchmarks for GCP - most of framework is still very centric on VM/Networks
  - Internal Encryption – Cloud networks are viewable by the clouds themselves and EU collaborators don’t like that, so we encrypt everything
  - Threat Modeling as part of SDLC – ie security BEFORE code
  - Supply Chain Analysis of Library vulnerabilities

Devs get freaked out by size of -53

We reduce it to this:

Just do good security practices – And write them down.

- Authentication at every level of your stack – Infrastructure and app
- Authorization at every level – every access to data checks to see if the access is legitimate
- Encryption at every level
- Audit trails at every level – alerts and metrics that humans respond to
- Assess these things through testing

That’s it.

The trick is actually doing it. All the time. And not getting in the way of science.

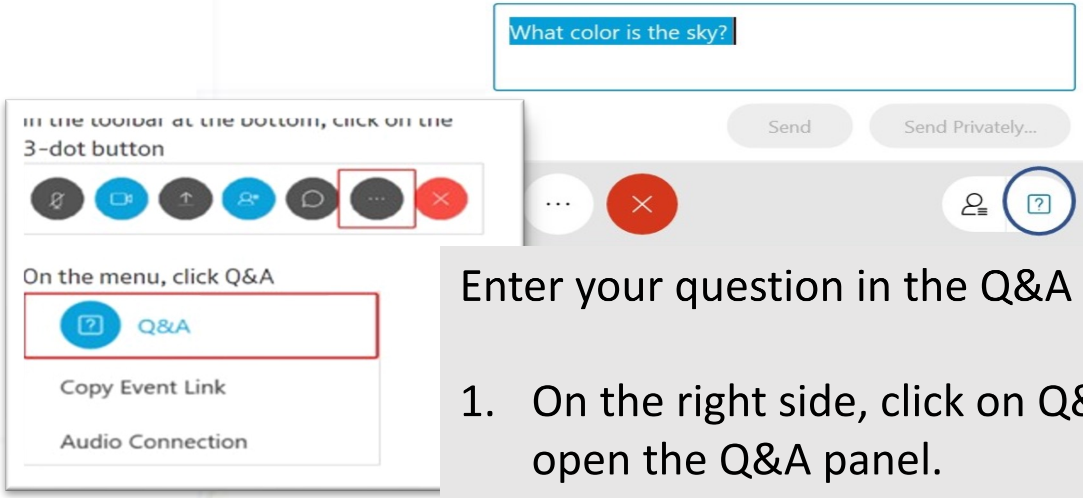
Questions?

WE'VE DOCUMENTED ALL OUR SECURITY PROCESSES.
AND YOUR TEAMS WILL FOLLOW THOSE PROCESSES?
YOUR TEAMS WILL FOLLOW THOSE PROCESSES?
imgflip.com

dbernick@broadinstitute.org

Genomic Data Security Through Risk Management

Moderated Questions and Answers



In the toolbar at the bottom, click on the 3-dot button

On the menu, click Q&A

Enter your question in the Q&A panel.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type in the box **your name, organization and question**.
3. Click send.

Break

Enjoy your break.
We’ll start again soon!

2:25 PM

Coming up next!

TOPIC	PRESENTERS
Session Four: Genomic Data Security in Electronic Health Records	Devin Absher (HudsonAlpha) Scott Newberry (HudsonAlpha) Abigail Watson (MITRE)

Welcome Back!

This meeting is being recorded.

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Genomic Data Security in Electronic Health Records

Devin Absher (HudsonAlpha)
Scott Newberry (HudsonAlpha)
Abigail Watson (MITRE)

Session Agenda and Speakers

The Integration of Genomic Data and Healthcare Outcomes

- **Role of Genomics in Healthcare Outcomes**
  - HudsonAlpha Institute for Biotechnology – Dr. Devin Absher, Faculty Investigator
- **Overview of FHIR**
  - HudsonAlpha Institute for Biotechnology – Scott Newberry, Director of Software Engineering
- **Securing Genetic Systems and Integrations**
  - MITRE – Abigail Watson, Principal FHIR Software Engineer

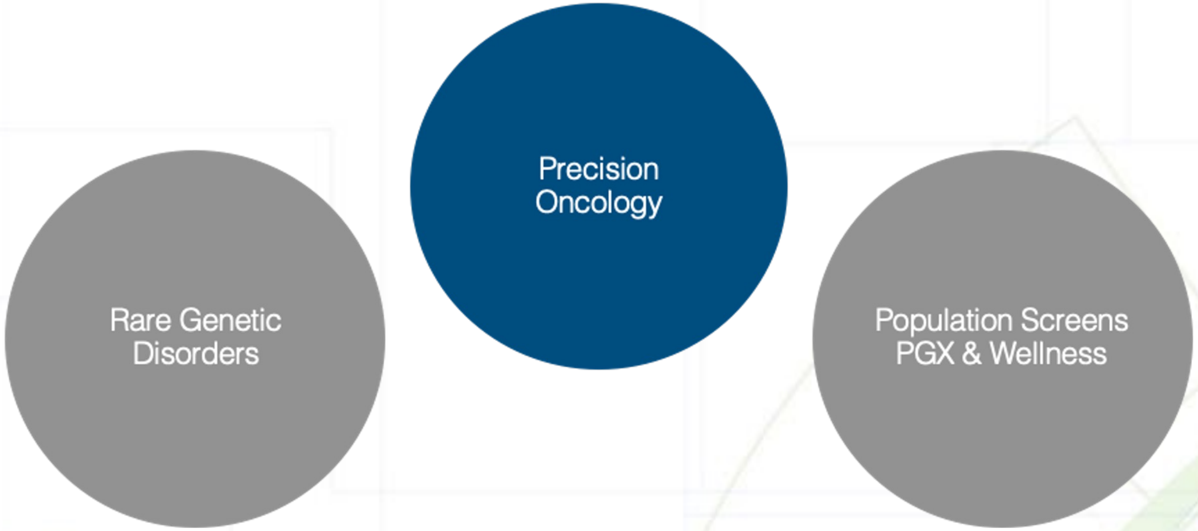
National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Dr. Devin Absher, HudsonAlpha

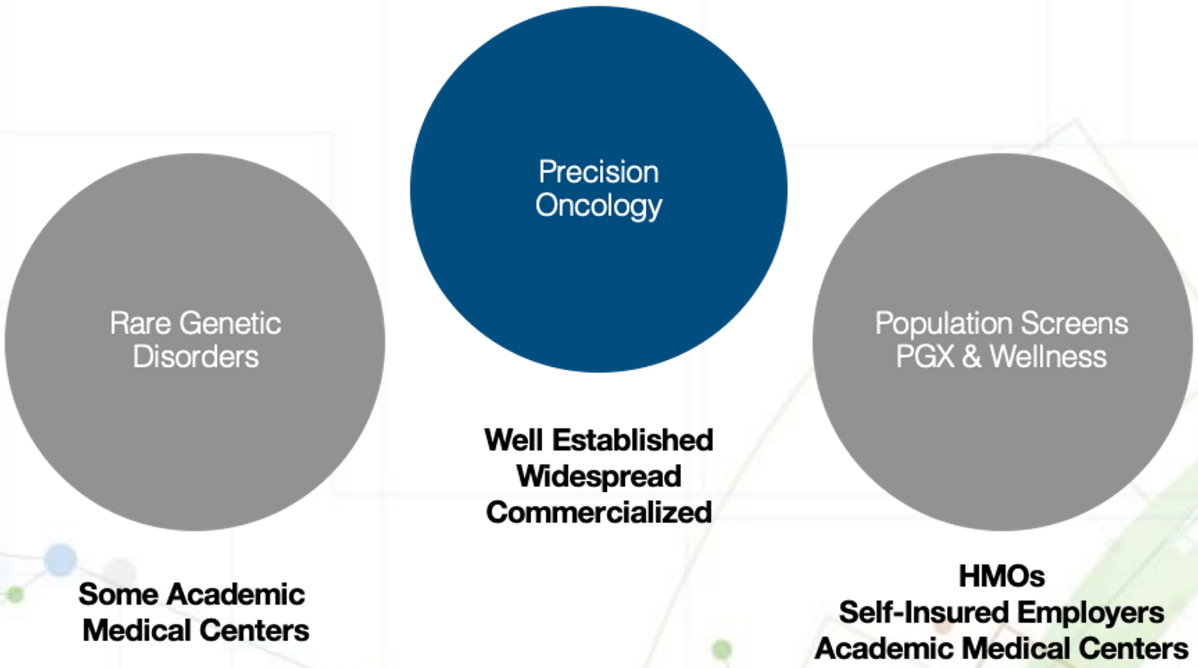
Role of Genomics in Healthcare Outcomes

Genomic Medicine Landscape



Role of Genomics in Healthcare Outcomes

Genomic Medicine Landscape



Precision Oncology

Well Established
Widespread
Commercialized

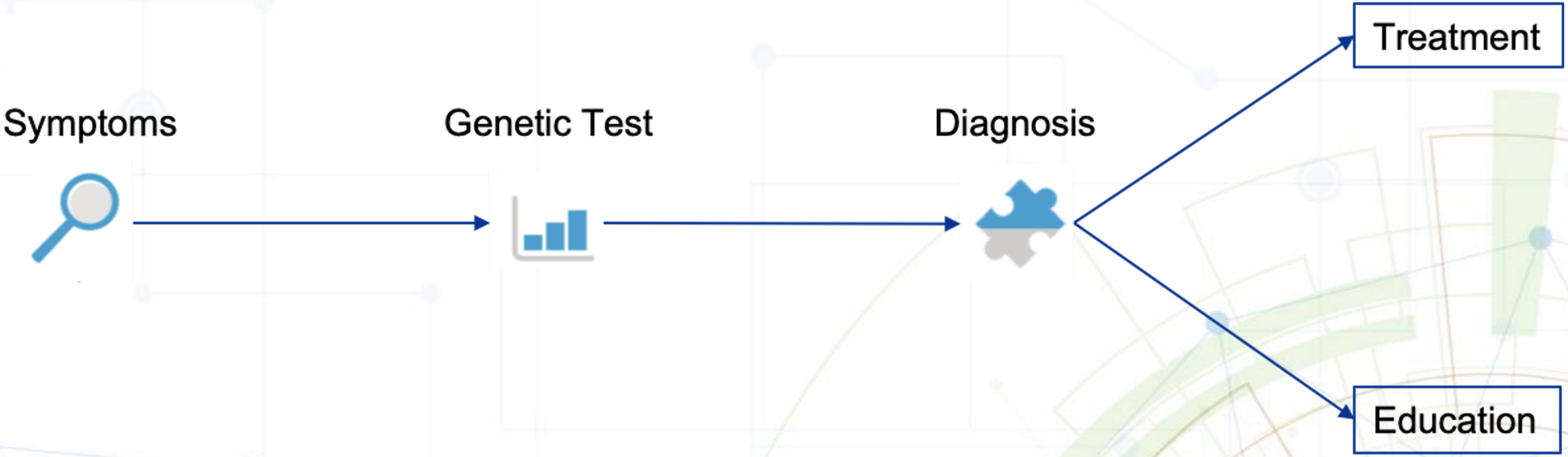
Rare Genetic Disorders

Some Academic
Medical Centers

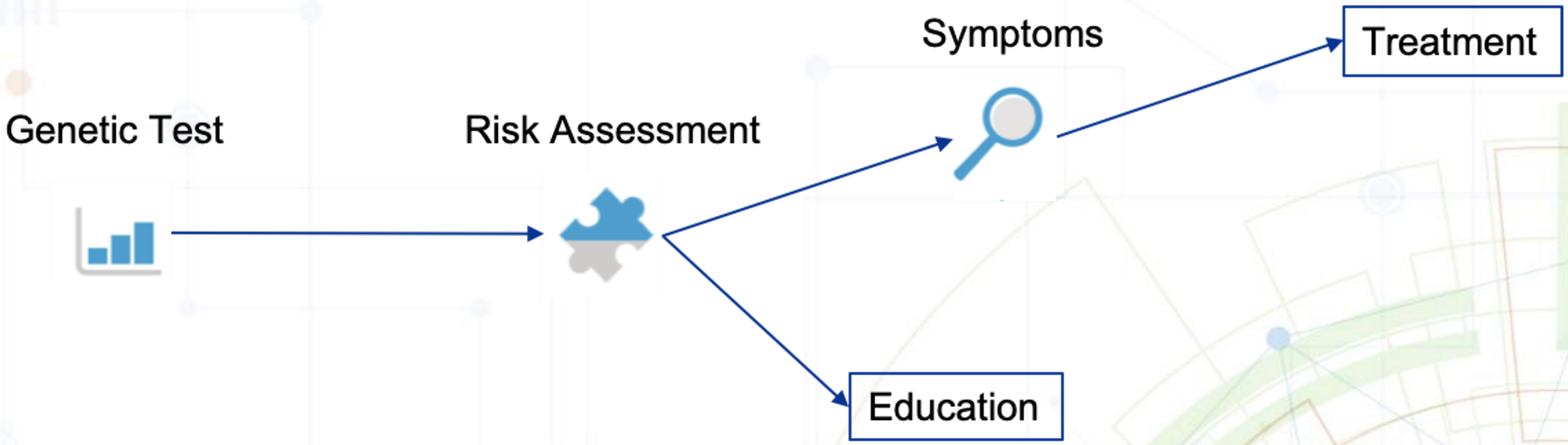
Population Screens
PGX & Wellness

HMOs
Self-Insured Employers
Academic Medical Centers

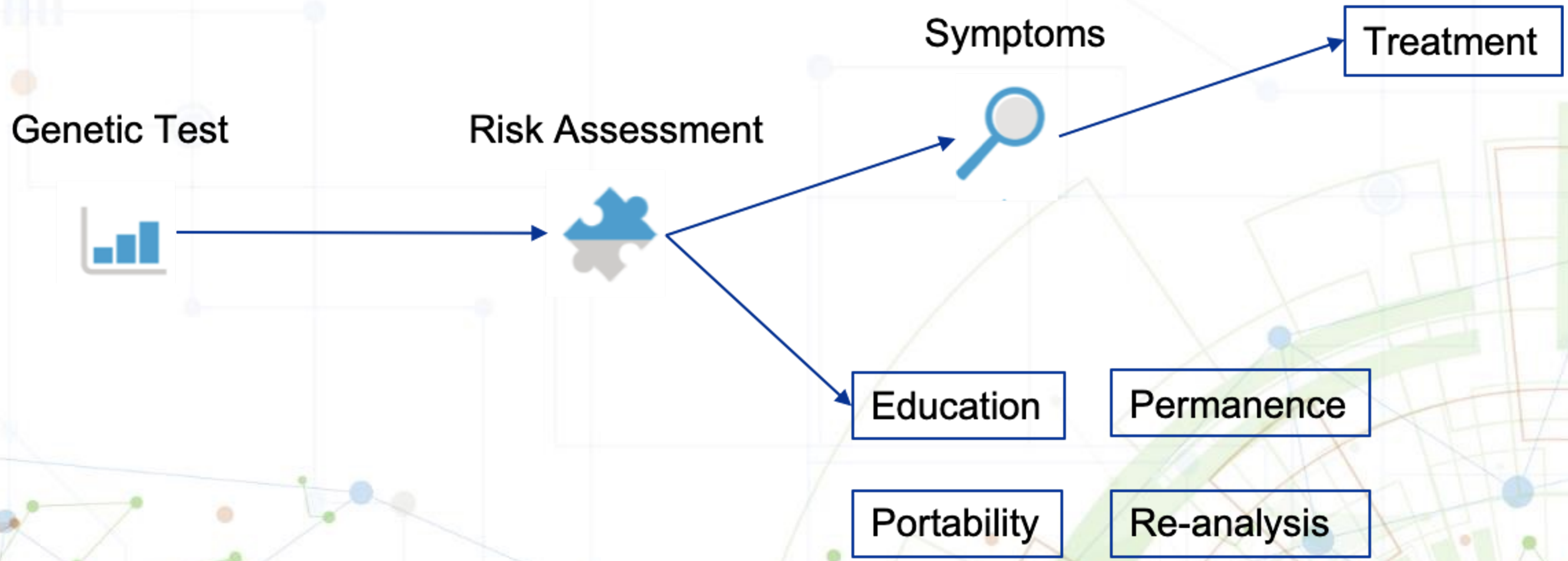
Role of Genomics in Healthcare Outcomes



Role of Genomics in Healthcare Outcomes



Role of Genomics in Healthcare Outcomes



Role of Genomics in Healthcare Outcomes

The Challenges

- Genomic data is large, complex, and can be medically relevant at any time in a patient’s lifespan
- Education and clinical decision support will be critical to successful implementation of precision medicine
- Portability, privacy, chain-of-custody, re-interpretation

National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

Scott Newberry, HudsonAlpha

FHIR Overview

HL7® FHIR®

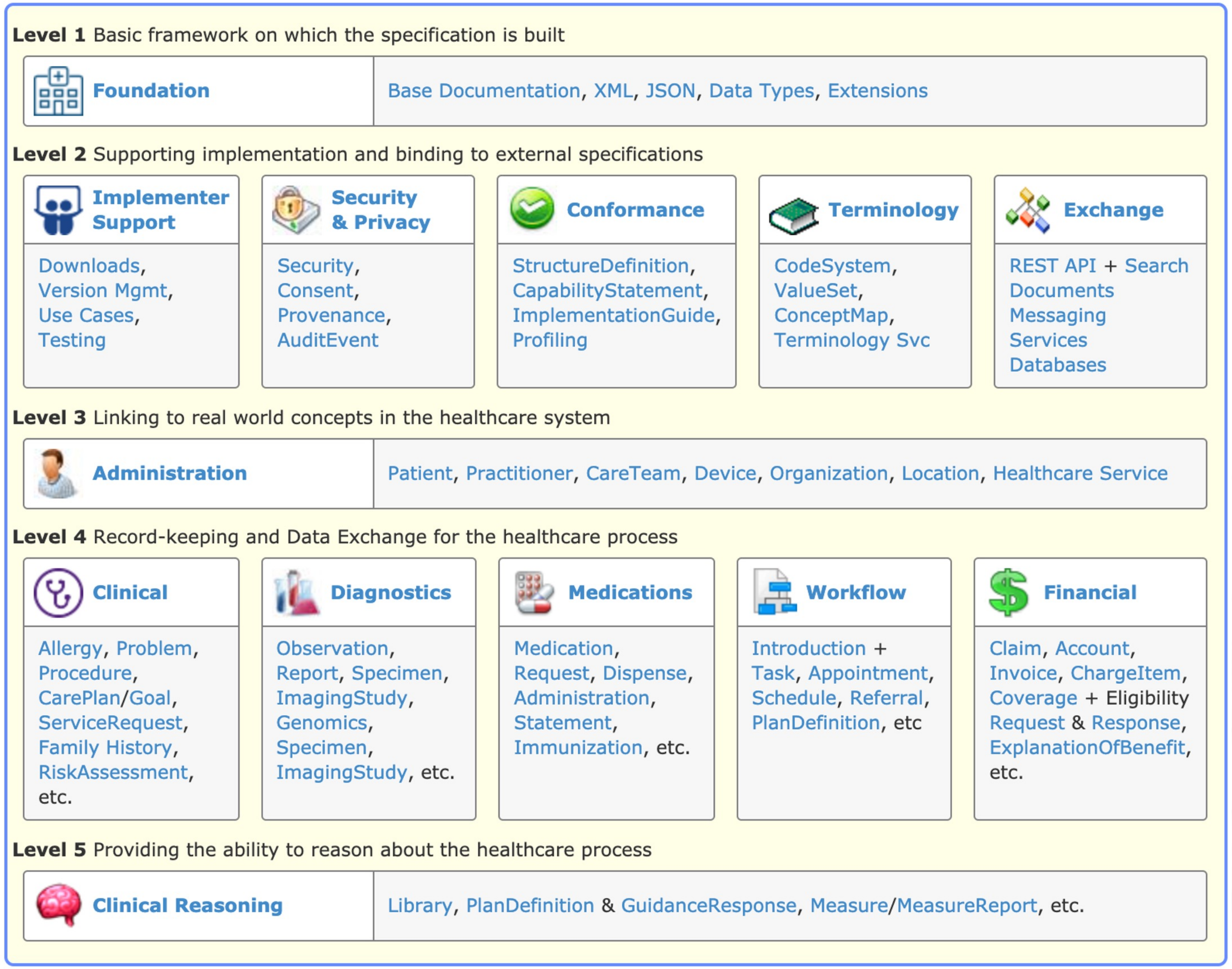
Fast Healthcare Interoperability Resources

Emerging standard across the healthcare industry

Specifies a data format and resources

Describes an API for programmatic exchange of health data

Supports nearly any healthcare use case - extensible where it doesn't



Level 1 Basic framework on which the specification is built

Foundation	Base Documentation, XML, JSON, Data Types, Extensions

Level 2 Supporting implementation and binding to external specifications

Implementer Support	**Security & Privacy**	**Conformance**	**Terminology**	**Exchange**
Downloads, Version Mgmt, Use Cases, Testing	Security, Consent, Provenance, AuditEvent	StructureDefinition, CapabilityStatement, ImplementationGuide, Profiling	CodeSystem, ValueSet, ConceptMap, Terminology Svc	REST API + Search Documents Messaging Services Databases

Level 3 Linking to real world concepts in the healthcare system

Administration	Patient, Practitioner, CareTeam, Device, Organization, Location, Healthcare Service

Level 4 Record-keeping and Data Exchange for the healthcare process

Clinical	**Diagnostics**	**Medications**	**Workflow**	**Financial**
Allergy, Problem, Procedure, CarePlan/Goal, ServiceRequest, Family History, RiskAssessment, etc.	Observation, Report, Specimen, ImagingStudy, Genomics, Specimen, ImagingStudy, etc.	Medication, Request, Dispense, Administration, Statement, Immunization, etc.	Introduction + Task, Appointment, Schedule, Referral, PlanDefinition, etc	Claim, Account, Invoice, ChargeItem, Coverage + Eligibility Request & Response, ExplanationOfBenefit, etc.

Level 5 Providing the ability to reason about the healthcare process

Clinical Reasoning	Library, PlanDefinition & GuidanceResponse, Measure/MeasureReport, etc.

FHIR Resources

DiagnosticReport - findings and interpretations of diagnostic tests

Observation - measurements made about a patient

MolecularSequence - a specific genetic sequence or variant

Consent - represents a patient’s choices regarding healthcare

Provenance - tracks info about the activity that created/destroyed/modified a resource

Observation

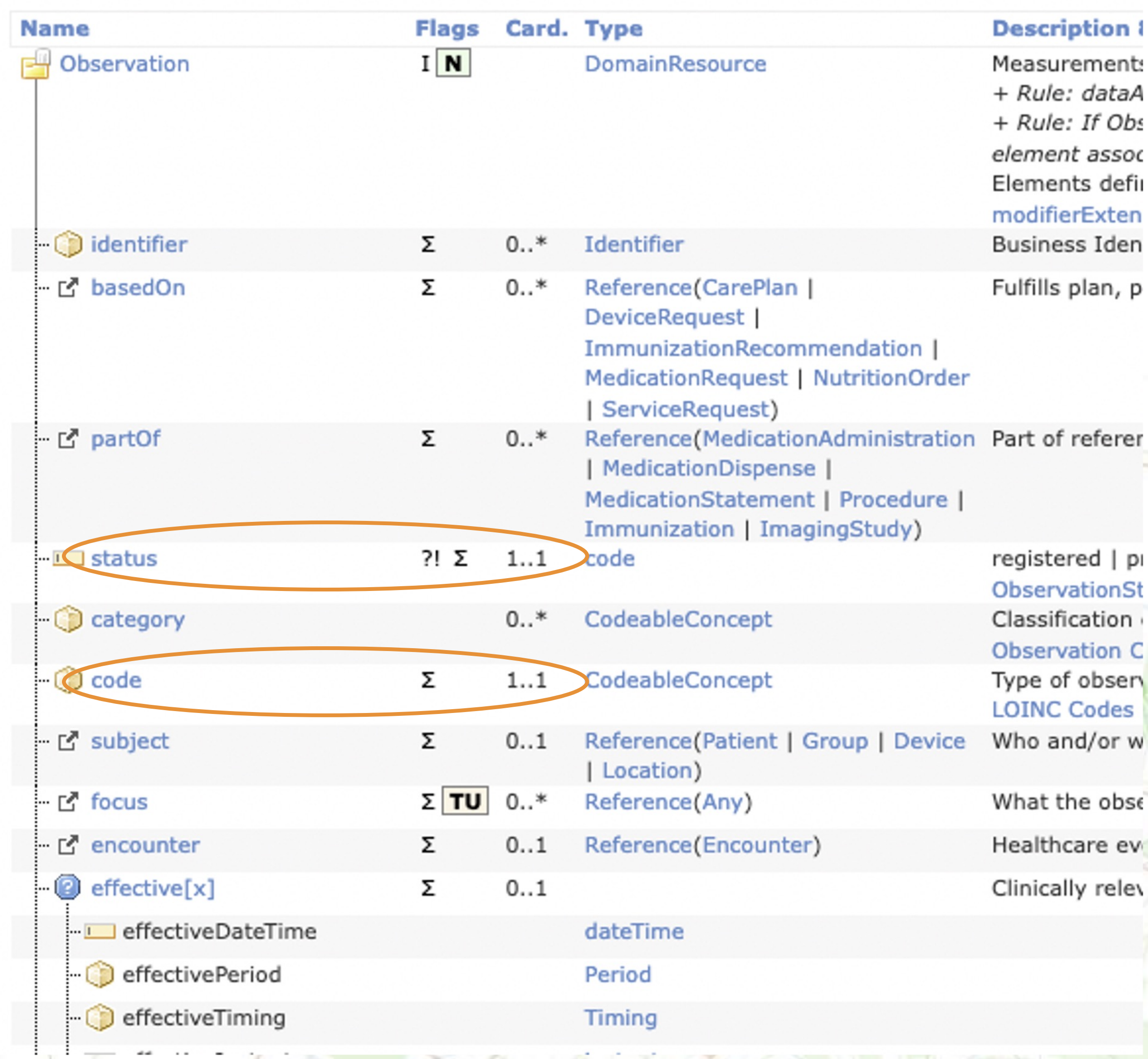
Required fields circled in orange

Most of the fields in the resource are optional

Most resources are broadly defined

Implementers can decide specifics regarding each resource they support

https://www.hl7.org/fhir/observation.html



Name	Flags	Card.	Type	Description
Observation	I N		DomainResource	Measurements + Rule: dataA + Rule: If Obs element assoc Elements defi modifierExten
identifier	Σ	0..*	Identifier	Business Iden
basedOn	Σ	0..*	Reference(CarePlan | DeviceRequest | ImmunizationRecommendation | MedicationRequest | NutritionOrder | ServiceRequest)	Fulfills plan, p
partOf	Σ	0..*	Reference(MedicationAdministration | MedicationDispense | MedicationStatement | Procedure | Immunization | ImagingStudy)	Part of referer
status	?! Σ	1..1	code	registered | p ObservationSt
category		0..*	CodeableConcept	Classification Observation C
code	Σ	1..1	CodeableConcept	Type of obser LOINC Codes
subject	Σ	0..1	Reference(Patient | Group | Device | Location)	Who and/or w
focus	Σ TU	0..*	Reference(Any)	What the obse
encounter	Σ	0..1	Reference(Encounter)	Healthcare ev
effective[x]	Σ	0..1		Clinically relev
effectiveDateTime			dateTime	
effectivePeriod			Period	
effectiveTiming			Timing	

FHIR Profiles

A set of specifications that describe the details about a given FHIR solution

Indicate which FHIR resources and API features are in use

Constrain and extend both APIs and resources

Allow for creation of new resources, if needed

Provide a common description language for consumers of your FHIR data

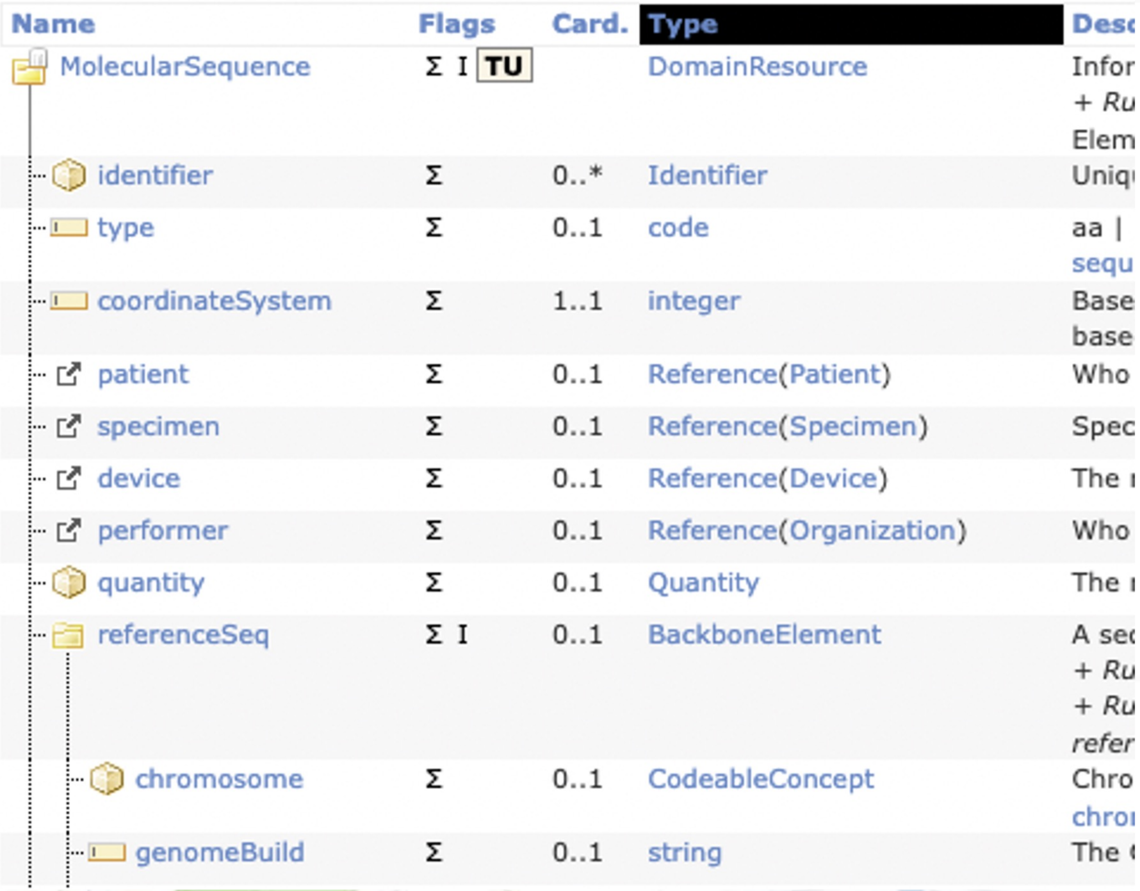
Genomics FHIR Profile and Implementation Guide

Extensions of FHIR to specifically address the genomics use case

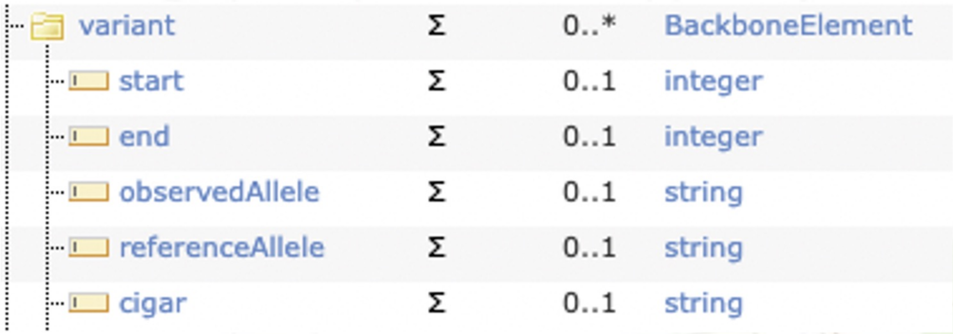
A new resource, MolecularSequence, to describe variants

Extensions of others to provide context and data related to next generation sequencing results

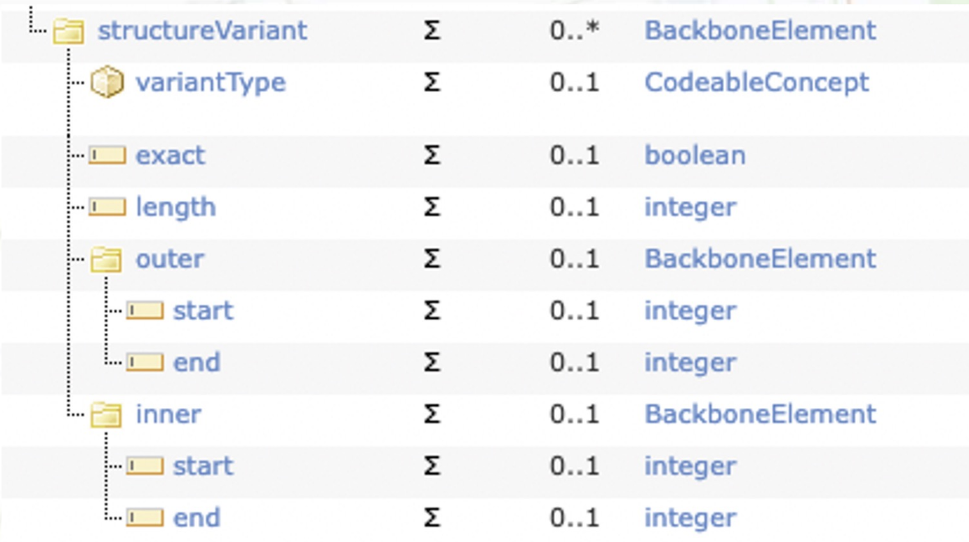
MolecularSequence Resource



Name	Flags	Card.	Type	Desc
MolecularSequence	Σ I TU		DomainResource	Infor + Ru Elem
identifier	Σ	0..*	Identifier	Uniq
type	Σ	0..1	code	aa | sequ
coordinateSystem	Σ	1..1	integer	Base base
patient	Σ	0..1	Reference(Patient)	Who
specimen	Σ	0..1	Reference(Specimen)	Spec
device	Σ	0..1	Reference(Device)	The
performer	Σ	0..1	Reference(Organization)	Who
quantity	Σ	0..1	Quantity	The
referenceSeq	Σ I	0..1	BackboneElement	A sec + Ru + Ru refer
chromosome	Σ	0..1	CodeableConcept	Chro chro
genomeBuild	Σ	0..1	string	The

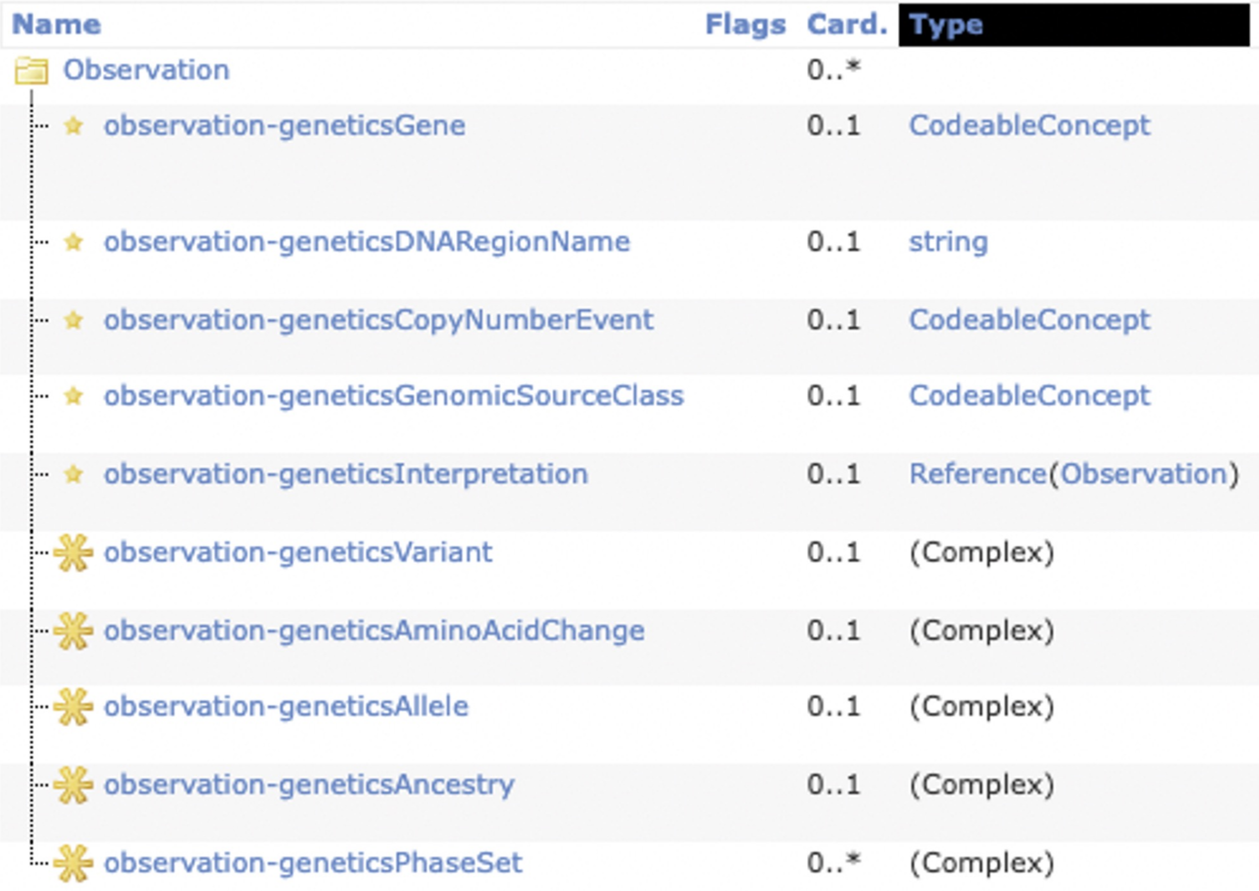


variant	Σ	0..*	BackboneElement
start	Σ	0..1	integer
end	Σ	0..1	integer
observedAllele	Σ	0..1	string
referenceAllele	Σ	0..1	string
cigar	Σ	0..1	string



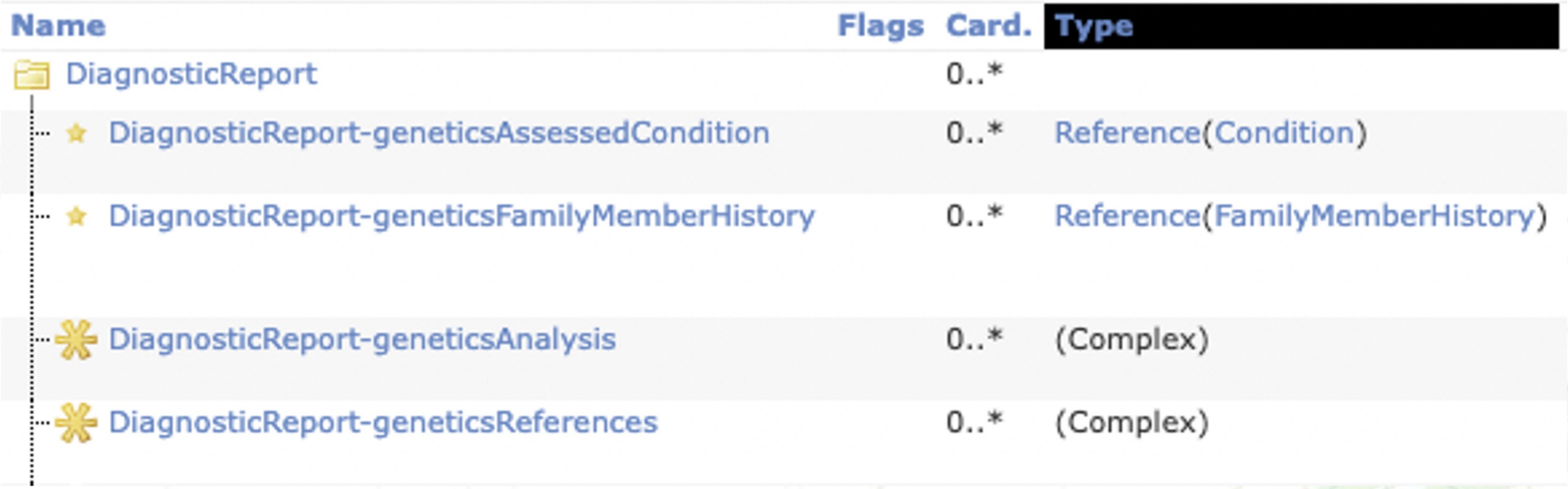
structureVariant	Σ	0..*	BackboneElement
variantType	Σ	0..1	CodeableConcept
exact	Σ	0..1	boolean
length	Σ	0..1	integer
outer	Σ	0..1	BackboneElement
start	Σ	0..1	integer
end	Σ	0..1	integer
inner	Σ	0..1	BackboneElement
start	Σ	0..1	integer
end	Σ	0..1	integer

Observation-genetics



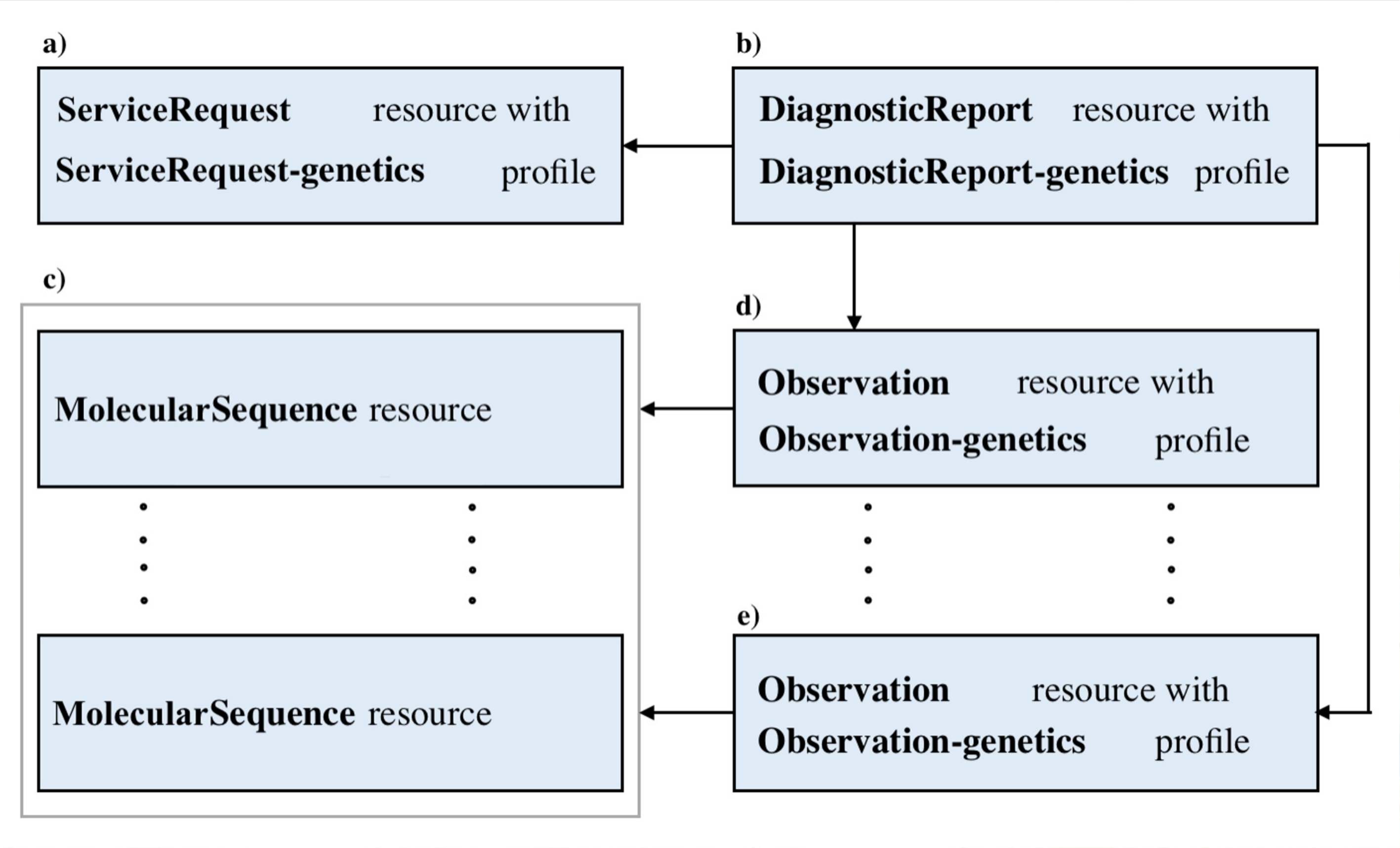
Name	Flags	Card.	Type
Observation		0..*	
observation-geneticsGene		0..1	CodeableConcept
observation-geneticsDNARegionName		0..1	string
observation-geneticsCopyNumberEvent		0..1	CodeableConcept
observation-geneticsGenomicSourceClass		0..1	CodeableConcept
observation-geneticsInterpretation		0..1	Reference(Observation)
observation-geneticsVariant		0..1	(Complex)
observation-geneticsAminoAcidChange		0..1	(Complex)
observation-geneticsAllele		0..1	(Complex)
observation-geneticsAncestry		0..1	(Complex)
observation-geneticsPhaseSet		0..*	(Complex)

DiagnosticReport-genetics



Name	Flags	Card.	Type
DiagnosticReport		0..*	
DiagnosticReport-geneticsAssessedCondition		0..*	Reference(Condition)
DiagnosticReport-geneticsFamilyMemberHistory		0..*	Reference(FamilyMemberHistory)
DiagnosticReport-geneticsAnalysis		0..*	(Complex)
DiagnosticReport-geneticsReferences		0..*	(Complex)

Tying it all together



a)
ServiceRequest resource with ServiceRequest-genetics profile
b)
DiagnosticReport resource with DiagnosticReport-genetics profile
c)
MolecularSequence resource
MolecularSequence resource
d)
Observation resource with Observation-genetics profile
e)
Observation resource with Observation-genetics profile

What about the “big” genomic data?

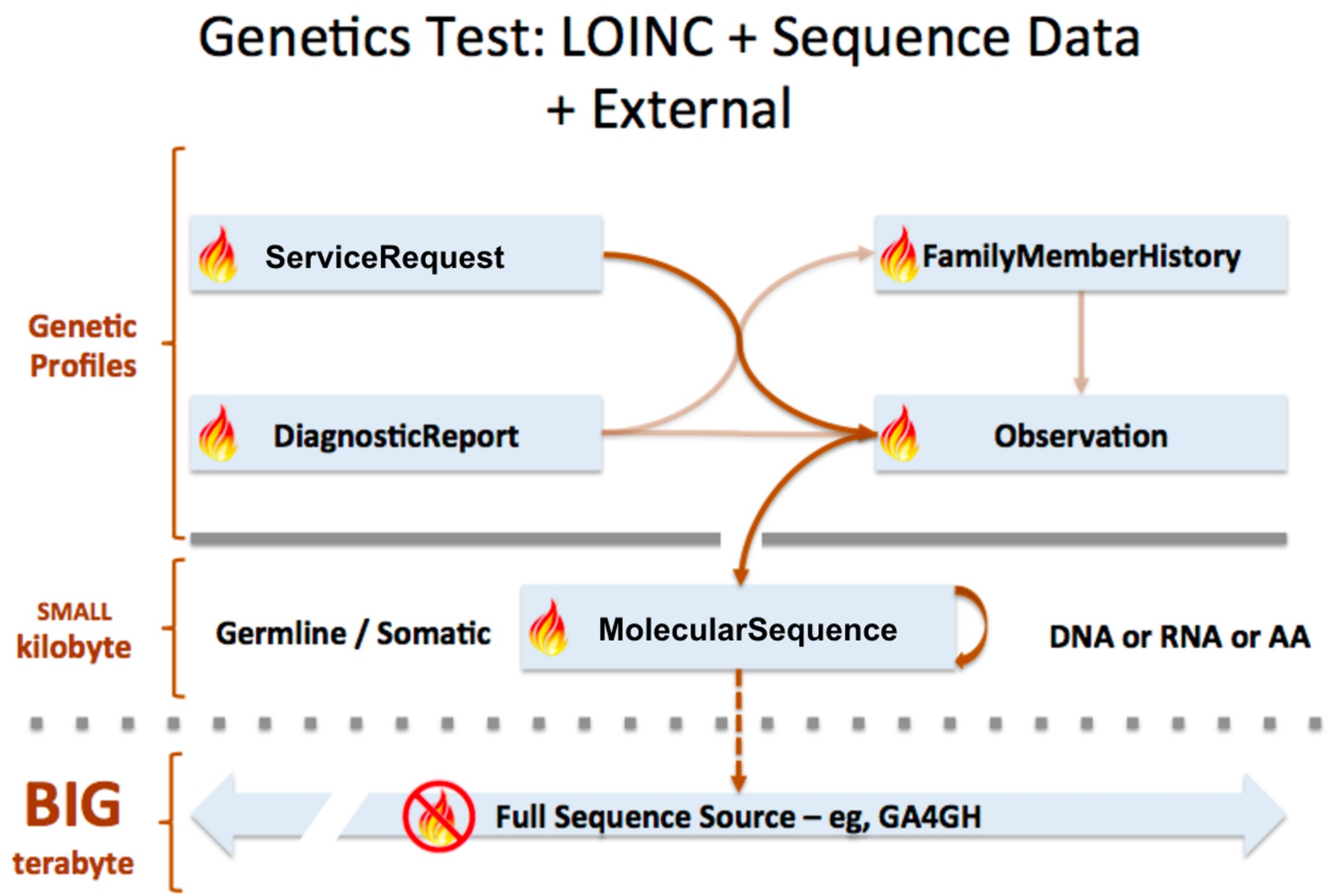
Genomics FHIR Profile mainly focuses on reported variants

Usually these are small in number and clinically actionable

MolecularSequence is not intended to store ALL variants

VCF & BAM files contain data that could be relevant in the future

“Big” data is available externally



Genetics Test: LOINC + Sequence Data + External

Genetic Profiles

ServiceRequest

FamilyMemberHistory

DiagnosticReport

Observation

SMALL kilobyte

Germline / Somatic

MolecularSequence

DNA or RNA or AA

BIG terabyte

Full Sequence Source – eg, GA4GH

Review

FHIR is an API/data standard for healthcare data

It is a foundational set of resources

Extensible for any healthcare use case via profiles

Genomics profile is a good starting point for actionable variant data

Integrating “big” genomic data into health records is the next step

Securing Genetic Systems and Integrations

SMART on FHIR

- OAuth2
- OpenID

UDAP Trust Framework (FAST)

- HTTPS
- SSL Certificates (X.509)

File system security

- GPG + UDAP/X.509
- Zip Compression

Radiology PACS Systems

- Large Files (Blob Security)
- DICOM App Entitites (AE Titles)
- Folder container format
- Pre-fetching subscription rules

FHIR Provenance

X-Header
Bundles

Advance Care Directives

FHIR Consent

HL7® FHIR®

National Cybersecurity Center of Excellence

NCCoE Virtual Workshop on Exploring Solutions for the Cybersecurity of Genomic Data

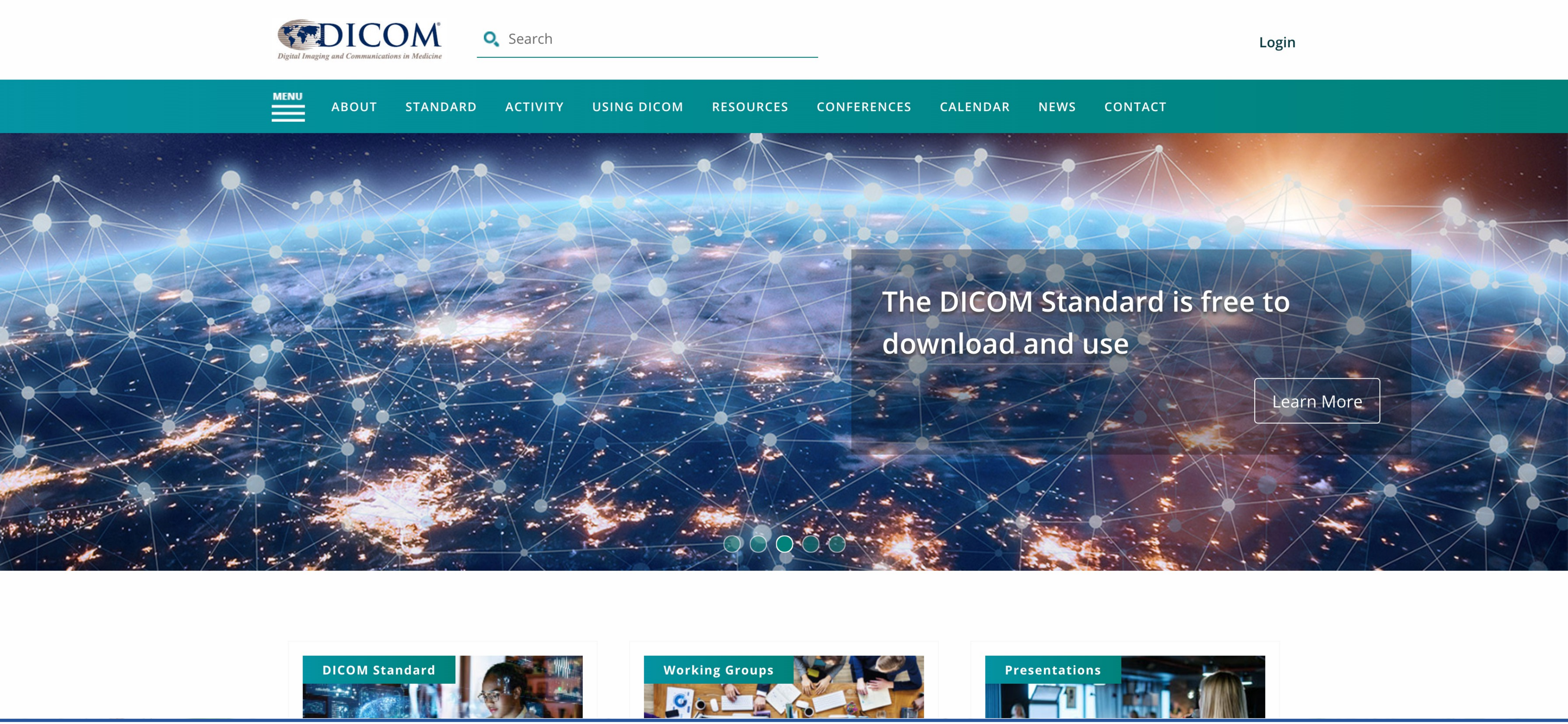
Abigail Watson
MS Biomedical Informatics
Principal FHIR Software Engineer
Open Health Services, MITRE

Radiology PACS Systems	https://www.dicomstandard.org/using/security/
- DICOM Standard	https://www.dicomstandard.org/
- DICOM App Entitites (AE Titles)	https://dicom.nema.org/dicom/2013/output/chtml/part07/sect_6.2.html
- Folder containers (DICOMDIR)	https://dicom.nema.org/medical/Dicom/2016b/output/chtml/part03/sect_F.2.2.2.html
- Pre-fetching subscription rules	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/prefetch-src
Fast Healthcare Interoperability Resources	https://hl7.org/fhir/
- Security Checklist	https://www.hl7.org/fhir/safety.html
SMART on FHIR	
- OAuth2	https://oauth.net/2/
- OpenID	https://openid.net/what-is-openid/
Provenance & Data Lineage	
- X-Header	https://www.hl7.org/fhir/provenance.html
- Bundle	https://www.hl7.org/fhir/bundle.html
Advance Care Directives	
- FHIR Consent	https://www.hl7.org/fhir/consent.html
- FHIR at Scale Taksforce (FAST)	https://oncprojecttracking.healthit.gov/wiki/pages/viewpage.action?pageId=43614268
- HTTPS	https://www.ssl.com/faqs/what-is-https/
- SSL Certificates (X.509)	https://www.ssl.com/faqs/what-is-an-x-509-certificate/
- UDAP Trust Framework (FAST)	https://www.udap.org/
File system security	
- PGP/GPG	https://www.privex.io/articles/what-is-gpg
- GPG + UDAP/X.509	https://stackoverflow.com/questions/41904252/how-to-convert-x509-certificate-and-private-key-in-pem-format-to-gpg-format

Q1: How do we secure genomics data?

Observation: Genomics files are large.

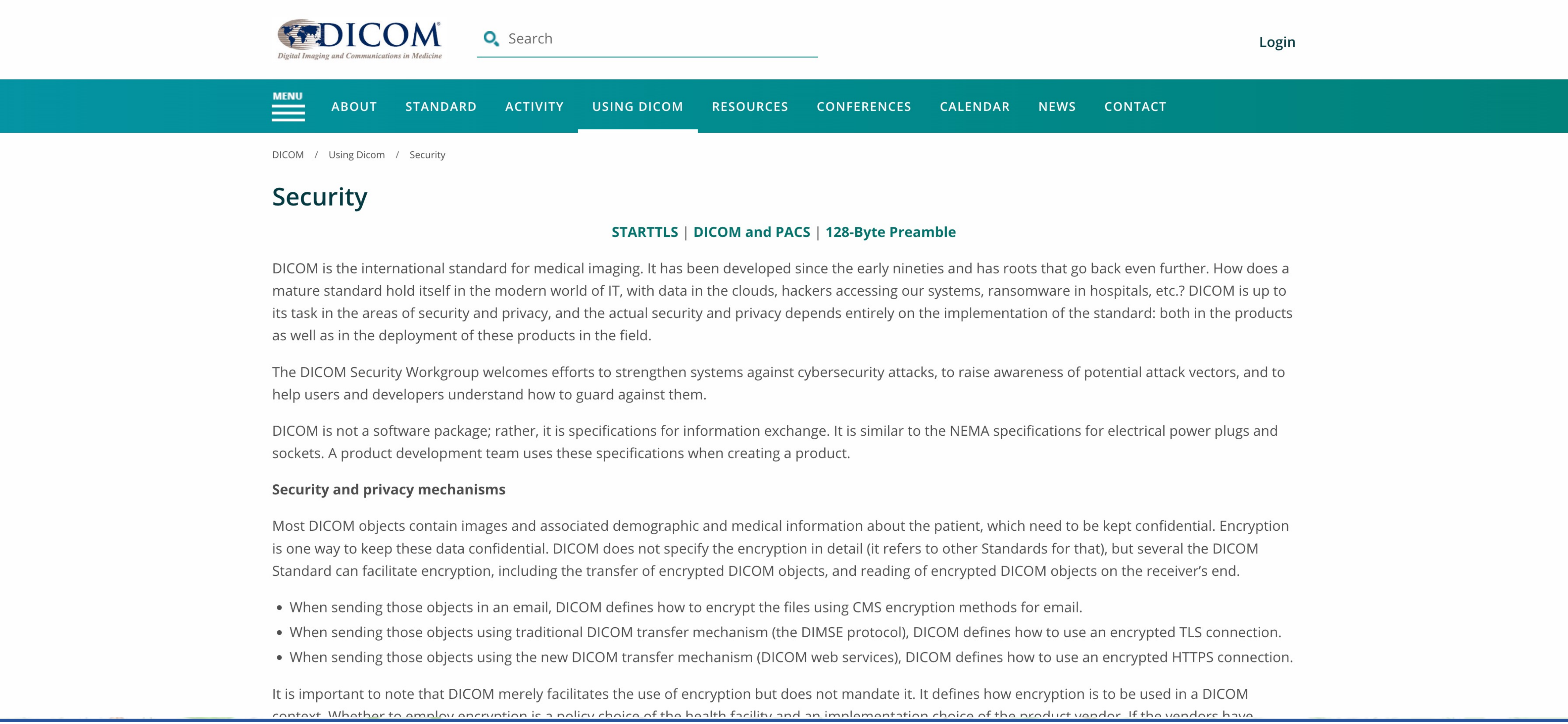
Q2: So… how do we currently secure large files?



The DICOM Standard is free to download and use

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



Security

STARTTLS | **DICOM and PACS** | **128-Byte Preamble**

DICOM is the international standard for medical imaging. It has been developed since the early nineties and has roots that go back even further. How does a mature standard hold itself in the modern world of IT, with data in the clouds, hackers accessing our systems, ransomware in hospitals, etc.? DICOM is up to its task in the areas of security and privacy, and the actual security and privacy depends entirely on the implementation of the standard: both in the products as well as in the deployment of these products in the field.

The DICOM Security Workgroup welcomes efforts to strengthen systems against cybersecurity attacks, to raise awareness of potential attack vectors, and to help users and developers understand how to guard against them.

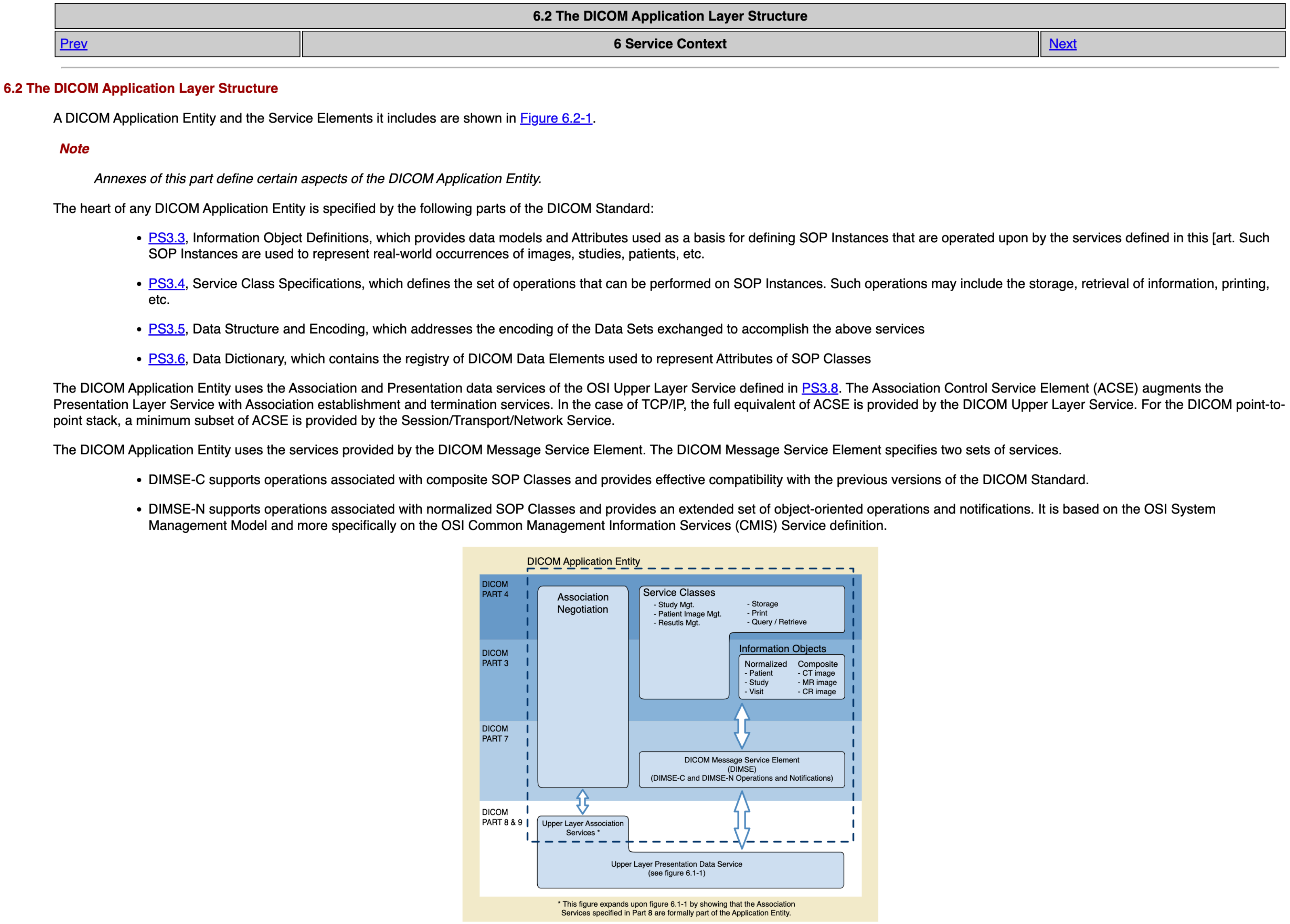
DICOM is not a software package; rather, it is specifications for information exchange. It is similar to the NEMA specifications for electrical power plugs and sockets. A product development team uses these specifications when creating a product.

Security and privacy mechanisms

Most DICOM objects contain images and associated demographic and medical information about the patient, which need to be kept confidential. Encryption is one way to keep these data confidential. DICOM does not specify the encryption in detail (it refers to other Standards for that), but several the DICOM Standard can facilitate encryption, including the transfer of encrypted DICOM objects, and reading of encrypted DICOM objects on the receiver's end.

- When sending those objects in an email, DICOM defines how to encrypt the files using CMS encryption methods for email.
- When sending those objects using traditional DICOM transfer mechanism (the DIMSE protocol), DICOM defines how to use an encrypted TLS connection.
- When sending those objects using the new DICOM transfer mechanism (DICOM web services), DICOM defines how to use an encrypted HTTPS connection.

It is important to note that DICOM merely facilitates the use of encryption but does not mandate it. It defines how encryption is to be used in a DICOM context. Whether to employ encryption is a policy choice of the health facility and an implementation choice of the product vendor. If the vendors have



6.2 The DICOM Application Layer Structure		
Prev	6 Service Context	Next

6.2 The DICOM Application Layer Structure

A DICOM Application Entity and the Service Elements it includes are shown in Figure 6.2-1.

Note

Annexes of this part define certain aspects of the DICOM Application Entity.

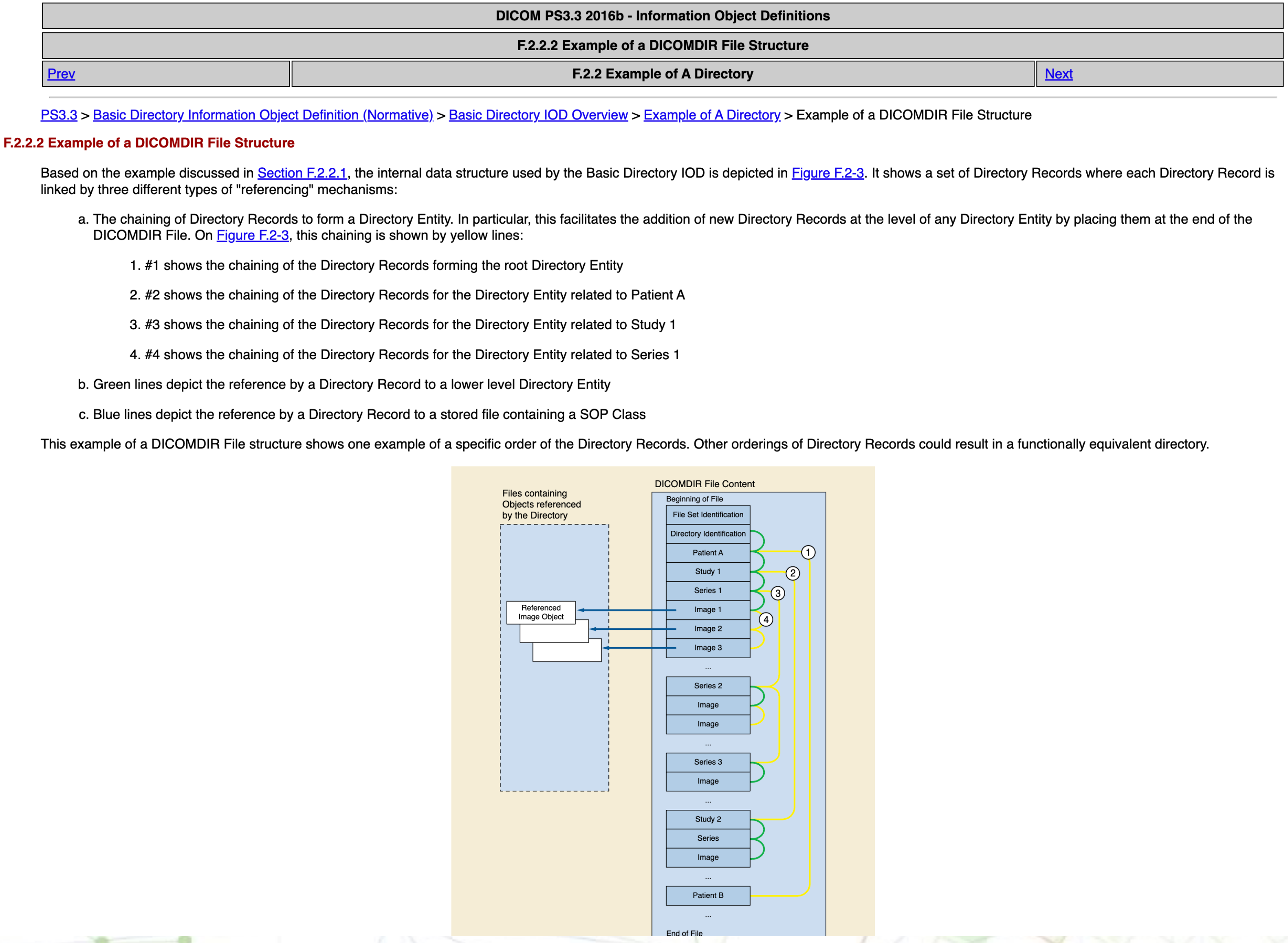
The heart of any DICOM Application Entity is specified by the following parts of the DICOM Standard:

- PS3.3, Information Object Definitions, which provides data models and Attributes used as a basis for defining SOP Instances that are operated upon by the services defined in this [art. Such SOP Instances are used to represent real-world occurrences of images, studies, patients, etc.
- PS3.4, Service Class Specifications, which defines the set of operations that can be performed on SOP Instances. Such operations may include the storage, retrieval of information, printing, etc.
- PS3.5, Data Structure and Encoding, which addresses the encoding of the Data Sets exchanged to accomplish the above services
- PS3.6, Data Dictionary, which contains the registry of DICOM Data Elements used to represent Attributes of SOP Classes

The DICOM Application Entity uses the Association and Presentation data services of the OSI Upper Layer Service defined in PS3.8. The Association Control Service Element (ACSE) augments the Presentation Layer Service with Association establishment and termination services. In the case of TCP/IP, the full equivalent of ACSE is provided by the DICOM Upper Layer Service. For the DICOM point-to-point stack, a minimum subset of ACSE is provided by the Session/Transport/Network Service.

The DICOM Application Entity uses the services provided by the DICOM Message Service Element. The DICOM Message Service Element specifies two sets of services.

- DIMSE-C supports operations associated with composite SOP Classes and provides effective compatibility with the previous versions of the DICOM Standard.
- DIMSE-N supports operations associated with normalized SOP Classes and provides an extended set of object-oriented operations and notifications. It is based on the OSI System Management Model and more specifically on the OSI Common Management Information Services (CMIS) Service definition.



DICOM PS3.3 2016b - Information Object Definitions

F.2.2.2 Example of a DICOMDIR File Structure

Prev	F.2.2 Example of A Directory	Next

PS3.3 > Basic Directory Information Object Definition (Normative) > Basic Directory IOD Overview > Example of A Directory > Example of a DICOMDIR File Structure

F.2.2.2 Example of a DICOMDIR File Structure

Based on the example discussed in Section F.2.2.1, the internal data structure used by the Basic Directory IOD is depicted in Figure F.2-3. It shows a set of Directory Records where each Directory Record is linked by three different types of "referencing" mechanisms:

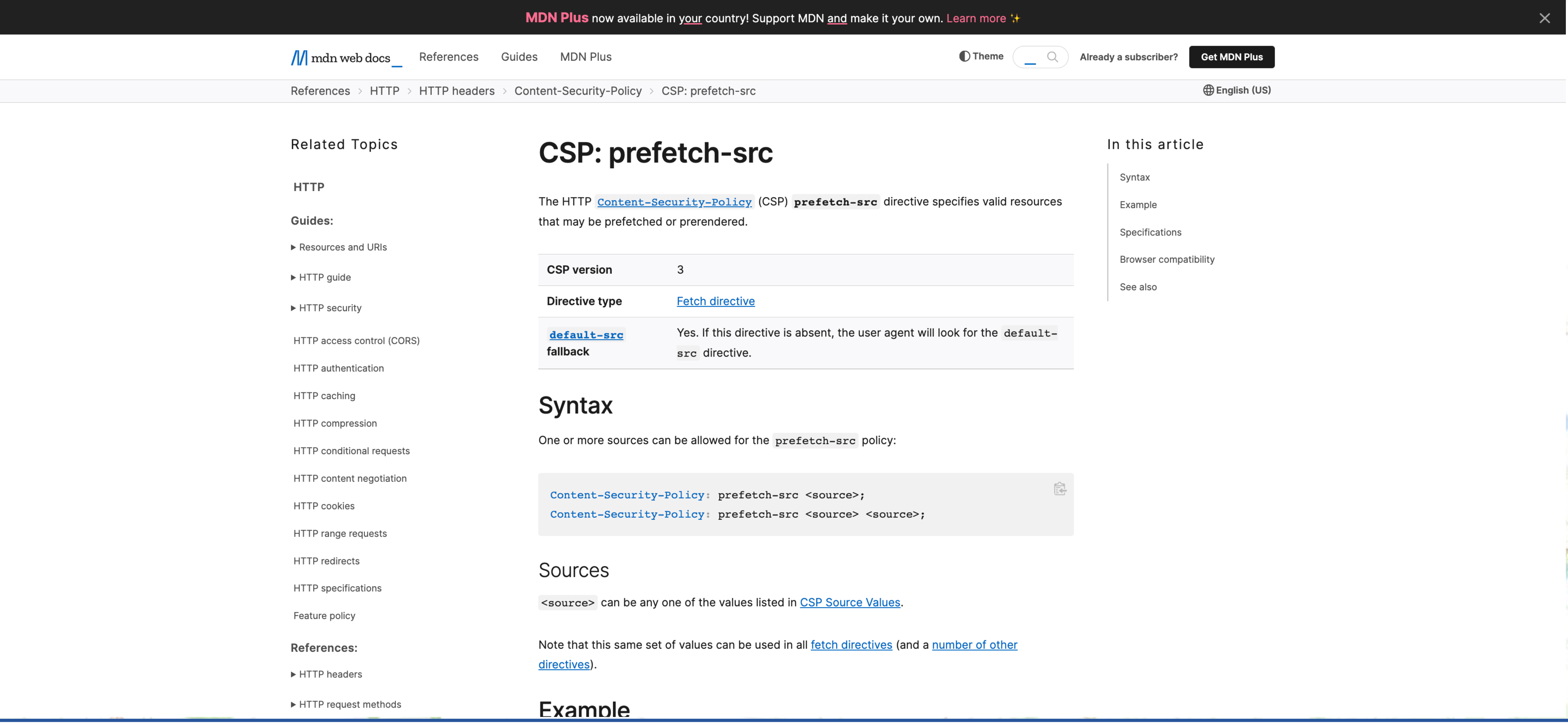
a. The chaining of Directory Records to form a Directory Entity. In particular, this facilitates the addition of new Directory Records at the level of any Directory Entity by placing them at the end of the DICOMDIR File. On Figure F.2-3, this chaining is shown by yellow lines:

1. #1 shows the chaining of the Directory Records forming the root Directory Entity
2. #2 shows the chaining of the Directory Records for the Directory Entity related to Patient A
3. #3 shows the chaining of the Directory Records for the Directory Entity related to Study 1
4. #4 shows the chaining of the Directory Records for the Directory Entity related to Series 1

b. Green lines depict the reference by a Directory Record to a lower level Directory Entity

c. Blue lines depict the reference by a Directory Record to a stored file containing a SOP Class

This example of a DICOMDIR File structure shows one example of a specific order of the Directory Records. Other orderings of Directory Records could result in a functionally equivalent directory.



CSP: prefetch-src

The HTTP `Content-Security-Policy` (CSP) **`prefetch-src`** directive specifies valid resources that may be prefetched or prerendered.

CSP version	3
Directive type	Fetch directive
`default-src` fallback	Yes. If this directive is absent, the user agent will look for the `default-src` directive.

Syntax

One or more sources can be allowed for the `prefetch-src` policy:

```
Content-Security-Policy: prefetch-src <source>;
Content-Security-Policy: prefetch-src <source> <source>;
```

Sources

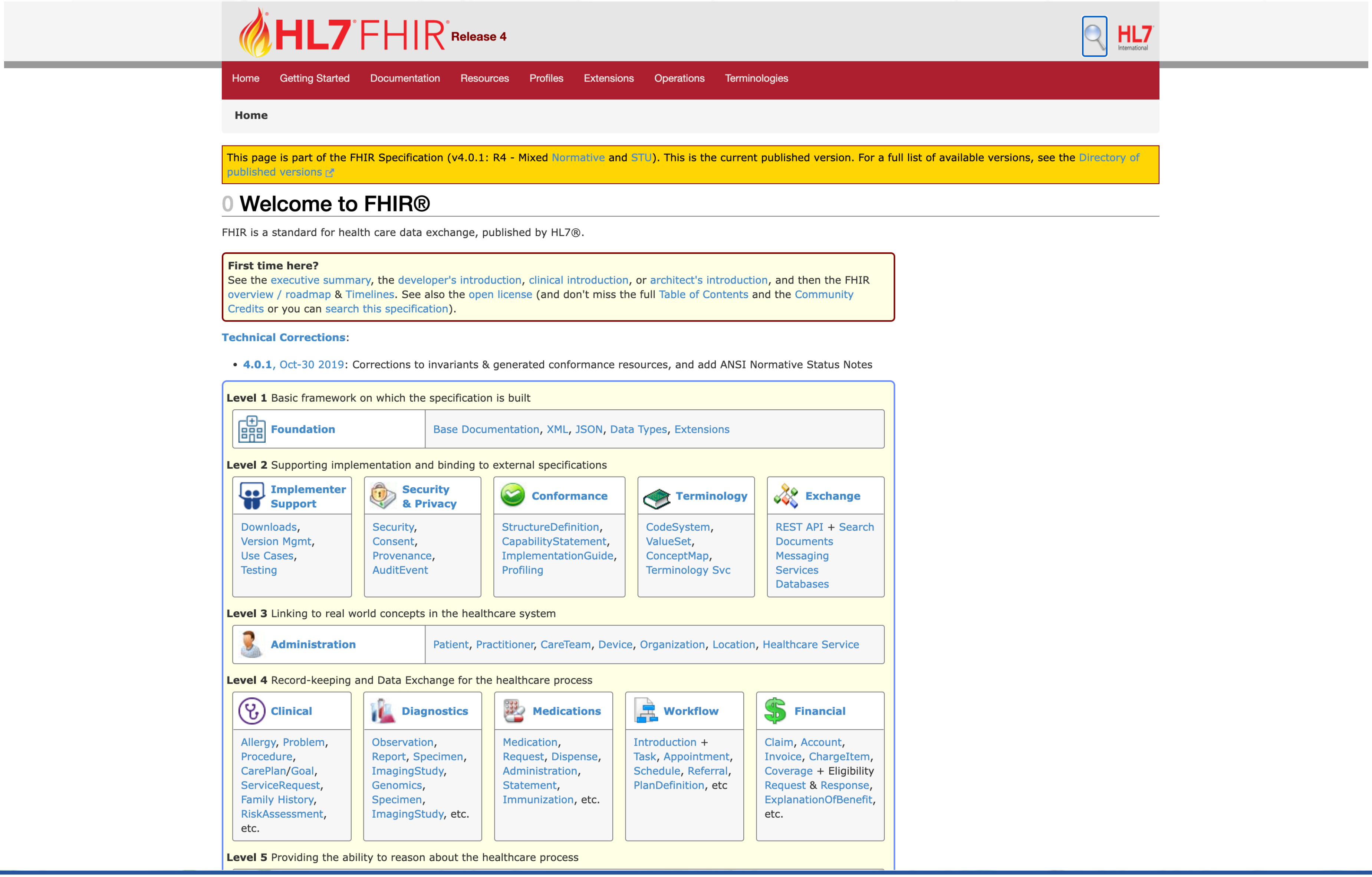
`<source>` can be any one of the values listed in CSP Source Values.

Note that this same set of values can be used in all fetch directives (and a number of other directives).

Example

Great. That's a start.

Q3: How would this work in practice with genomics and the latest web technologies and government standards?



This page is part of the FHIR Specification (v4.0.1: R4 - Mixed Normative and STU). This is the current published version. For a full list of available versions, see the Directory of published versions

0 Welcome to FHIR®

FHIR is a standard for health care data exchange, published by HL7®.

First time here?
See the executive summary, the developer's introduction, clinical introduction, or architect's introduction, and then the FHIR overview / roadmap & Timelines. See also the open license (and don't miss the full Table of Contents and the Community Credits or you can search this specification).

Technical Corrections:

- **4.0.1**, Oct-30 2019: Corrections to invariants & generated conformance resources, and add ANSI Normative Status Notes

Level 1 Basic framework on which the specification is built

Foundation	Base Documentation, XML, JSON, Data Types, Extensions

Level 2 Supporting implementation and binding to external specifications

Implementer Support	**Security & Privacy**	**Conformance**	**Terminology**	**Exchange**
Downloads, Version Mgmt, Use Cases, Testing	Security, Consent, Provenance, AuditEvent	StructureDefinition, CapabilityStatement, ImplementationGuide, Profiling	CodeSystem, ValueSet, ConceptMap, Terminology Svc	REST API + Search Documents Messaging Services Databases

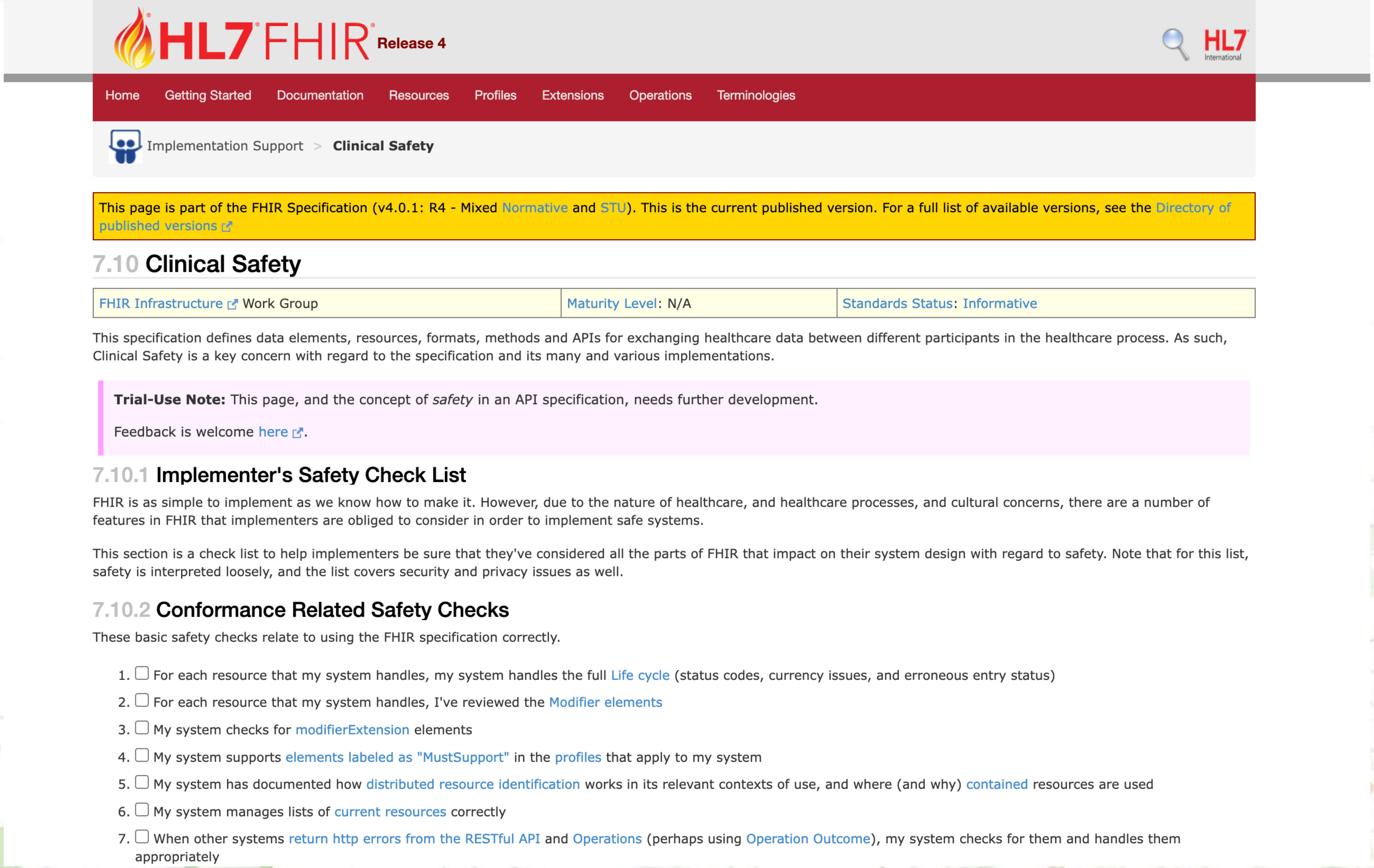
Level 3 Linking to real world concepts in the healthcare system

Administration	Patient, Practitioner, CareTeam, Device, Organization, Location, Healthcare Service

Level 4 Record-keeping and Data Exchange for the healthcare process

Clinical	**Diagnostics**	**Medications**	**Workflow**	**Financial**
Allergy, Problem, Procedure, CarePlan/Goal, ServiceRequest, Family History, RiskAssessment, etc.	Observation, Report, Specimen, ImagingStudy, Genomics, Specimen, ImagingStudy, etc.	Medication, Request, Dispense, Administration, Statement, Immunization, etc.	Introduction + Task, Appointment, Schedule, Referral, PlanDefinition, etc	Claim, Account, Invoice, ChargeItem, Coverage + Eligibility Request & Response, ExplanationOfBenefit, etc.

Level 5 Providing the ability to reason about the healthcare process



This page is part of the FHIR Specification (v4.0.1: R4 - Mixed Normative and STU). This is the current published version. For a full list of available versions, see the Directory of published versions

7.10 Clinical Safety

FHIR Infrastructure Work Group	Maturity Level: N/A	Standards Status: Informative

This specification defines data elements, resources, formats, methods and APIs for exchanging healthcare data between different participants in the healthcare process. As such, Clinical Safety is a key concern with regard to the specification and its many and various implementations.

> **Trial-Use Note:** This page, and the concept of *safety* in an API specification, needs further development.
>
> Feedback is welcome here.

7.10.1 Implementer's Safety Check List

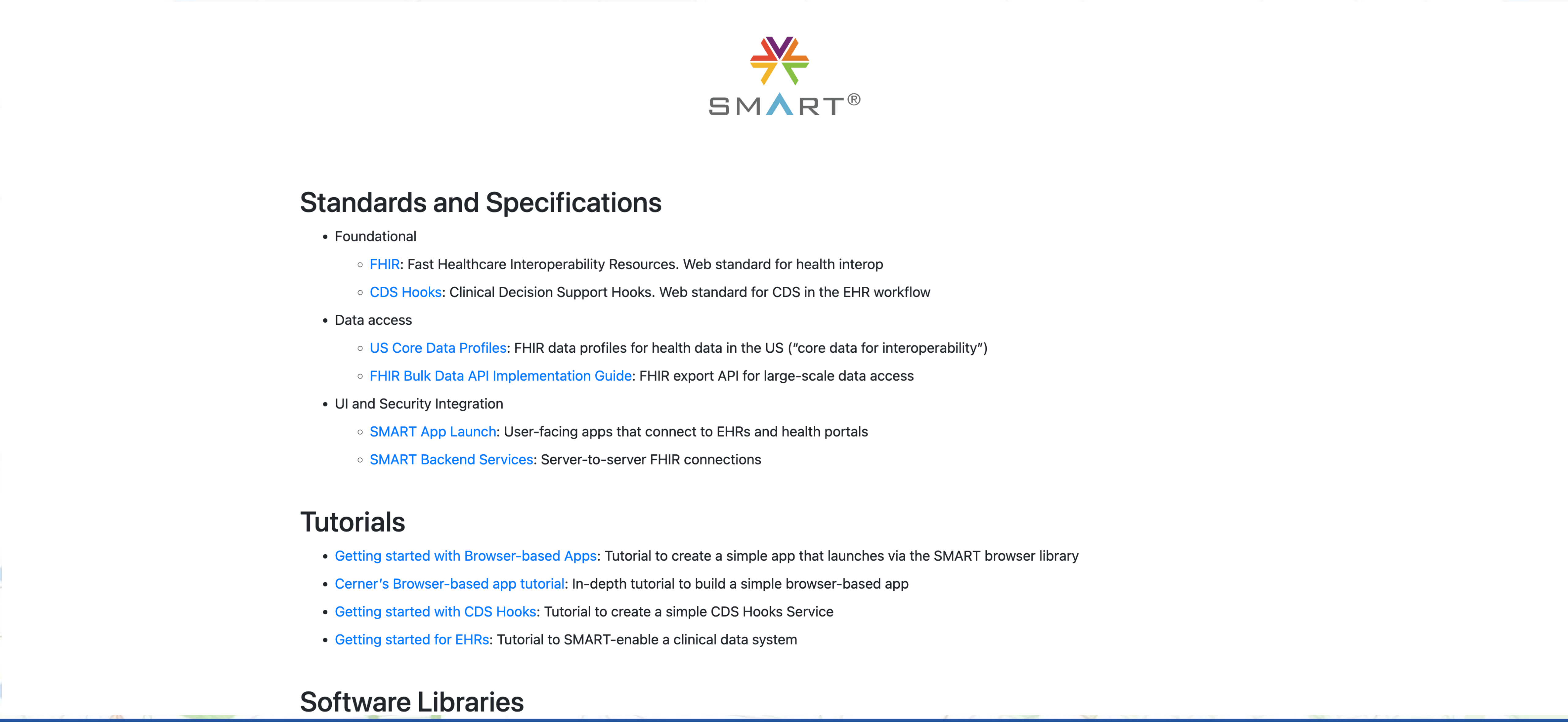
FHIR is as simple to implement as we know how to make it. However, due to the nature of healthcare, and healthcare processes, and cultural concerns, there are a number of features in FHIR that implementers are obliged to consider in order to implement safe systems.

This section is a check list to help implementers be sure that they've considered all the parts of FHIR that impact on their system design with regard to safety. Note that for this list, safety is interpreted loosely, and the list covers security and privacy issues as well.

7.10.2 Conformance Related Safety Checks

These basic safety checks relate to using the FHIR specification correctly.

1. □ For each resource that my system handles, my system handles the full Life cycle (status codes, currency issues, and erroneous entry status)
2. □ For each resource that my system handles, I've reviewed the Modifier elements
3. □ My system checks for modifierExtension elements
4. □ My system supports elements labeled as "MustSupport" in the profiles that apply to my system
5. □ My system has documented how distributed resource identification works in its relevant contexts of use, and where (and why) contained resources are used
6. □ My system manages lists of current resources correctly
7. □ When other systems return http errors from the RESTful API and Operations (perhaps using Operation Outcome), my system checks for them and handles them appropriately



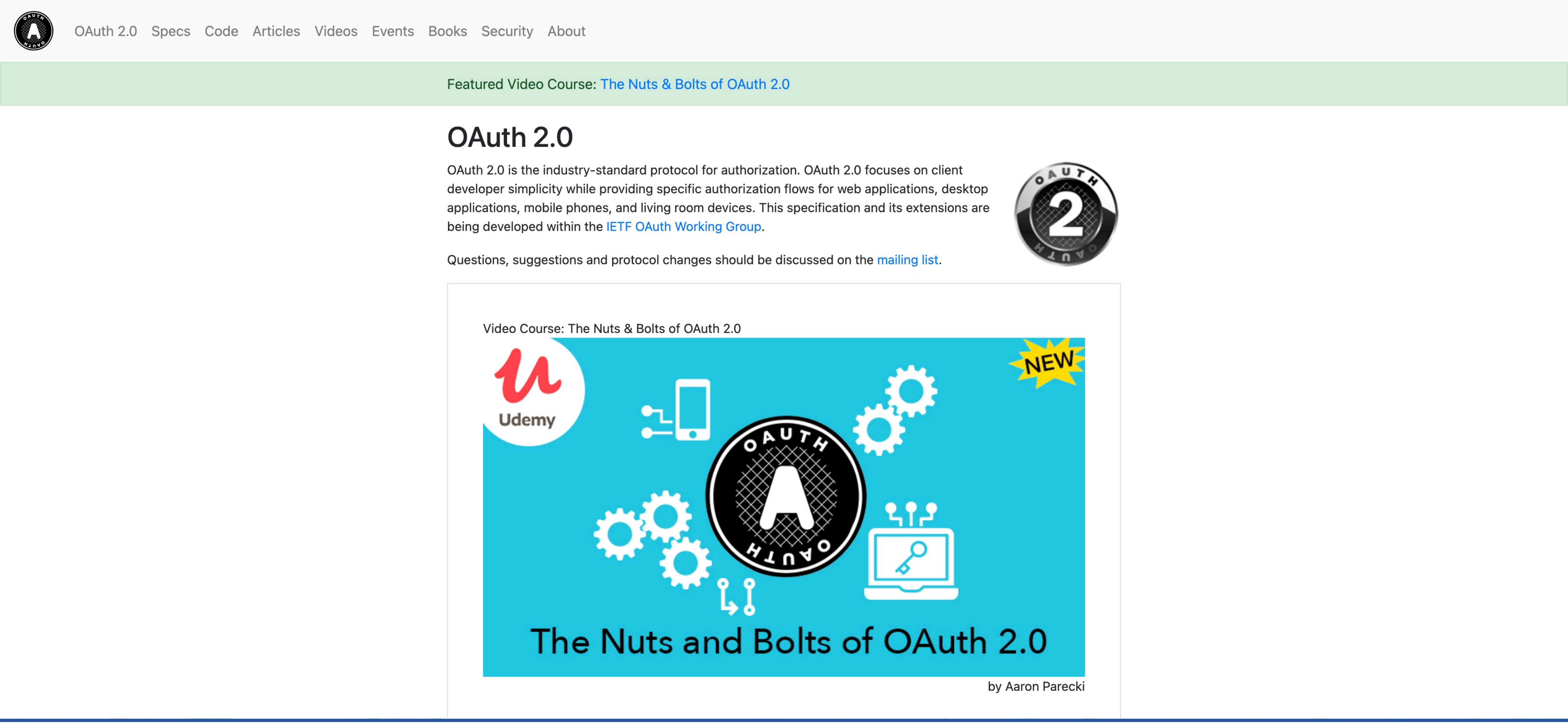
Standards and Specifications

- Foundational
  - FHIR: Fast Healthcare Interoperability Resources. Web standard for health interop
  - CDS Hooks: Clinical Decision Support Hooks. Web standard for CDS in the EHR workflow
- Data access
  - US Core Data Profiles: FHIR data profiles for health data in the US ("core data for interoperability")
  - FHIR Bulk Data API Implementation Guide: FHIR export API for large-scale data access
- UI and Security Integration
  - SMART App Launch: User-facing apps that connect to EHRs and health portals
  - SMART Backend Services: Server-to-server FHIR connections

Tutorials

- Getting started with Browser-based Apps: Tutorial to create a simple app that launches via the SMART browser library
- Cerner's Browser-based app tutorial: In-depth tutorial to build a simple browser-based app
- Getting started with CDS Hooks: Tutorial to create a simple CDS Hooks Service
- Getting started for EHRs: Tutorial to SMART-enable a clinical data system

Software Libraries



Featured Video Course: The Nuts & Bolts of OAuth 2.0

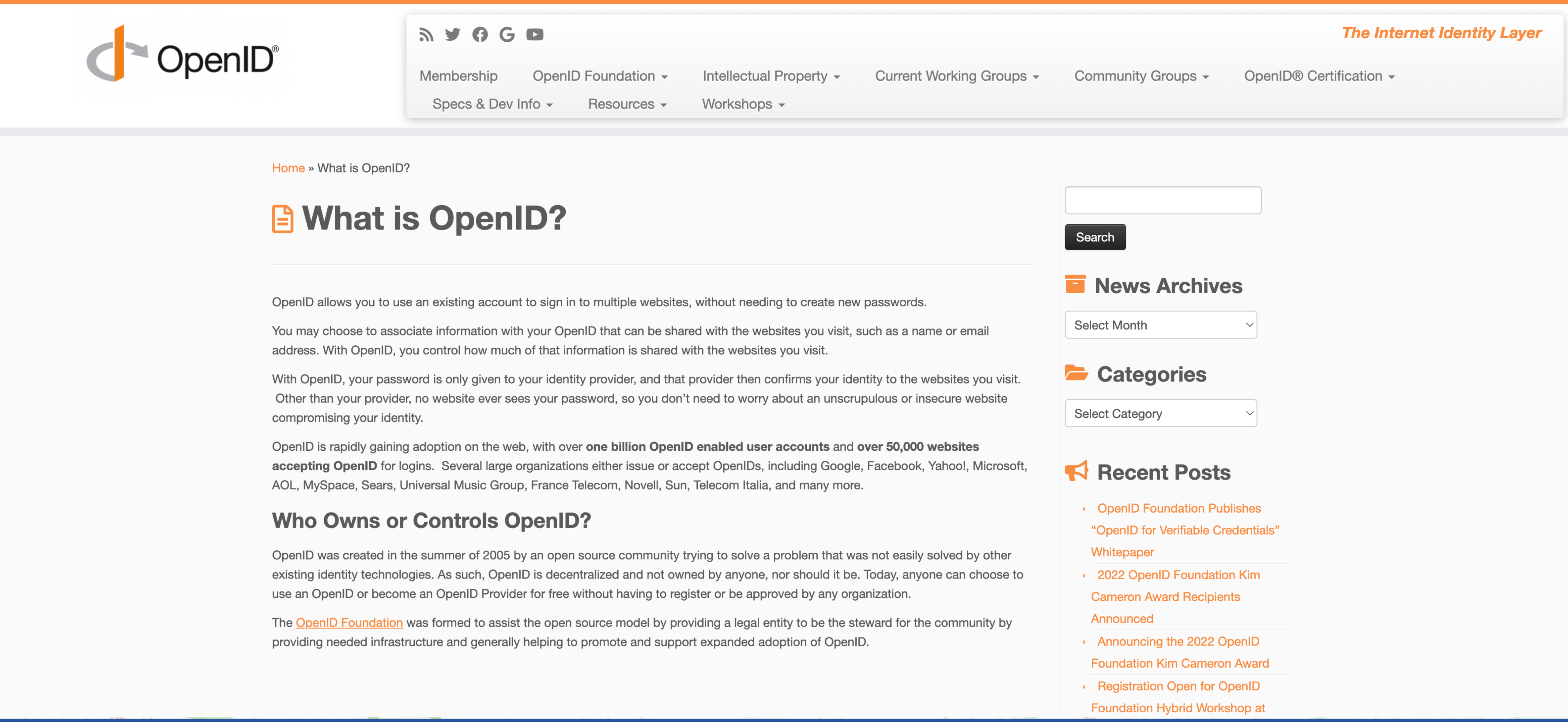
OAuth 2.0

OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices. This specification and its extensions are being developed within the IETF OAuth Working Group.

Questions, suggestions and protocol changes should be discussed on the mailing list.

Video Course: The Nuts & Bolts of OAuth 2.0

by Aaron Parecki



What is OpenID?

OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.

You may choose to associate information with your OpenID that can be shared with the websites you visit, such as a name or email address. With OpenID, you control how much of that information is shared with the websites you visit.

With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. Other than your provider, no website ever sees your password, so you don't need to worry about an unscrupulous or insecure website compromising your identity.

OpenID is rapidly gaining adoption on the web, with over **one billion OpenID enabled user accounts** and **over 50,000 websites accepting OpenID** for logins. Several large organizations either issue or accept OpenIDs, including Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia, and many more.

Who Owns or Controls OpenID?

OpenID was created in the summer of 2005 by an open source community trying to solve a problem that was not easily solved by other existing identity technologies. As such, OpenID is decentralized and not owned by anyone, nor should it be. Today, anyone can choose to use an OpenID or become an OpenID Provider for free without having to register or be approved by any organization.

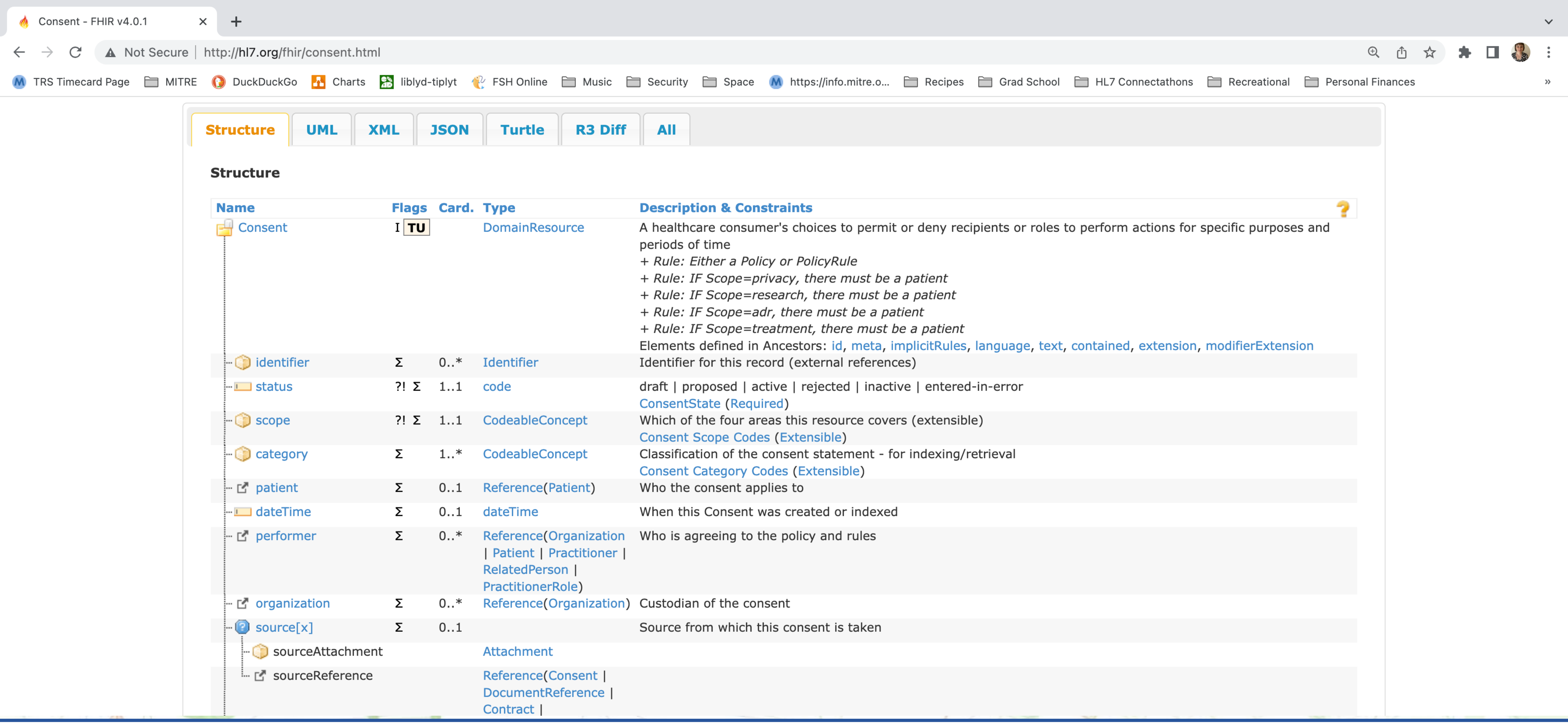
The OpenID Foundation was formed to assist the open source model by providing a legal entity to be the steward for the community by providing needed infrastructure and generally helping to promote and support expanded adoption of OpenID.

News Archives

Categories

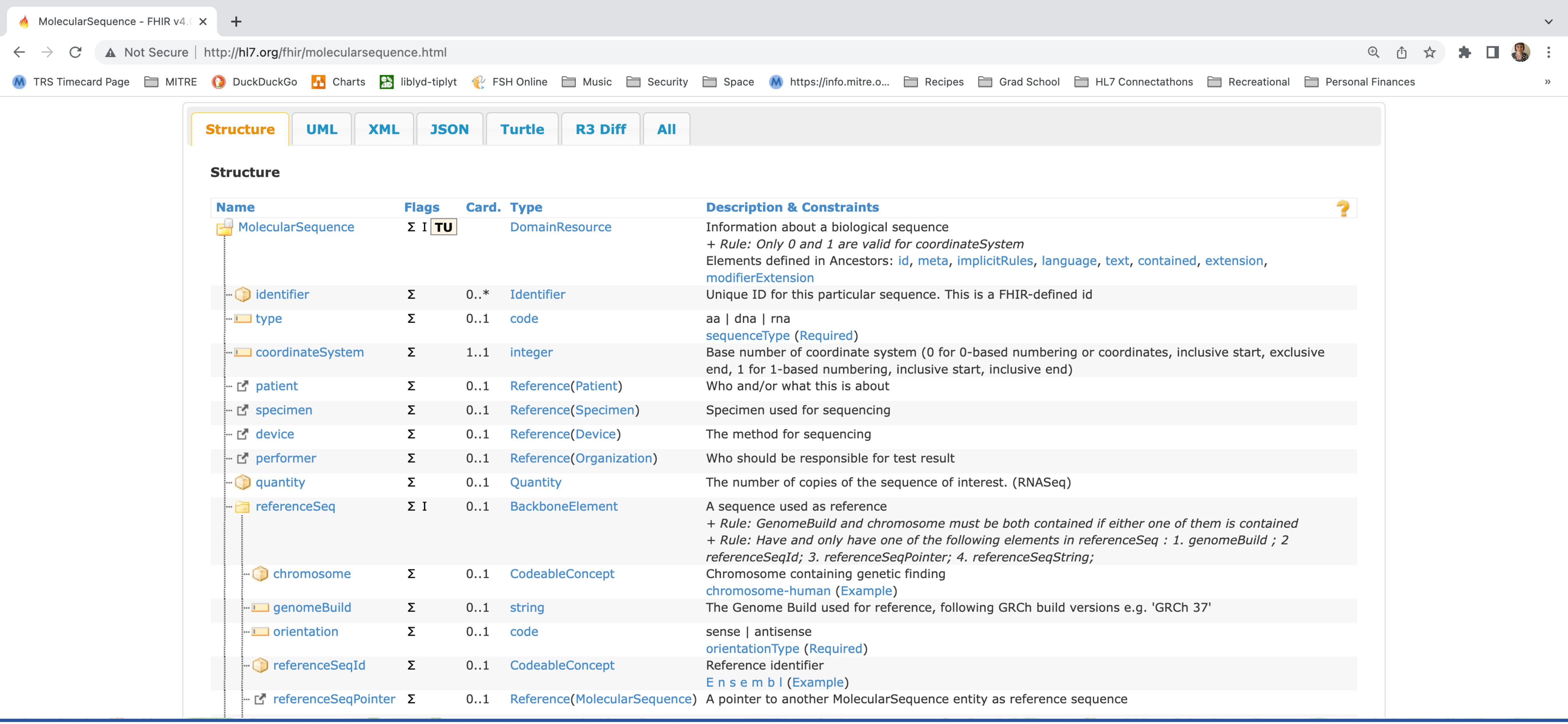
Recent Posts

- OpenID Foundation Publishes "OpenID for Verifiable Credentials" Whitepaper
- 2022 OpenID Foundation Kim Cameron Award Recipients Announced
- Announcing the 2022 OpenID Foundation Kim Cameron Award
- Registration Open for OpenID Foundation Hybrid Workshop at



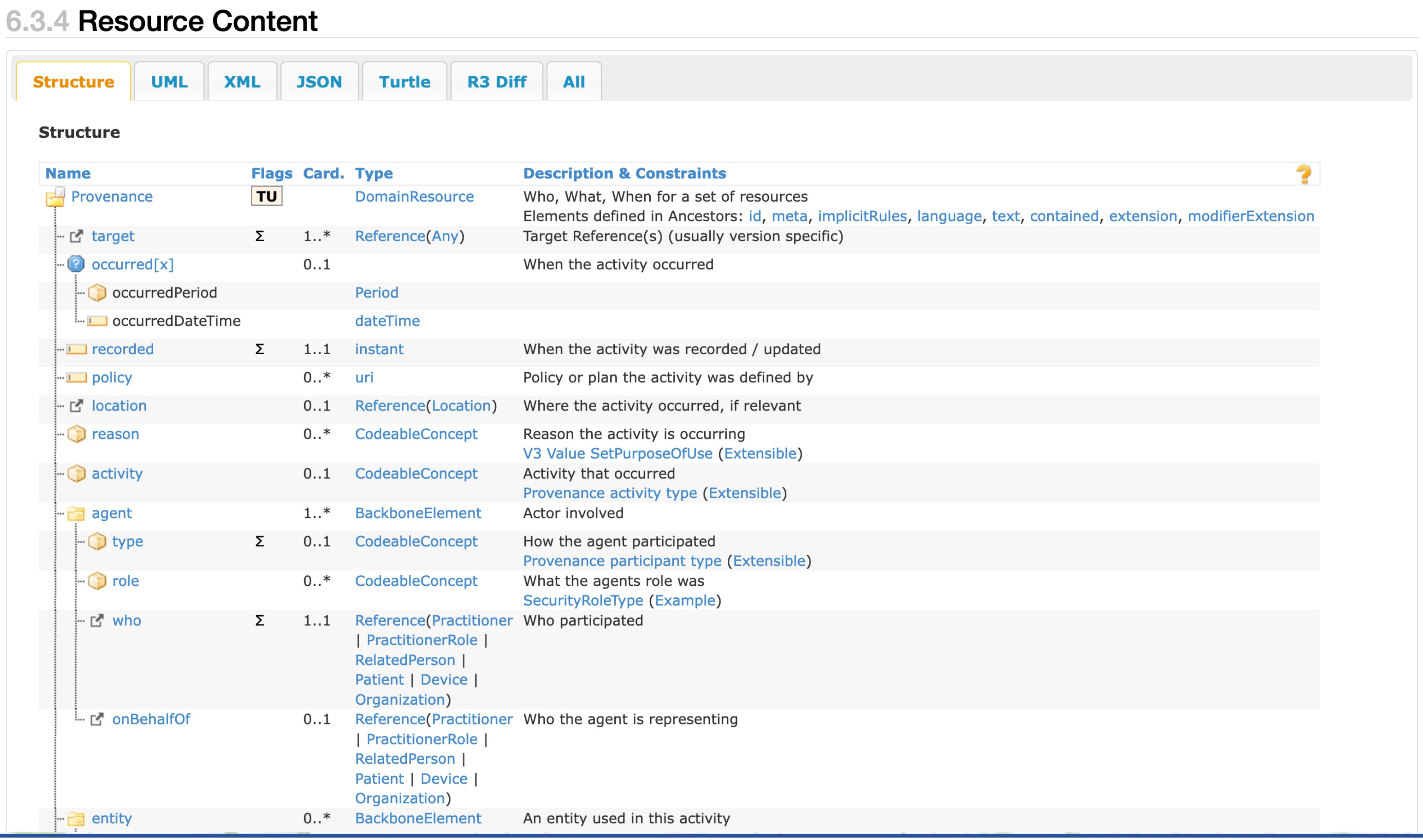
Structure

Name	Flags	Card.	Type	Description & Constraints
Consent	I TU		DomainResource	A healthcare consumer's choices to permit or deny recipients or roles to perform actions for specific purposes and periods of time *+ Rule: Either a Policy or PolicyRule* *+ Rule: IF Scope=privacy, there must be a patient* *+ Rule: IF Scope=research, there must be a patient* *+ Rule: IF Scope=adr, there must be a patient* *+ Rule: IF Scope=treatment, there must be a patient* Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
identifier	Σ	0..*	Identifier	Identifier for this record (external references)
status	?! Σ	1..1	code	draft | proposed | active | rejected | inactive | entered-in-error ConsentState (Required)
scope	?! Σ	1..1	CodeableConcept	Which of the four areas this resource covers (extensible) Consent Scope Codes (Extensible)
category	Σ	1..*	CodeableConcept	Classification of the consent statement - for indexing/retrieval Consent Category Codes (Extensible)
patient	Σ	0..1	Reference(Patient)	Who the consent applies to
dateTime	Σ	0..1	dateTime	When this Consent was created or indexed
performer	Σ	0..*	Reference(Organization | Patient | Practitioner | RelatedPerson | PractitionerRole)	Who is agreeing to the policy and rules
organization	Σ	0..*	Reference(Organization)	Custodian of the consent
source[x]	Σ	0..1		Source from which this consent is taken
sourceAttachment			Attachment	
sourceReference			Reference(Consent | DocumentReference | Contract |	



Structure

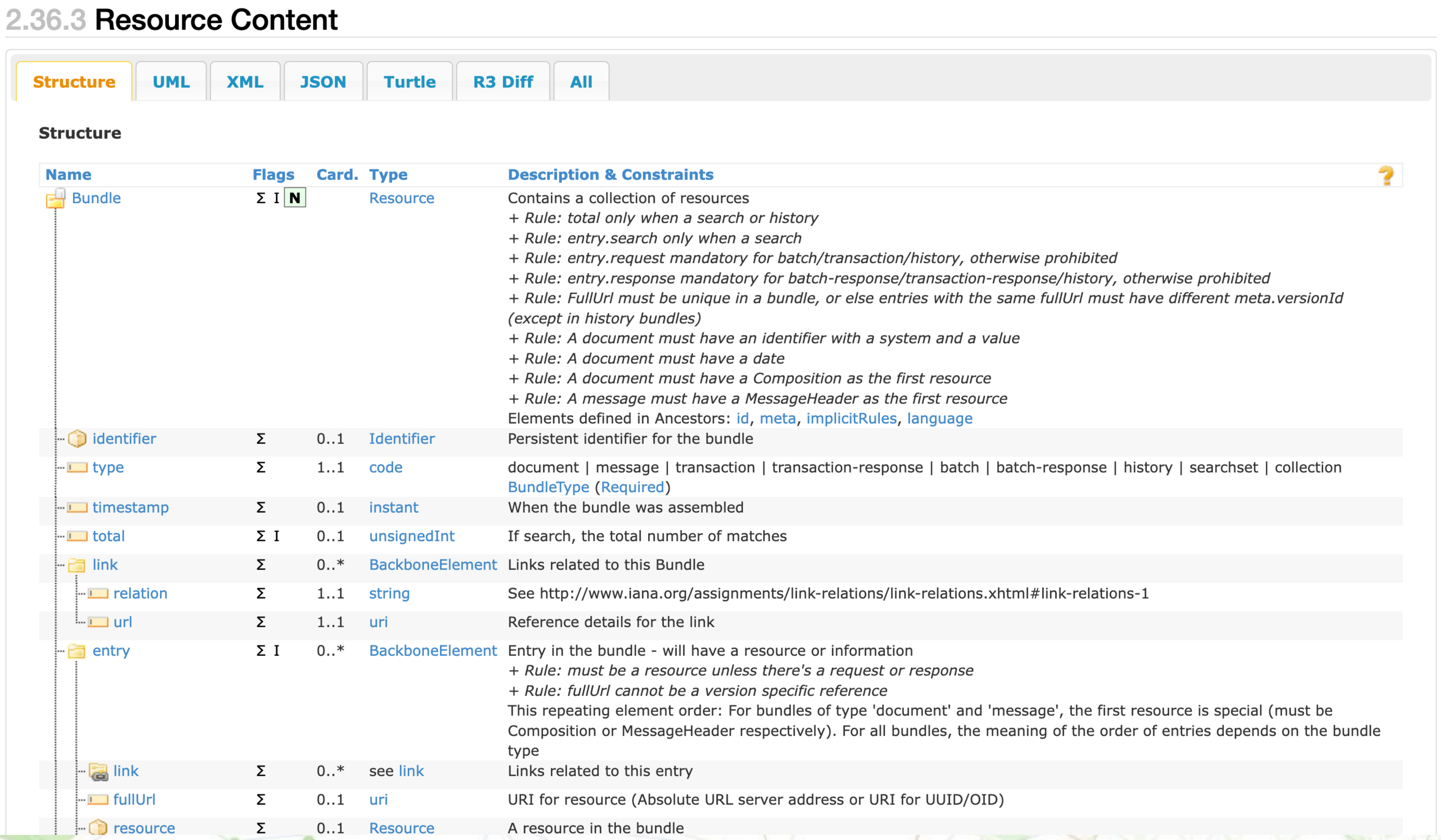
Name	Flags	Card.	Type	Description & Constraints
MolecularSequence	Σ I TU		DomainResource	Information about a biological sequence *+ Rule: Only 0 and 1 are valid for coordinateSystem* Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
identifier	Σ	0..*	Identifier	Unique ID for this particular sequence. This is a FHIR-defined id
type	Σ	0..1	code	aa | dna | rna sequenceType (Required)
coordinateSystem	Σ	1..1	integer	Base number of coordinate system (0 for 0-based numbering or coordinates, inclusive start, exclusive end, 1 for 1-based numbering, inclusive start, inclusive end)
patient	Σ	0..1	Reference(Patient)	Who and/or what this is about
specimen	Σ	0..1	Reference(Specimen)	Specimen used for sequencing
device	Σ	0..1	Reference(Device)	The method for sequencing
performer	Σ	0..1	Reference(Organization)	Who should be responsible for test result
quantity	Σ	0..1	Quantity	The number of copies of the sequence of interest. (RNASeq)
referenceSeq	Σ I	0..1	BackboneElement	A sequence used as reference *+ Rule: GenomeBuild and chromosome must be both contained if either one of them is contained* *+ Rule: Have and only have one of the following elements in referenceSeq : 1. genomeBuild ; 2 referenceSeqId; 3. referenceSeqPointer; 4. referenceSeqString;*
chromosome	Σ	0..1	CodeableConcept	Chromosome containing genetic finding chromosome-human (Example)
genomeBuild	Σ	0..1	string	The Genome Build used for reference, following GRCh build versions e.g. 'GRCh 37'
orientation	Σ	0..1	code	sense | antisense orientationType (Required)
referenceSeqId	Σ	0..1	CodeableConcept	Reference identifier Ensembl (Example)
referenceSeqPointer	Σ	0..1	Reference(MolecularSequence)	A pointer to another MolecularSequence entity as reference sequence



6.3.4 Resource Content

Structure

Name	Flags	Card.	Type	Description & Constraints
Provenance	TU		DomainResource	Who, What, When for a set of resources Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
target	Σ	1..*	Reference(Any)	Target Reference(s) (usually version specific)
occurred[x]		0..1		When the activity occurred
occurredPeriod			Period	
occurredDateTime			dateTime	
recorded	Σ	1..1	instant	When the activity was recorded / updated
policy		0..*	uri	Policy or plan the activity was defined by
location		0..1	Reference(Location)	Where the activity occurred, if relevant
reason		0..*	CodeableConcept	Reason the activity is occurring V3 Value SetPurposeOfUse (Extensible)
activity		0..1	CodeableConcept	Activity that occurred Provenance activity type (Extensible)
agent		1..*	BackboneElement	Actor involved
type	Σ	0..1	CodeableConcept	How the agent participated Provenance participant type (Extensible)
role		0..*	CodeableConcept	What the agents role was SecurityRoleType (Example)
who	Σ	1..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	Who participated
onBehalfOf		0..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	Who the agent is representing
entity		0..*	BackboneElement	An entity used in this activity



2.36.3 Resource Content

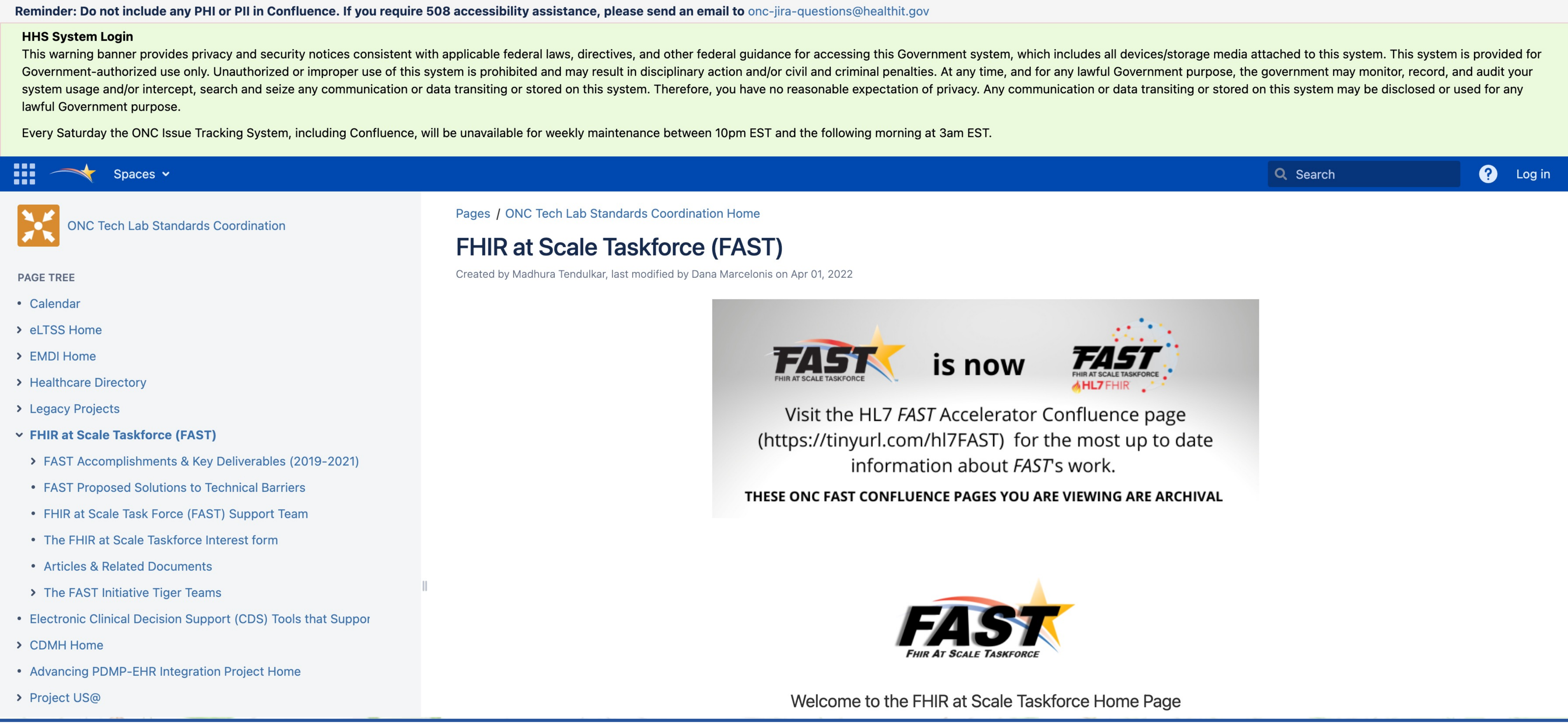
Structure | UML | XML | JSON | Turtle | R3 Diff | All

Structure

Name	Flags	Card.	Type	Description & Constraints
Bundle	Σ I N		Resource	Contains a collection of resources + *Rule: total only when a search or history* + *Rule: entry.search only when a search* + *Rule: entry.request mandatory for batch/transaction/history, otherwise prohibited* + *Rule: entry.response mandatory for batch-response/transaction-response/history, otherwise prohibited* + *Rule: FullUrl must be unique in a bundle, or else entries with the same fullUrl must have different meta.versionId (except in history bundles)* + *Rule: A document must have an identifier with a system and a value* + *Rule: A document must have a date* + *Rule: A document must have a Composition as the first resource* + *Rule: A message must have a MessageHeader as the first resource* Elements defined in Ancestors: id, meta, implicitRules, language
identifier	Σ	0..1	Identifier	Persistent identifier for the bundle
type	Σ	1..1	code	document | message | transaction | transaction-response | batch | batch-response | history | searchset | collection BundleType (Required)
timestamp	Σ	0..1	instant	When the bundle was assembled
total	Σ I	0..1	unsignedInt	If search, the total number of matches
link	Σ	0..*	BackboneElement	Links related to this Bundle
relation	Σ	1..1	string	See http://www.iana.org/assignments/link-relations/link-relations.xhtml#link-relations-1
url	Σ	1..1	uri	Reference details for the link
entry	Σ I	0..*	BackboneElement	Entry in the bundle - will have a resource or information + *Rule: must be a resource unless there's a request or response* + *Rule: fullUrl cannot be a version specific reference* This repeating element order: For bundles of type 'document' and 'message', the first resource is special (must be Composition or MessageHeader respectively). For all bundles, the meaning of the order of entries depends on the bundle type
link	Σ	0..*	see link	Links related to this entry
fullUrl	Σ	0..1	uri	URI for resource (Absolute URL server address or URI for UUID/OID)
resource	Σ	0..1	Resource	A resource in the bundle

Might also use:

- Media
- DocumentReference
- DocumentManifest
- DiagnosticReport



Reminder: Do not include any PHI or PII in Confluence. If you require 508 accessibility assistance, please send an email to onc-jira-questions@healthit.gov

HHS System Login

This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes all devices/storage media attached to this system. This system is provided for Government-authorized use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. At any time, and for any lawful Government purpose, the government may monitor, record, and audit your system usage and/or intercept, search and seize any communication or data transiting or stored on this system. Therefore, you have no reasonable expectation of privacy. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

Every Saturday the ONC Issue Tracking System, including Confluence, will be unavailable for weekly maintenance between 10pm EST and the following morning at 3am EST.

ONC Tech Lab Standards Coordination

PAGE TREE

- Calendar
- eLTSS Home
- EMDI Home
- Healthcare Directory
- Legacy Projects
- FHIR at Scale Taskforce (FAST)
  - FAST Accomplishments & Key Deliverables (2019-2021)
  - FAST Proposed Solutions to Technical Barriers
  - FHIR at Scale Task Force (FAST) Support Team
  - The FHIR at Scale Taskforce Interest form
  - Articles & Related Documents
  - The FAST Initiative Tiger Teams
- Electronic Clinical Decision Support (CDS) Tools that Suppor
- CDMH Home
- Advancing PDMP-EHR Integration Project Home
- Project US@

Pages / ONC Tech Lab Standards Coordination Home

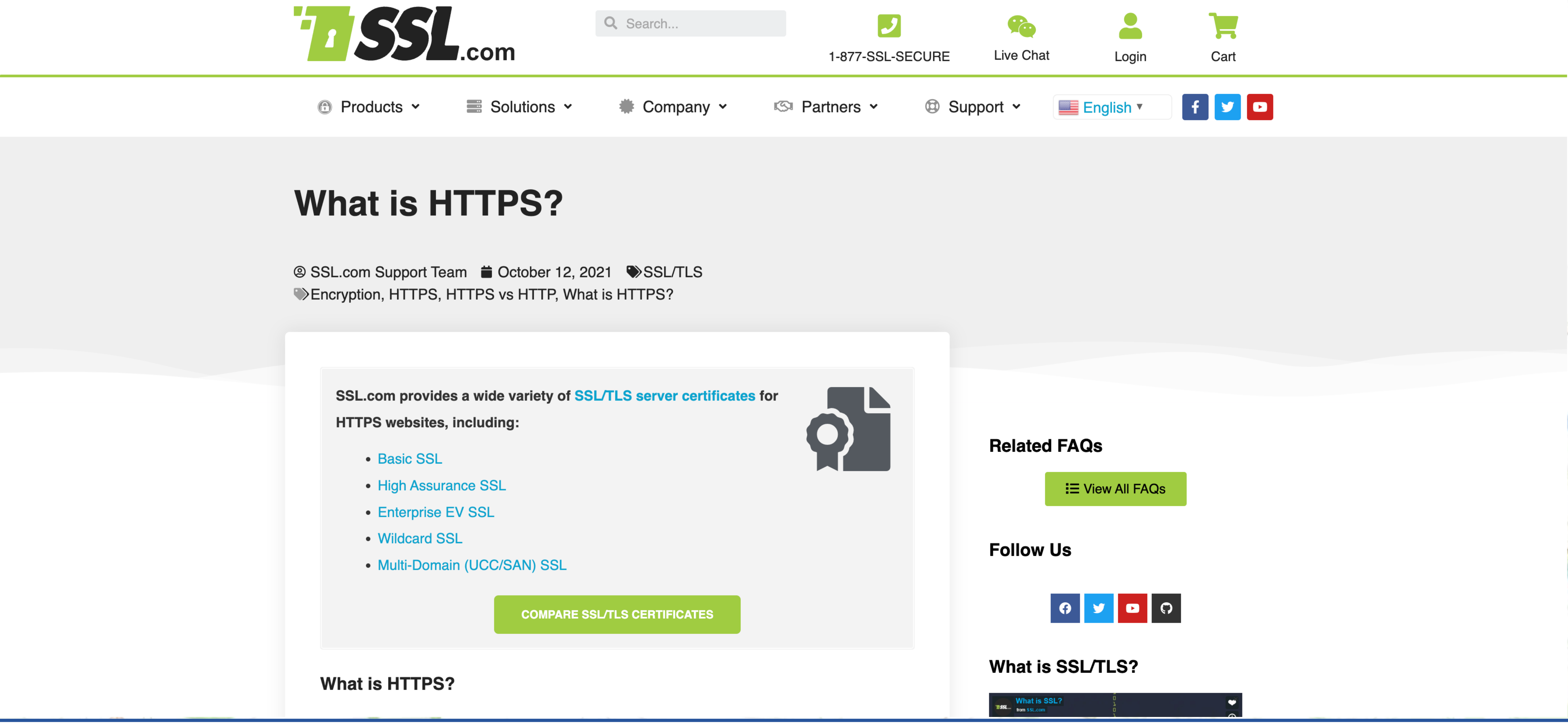
FHIR at Scale Taskforce (FAST)

Created by Madhura Tendulkar, last modified by Dana Marcelonis on Apr 01, 2022

Visit the HL7 *FAST* Accelerator Confluence page (https://tinyurl.com/hl7FAST) for the most up to date information about *FAST*'s work.

THESE ONC FAST CONFLUENCE PAGES YOU ARE VIEWING ARE ARCHIVAL

Welcome to the FHIR at Scale Taskforce Home Page



What is HTTPS?

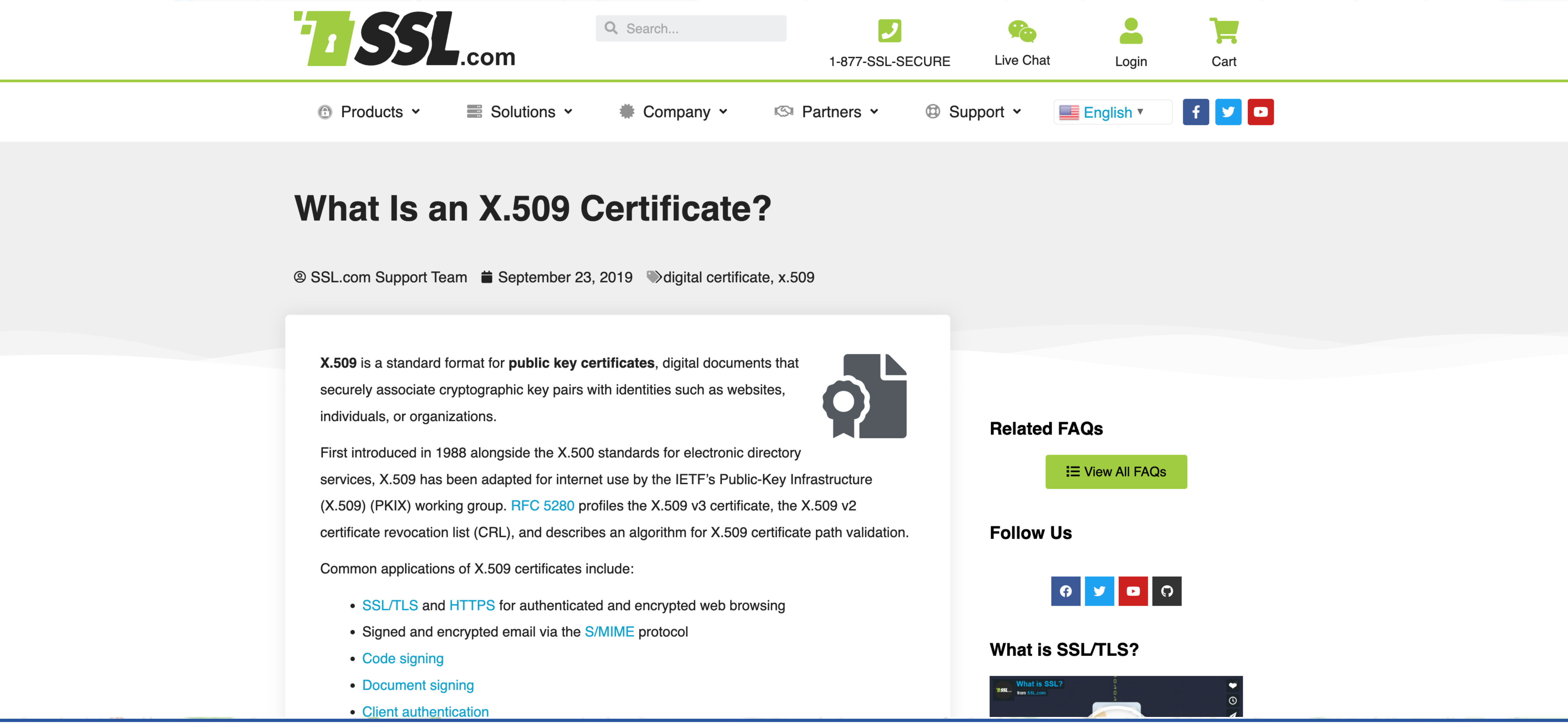
SSL.com Support Team October 12, 2021 SSL/TLS
Encryption, HTTPS, HTTPS vs HTTP, What is HTTPS?

SSL.com provides a wide variety of SSL/TLS server certificates for HTTPS websites, including:

- Basic SSL
- High Assurance SSL
- Enterprise EV SSL
- Wildcard SSL
- Multi-Domain (UCC/SAN) SSL

COMPARE SSL/TLS CERTIFICATES

What is HTTPS?



What Is an X.509 Certificate?

SSL.com Support Team September 23, 2019 digital certificate, x.509

X.509 is a standard format for **public key certificates**, digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations.

First introduced in 1988 alongside the X.500 standards for electronic directory services, X.509 has been adapted for internet use by the IETF's Public-Key Infrastructure (X.509) (PKIX) working group. RFC 5280 profiles the X.509 v3 certificate, the X.509 v2 certificate revocation list (CRL), and describes an algorithm for X.509 certificate path validation.

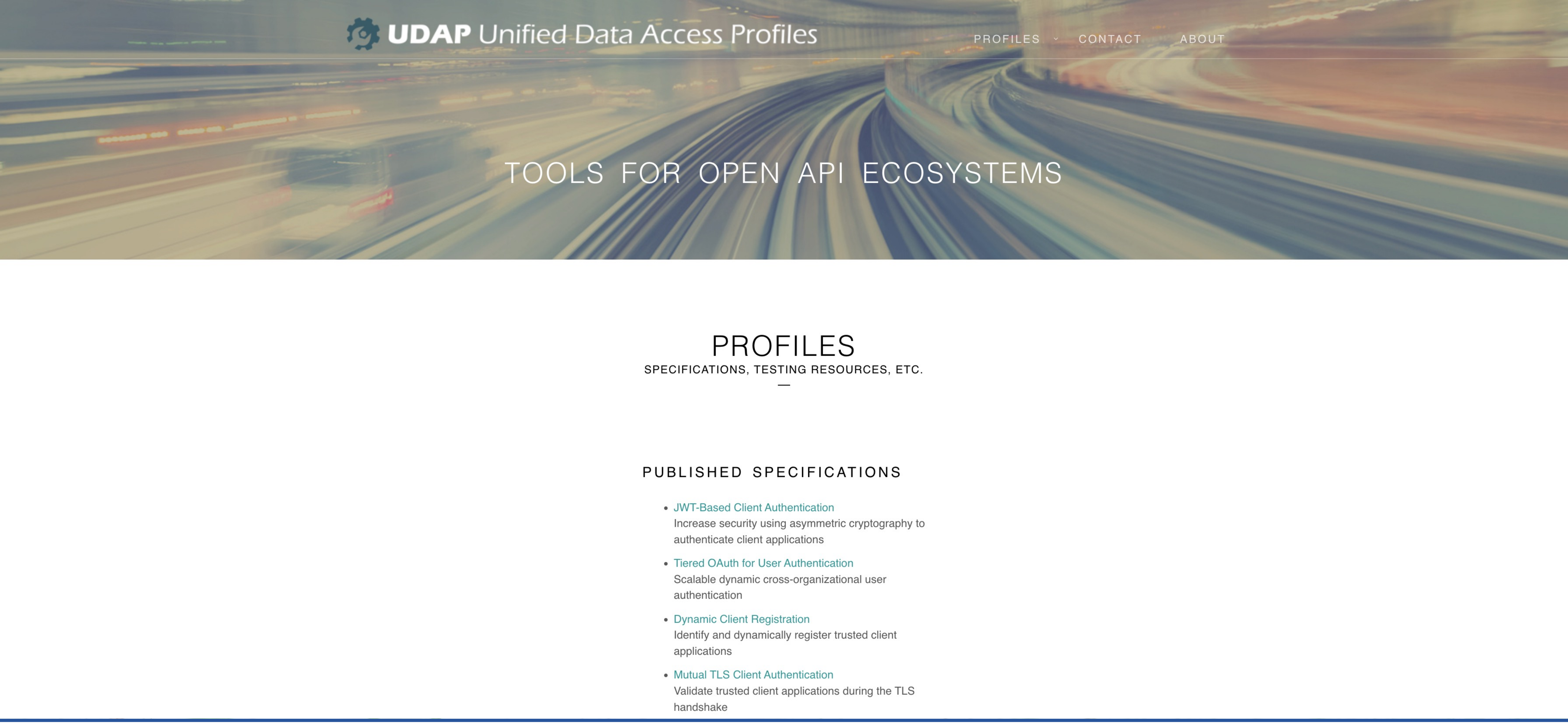
Common applications of X.509 certificates include:

- SSL/TLS and HTTPS for authenticated and encrypted web browsing
- Signed and encrypted email via the S/MIME protocol
- Code signing
- Document signing
- Client authentication

Related FAQs

Follow Us

What is SSL/TLS?



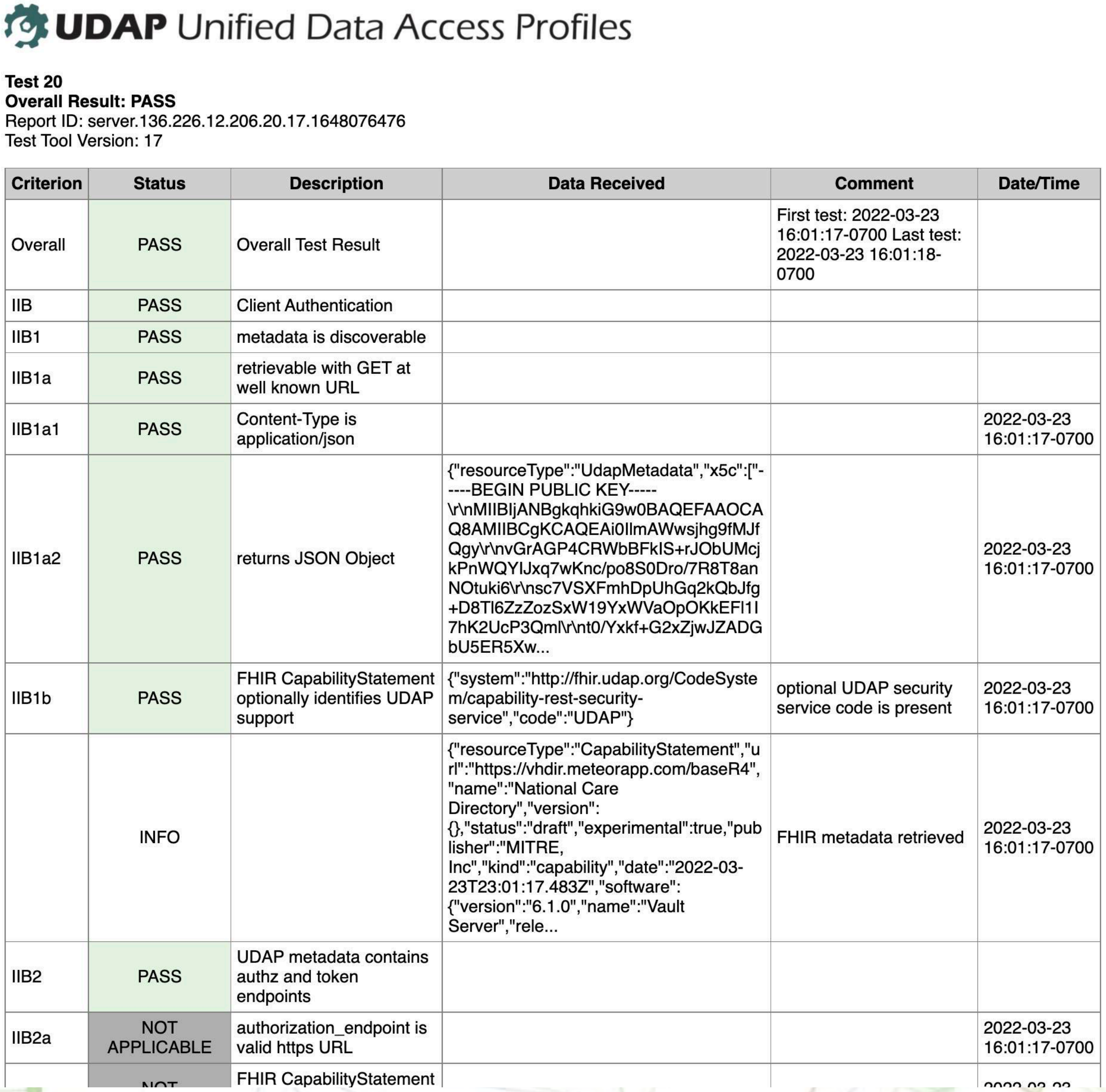
TOOLS FOR OPEN API ECOSYSTEMS

PROFILES

SPECIFICATIONS, TESTING RESOURCES, ETC.

PUBLISHED SPECIFICATIONS

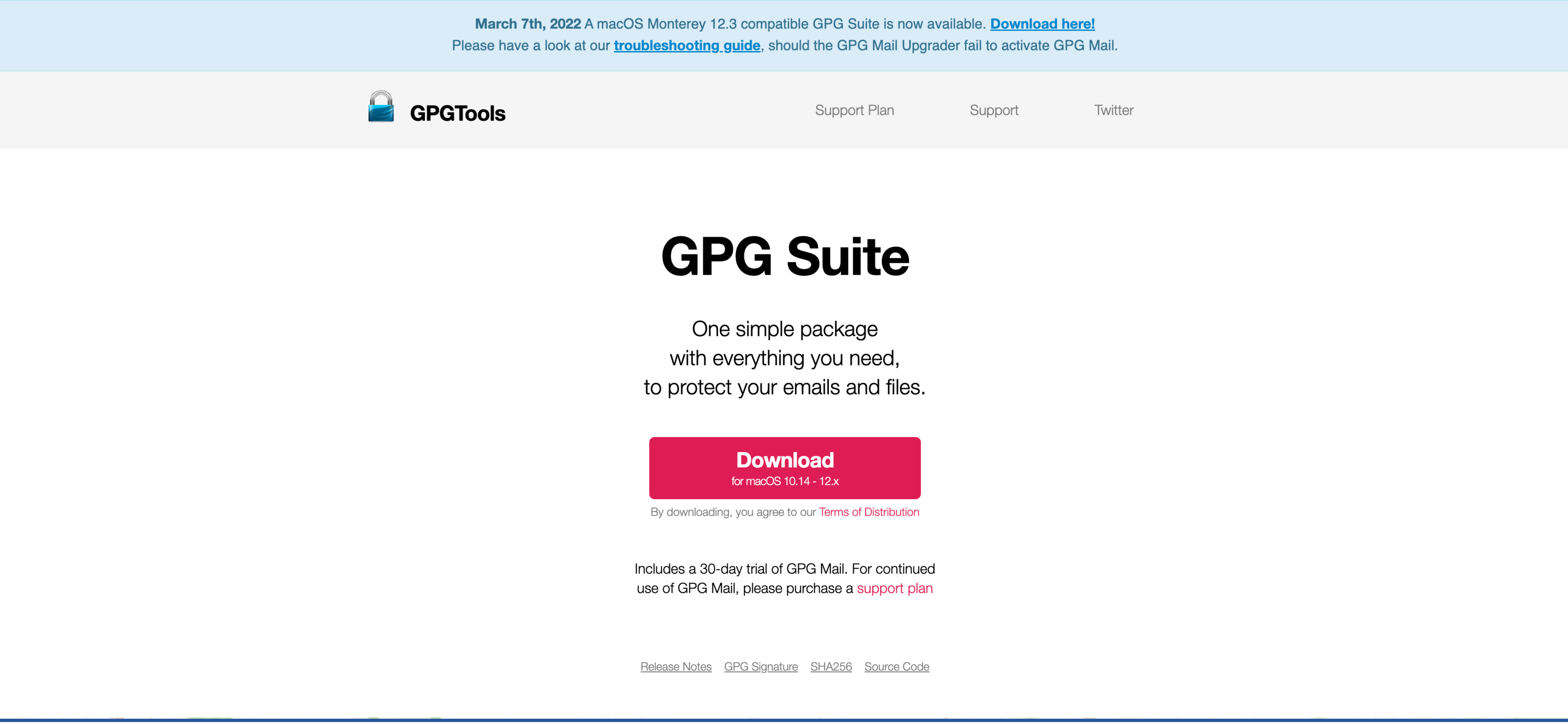
- JWT-Based Client Authentication
  Increase security using asymmetric cryptography to authenticate client applications
- Tiered OAuth for User Authentication
  Scalable dynamic cross-organizational user authentication
- Dynamic Client Registration
  Identify and dynamically register trusted client applications
- Mutual TLS Client Authentication
  Validate trusted client applications during the TLS handshake



UDAP Unified Data Access Profiles

Test 20
Overall Result: PASS
Report ID: server.136.226.12.206.20.17.1648076476
Test Tool Version: 17

Criterion	Status	Description	Data Received	Comment	Date/Time
Overall	PASS	Overall Test Result		First test: 2022-03-23 16:01:17-0700 Last test: 2022-03-23 16:01:18-0700	
IIB	PASS	Client Authentication			
IIB1	PASS	metadata is discoverable			
IIB1a	PASS	retrievable with GET at well known URL			
IIB1a1	PASS	Content-Type is application/json			2022-03-23 16:01:17-0700
IIB1a2	PASS	returns JSON Object	{"resourceType":"UdapMetadata","x5c":["-----BEGIN PUBLIC KEY-----\r\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi0IlmAWwsjhg9fMJfQgy\r\nvGrAGP4CRWbBFkIS+rJObUMcjkPnWQYIJxq7wKnc/po8S0Dro/7R8T8anNOtuki6\r\nsc7VSXFmhDpUhGq2kQbJfg+D8Tl6ZzZozSxW19YxWVaOpOKkEFl1I7hK2UcP3Qml\r\nt0/Yxkf+G2xZjwJZADGbU5ER5Xw...		2022-03-23 16:01:17-0700
IIB1b	PASS	FHIR CapabilityStatement optionally identifies UDAP support	{"system":"http://fhir.udap.org/CodeSystem/capability-rest-security-service","code":"UDAP"}	optional UDAP security service code is present	2022-03-23 16:01:17-0700
	INFO		{"resourceType":"CapabilityStatement","url":"https://vhdir.meteorapp.com/baseR4","name":"National Care Directory","version":{},"status":"draft","experimental":true,"publisher":"MITRE, Inc","kind":"capability","date":"2022-03-23T23:01:17.483Z","software":{"version":"6.1.0","name":"Vault Server","rele...	FHIR metadata retrieved	2022-03-23 16:01:17-0700
IIB2	PASS	UDAP metadata contains authz and token endpoints			
IIB2a	NOT APPLICABLE	authorization_endpoint is valid https URL			2022-03-23 16:01:17-0700
	NOT	FHIR CapabilityStatement			2022-03-23



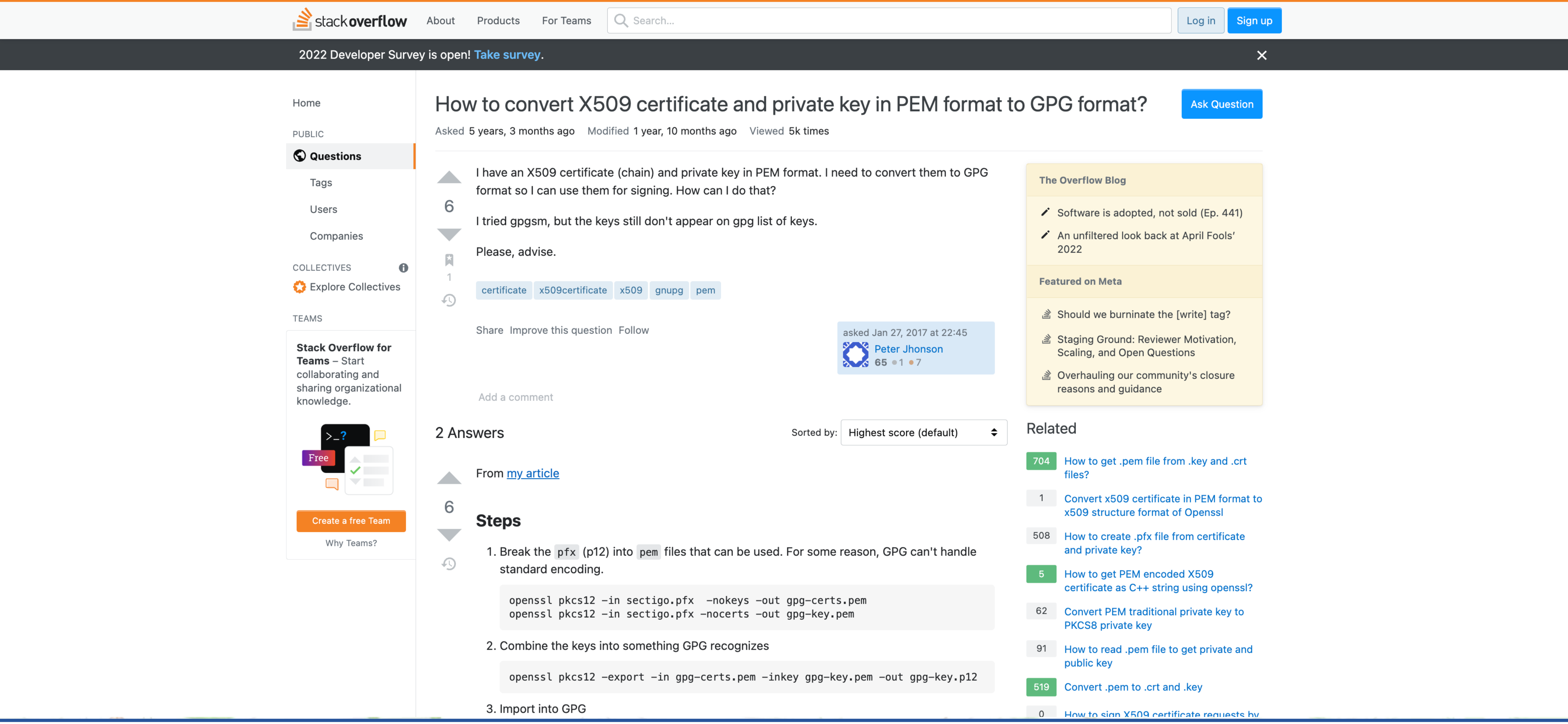
March 7th, 2022 A macOS Monterey 12.3 compatible GPG Suite is now available. Download here!
Please have a look at our troubleshooting guide, should the GPG Mail Upgrader fail to activate GPG Mail.

GPG Suite

One simple package
with everything you need,
to protect your emails and files.

By downloading, you agree to our Terms of Distribution

Includes a 30-day trial of GPG Mail. For continued use of GPG Mail, please purchase a support plan



How to convert X509 certificate and private key in PEM format to GPG format?

Asked 5 years, 3 months ago Modified 1 year, 10 months ago Viewed 5k times

6

I have an X509 certificate (chain) and private key in PEM format. I need to convert them to GPG format so I can use them for signing. How can I do that?

I tried gpgsm, but the keys still don't appear on gpg list of keys.

Please, advise.

certificate x509certificate x509 gnupg pem

Share Improve this question Follow

asked Jan 27, 2017 at 22:45
Peter Jhonson
65 ●1 ●7

Add a comment

2 Answers

Sorted by: Highest score (default)

6

From my article

Steps

1. Break the `pfx` (p12) into `pem` files that can be used. For some reason, GPG can't handle standard encoding.

```
openssl pkcs12 -in sectigo.pfx  -nokeys -out gpg-certs.pem
openssl pkcs12 -in sectigo.pfx -nocerts -out gpg-key.pem
```

2. Combine the keys into something GPG recognizes

```
openssl pkcs12 -export -in gpg-certs.pem -inkey gpg-key.pem -out gpg-key.p12
```

3. Import into GPG

The Overflow Blog

- Software is adopted, not sold (Ep. 441)
- An unfiltered look back at April Fools' 2022

Featured on Meta

- Should we burninate the [write] tag?
- Staging Ground: Reviewer Motivation, Scaling, and Open Questions
- Overhauling our community's closure reasons and guidance

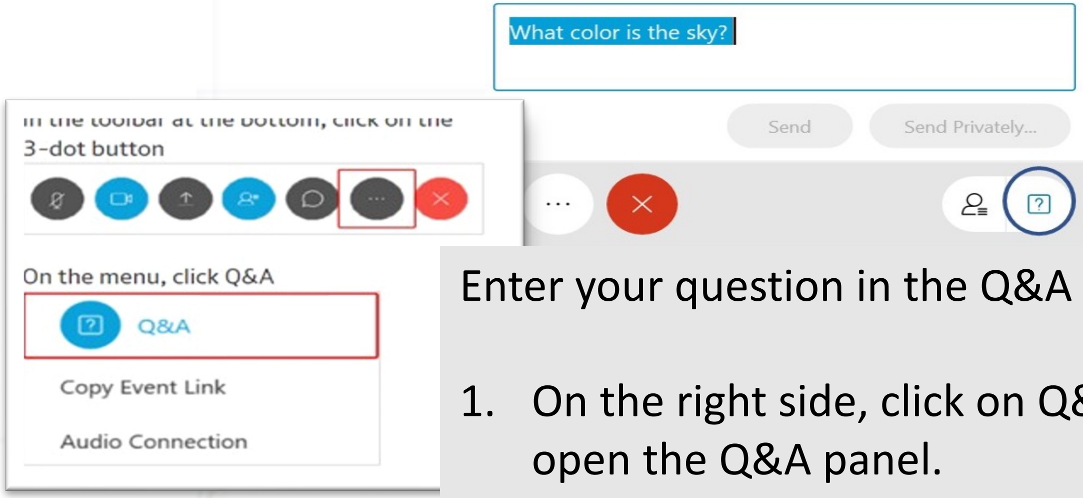
Related

704	How to get .pem file from .key and .crt files?
1	Convert x509 certificate in PEM format to x509 structure format of Openssl
508	How to create .pfx file from certificate and private key?
5	How to get PEM encoded X509 certificate as C++ string using openssl?
62	Convert PEM traditional private key to PKCS8 private key
91	How to read .pem file to get private and public key
519	Convert .pem to .crt and .key
0	How to sign X509 certificate requests by

Thank you!

Genomic Data Security in Electronic Health Records

Moderated Questions and Answers



In the toolbar at the bottom, click on the 3-dot button

On the menu, click Q&A

What color is the sky?

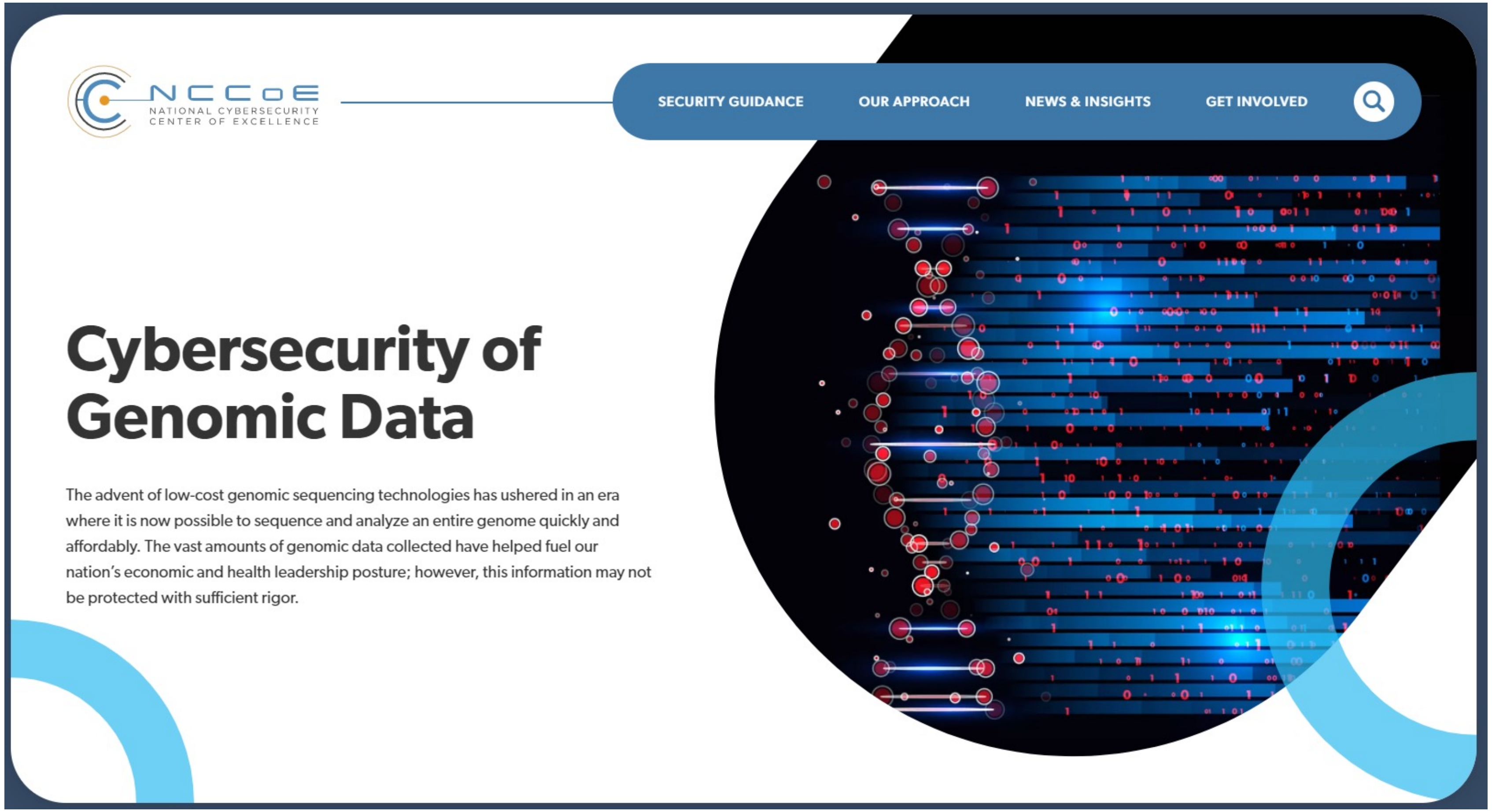
Enter your question in the Q&A panel.

1. On the right side, click on Q&A header to open the Q&A panel.
2. Type in the box **your name, organization and question**.
3. Click send.

Workshop Close Out

Ron Pulivarti, NIST NCCoE

NCCoE Cybersecurity of Genomic Data Project Page



Cybersecurity of Genomic Data

The advent of low-cost genomic sequencing technologies has ushered in an era where it is now possible to sequence and analyze an entire genome quickly and affordably. The vast amounts of genomic data collected have helped fuel our nation's economic and health leadership posture; however, this information may not be protected with sufficient rigor.

https://www.nccoe.nist.gov/projects/cybersecurity-genomic-data

Thank you for joining!

Contribute to the conversation

Email genomic_cybersecurity_nccoe@nist.gov