Global Goods Open Mic Webinar:

OpenFN implementation in LMICs

Global Goods Webinar Series: OpenFN

Security and Scale Considerations for Governments

Learning from an OpenFn implementation by UNICEF and the Thai MoPH

Primero is in 60+ countries.

@Rob, child protection requires partnership—work cuts across organizations and systems.

How can they automate these cross-partner workflows in a secure, stable, and scalable way?

OpenFn is the leading Digital Public Good **for workflow automation**

With **8M** transactions per year
and approximately **40M** records across **40+** countries

we enable secure data integration and interoperability for governments and NGOs worldwide.

Secure, stable, scalable.
We call it *S3* and it's our mantra.

Why does secure come first?

We've been designated a CLASS-I system by UNICEF.

1. Categorization

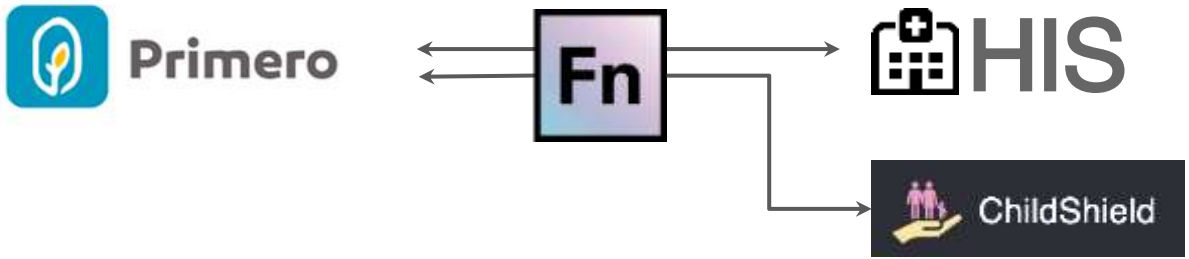
This document describes UNICEF's security requirements for systems classified as Class I. UNICEF recognizes 4 classes of information: Class I - Confidential, Class II - Internal, Class III - Restricted and Class VI - Public. All classes are based on the business value of the information. As such it is the business that drives the data classification.

Class I systems carry the highest classification throughout the organization. This classification is designated for highly sensitive and critical UNICEF ICT assets.

System Classification	Description	Asset Rating		
		Confidentiality	Integrity	Availability
Class I	A system which stores and / or processes confidential information critical to UNICEF operations, individual's safety and / or is directly linked to critical business processes. Unauthorized access may severely impact UNICEF operations / business processes, individual's personal safety and or their identity.	HIGH	HIGH	HIGH

Building integrated child protection systems in Thailand

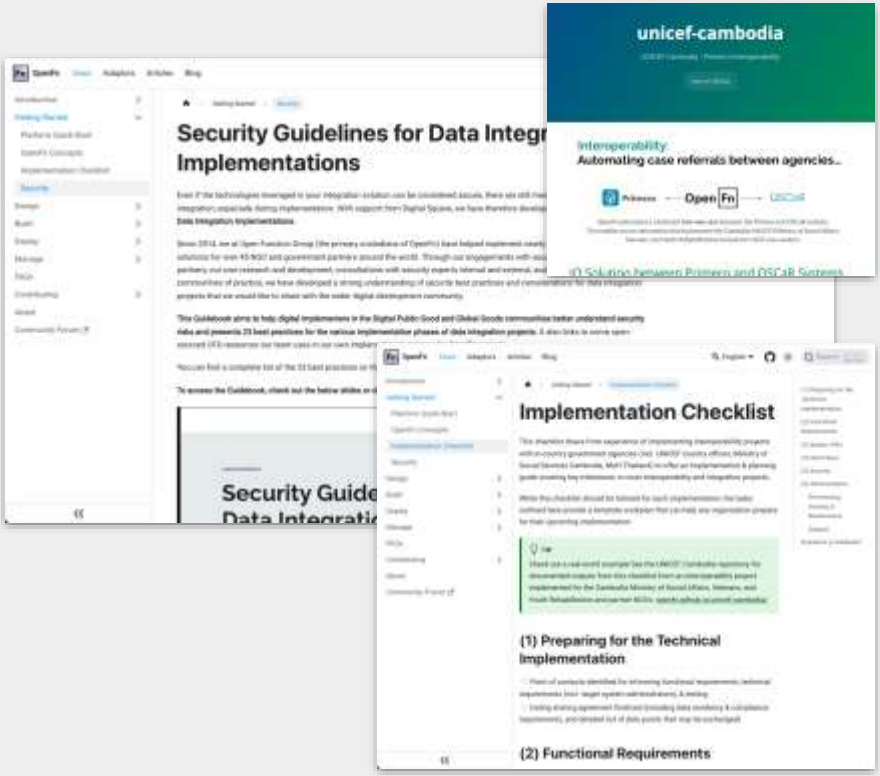
@Rob, what is the MOPH trying to deliver?



How does UNICEF prepare

to implement OpenFn securely?

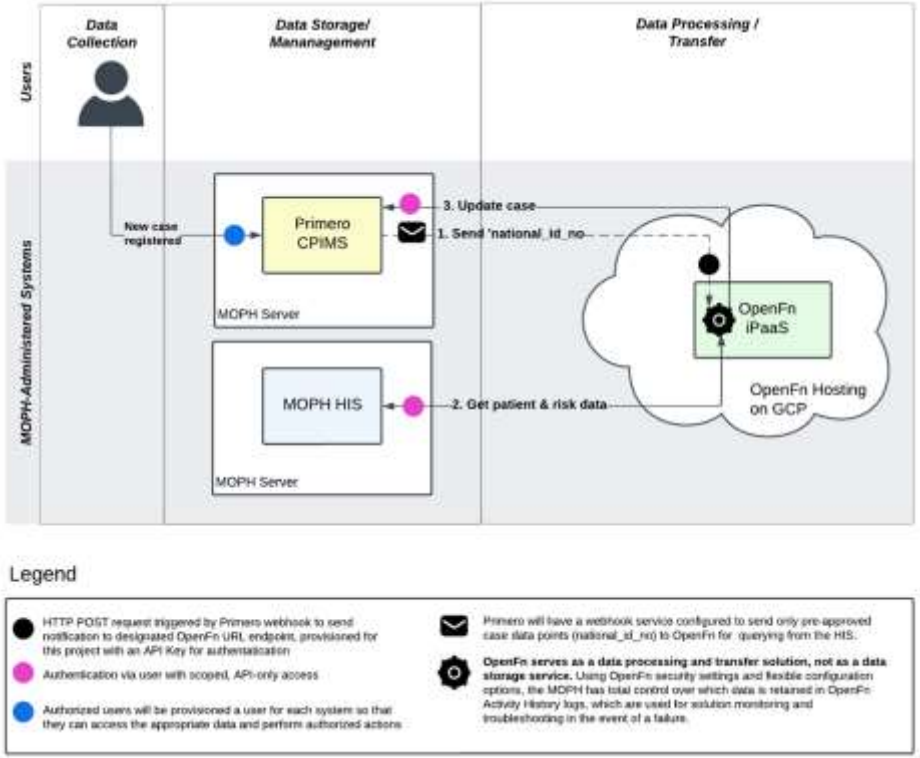
@Aleksa, processes?



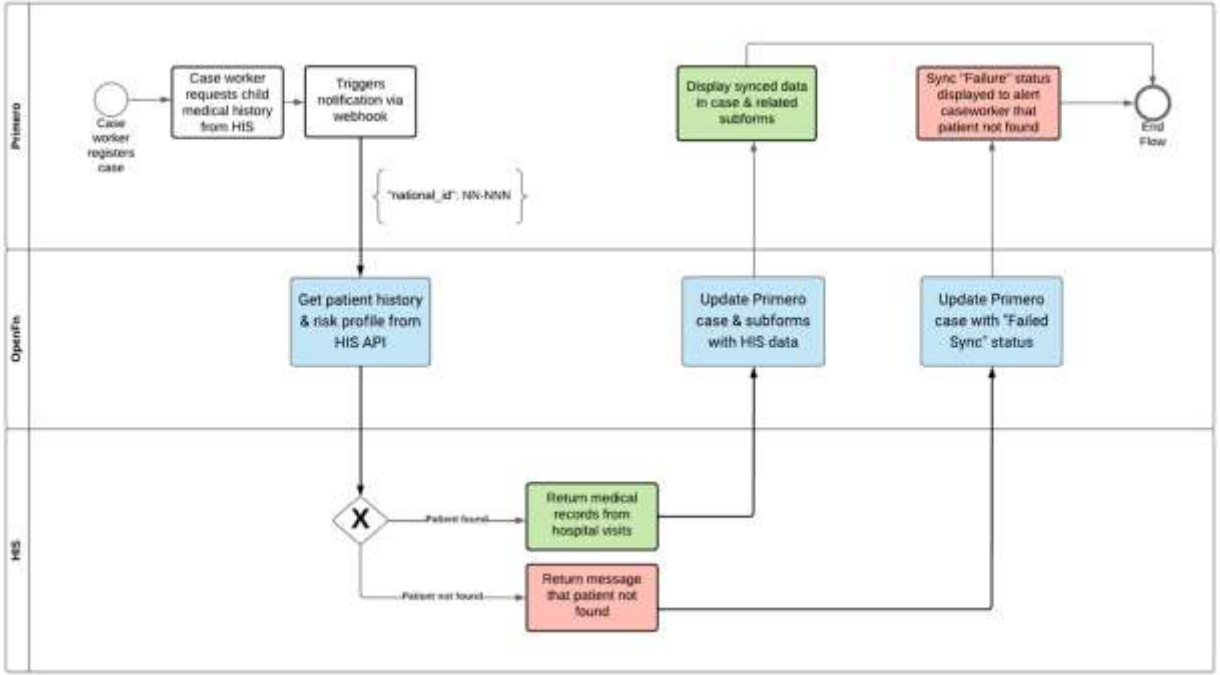
Check out: docs.openfn.org

Thailand MOPH Child Protection Interoperability Solution

The first step is to understand relevant data security requirements and data sharing agreements.



Next comes the workflow definition–driven by program standard processes and aligned with security, legal, and compliance requirements.



@Nino, so far we've discussed ***implementation*** security, because Thailand is using OpenFn as a SaaS… for now.

Can we step back and discuss how Global Goods get built and deployed securely?

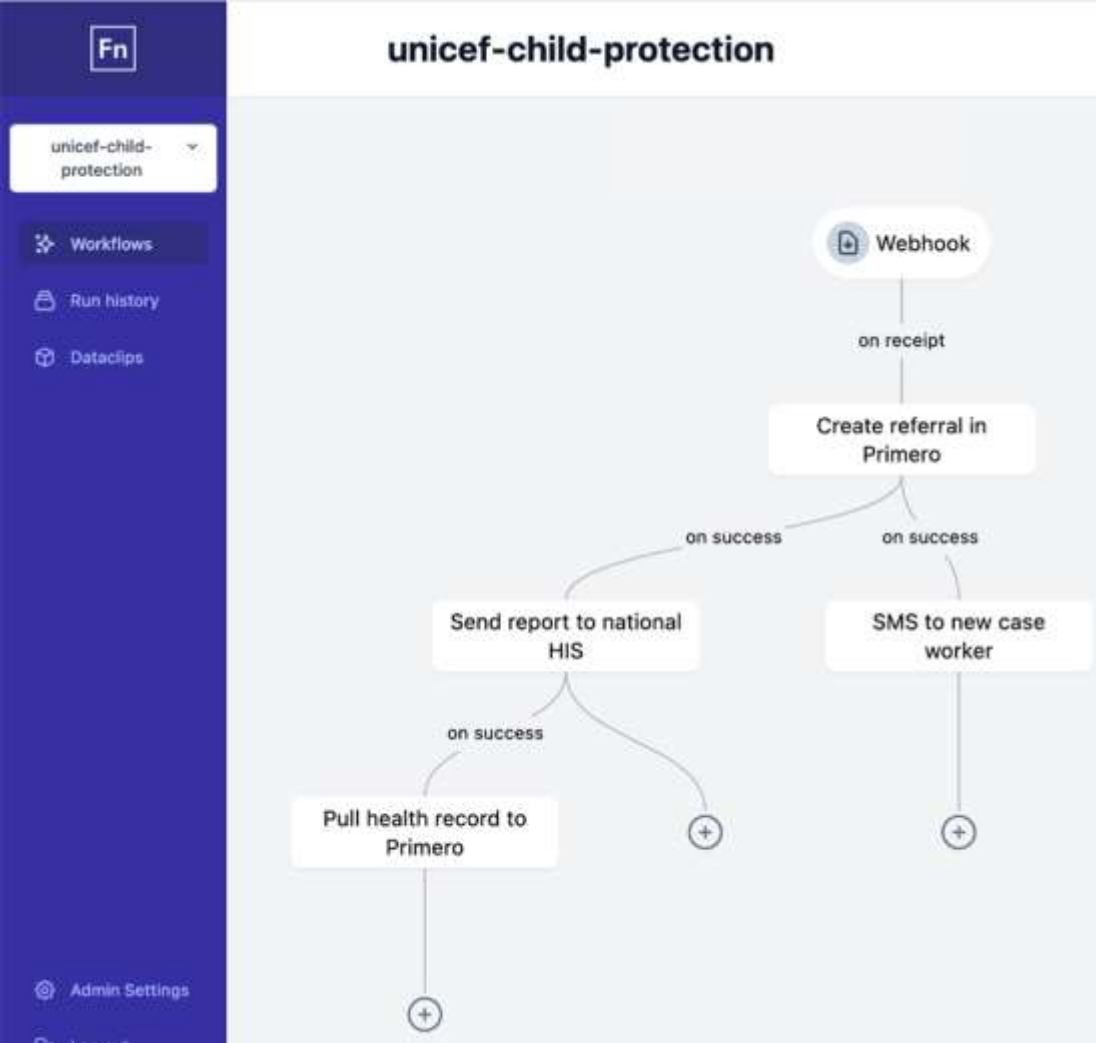
The 8 Principles of Secure Development & Deployment

1. Secure development is everyone's concern
2. Keep your security knowledge up-to-date
3. Produce clean & maintainable code
4. Secure your development environment
5. Protect your code repository
6. Secure the build and deployment pipeline
7. Continually test your security
8. Plan for security flaws

Thailand starts on OpenFn SaaS, so they can focus on the security of their workflows (not infrastructure and deployment) but they're considering local…

@Rob, the MoPH is already on a ***hybrid-deployment*** for Primero. What's that?

They plan to shift to OpenFn ***Lightning*** and are considering local deployment as an option. Let’s talk about what that means.



Open Fn Lightning

coming soon…

The v2 is fully open-source & includes:

- ➔ a new visual workflow builder
- ➔ an enhanced audit trail
- ➔ faster runtimes
- ➔ more powerful dev tools

What should Thailand consider?

As they decide between a hosted DPG, deploying locally, or a hybrid model?

1. How to develop local capacity to take over the deployment?
2. Continue with cloud/managed hosting from OpenFn?
3. Use an unlimited/single-tenant deployment or a standard deployment?
4. Consider data residency?
5. Deploy on their own local servers?
6. Consider maintenance, patch, upgrade support from OpenFn?

And from a security perspective?

@Nino, how do you recommend approaching this question?

Consider the 10 steps:

1. Risk management regime
2. Secure configuration
3. Home and mobile working
4. Incident management
5. Malware prevention
6. Managing user privileges
7. Monitoring
8. Network security
9. Removable media controls
10. User education and awareness

What does this mean for the broader Global Goods community?

It’s **not enough for us to simply *build*** open source software because a secure global good deployed in an insecure manner is not secure.

High quality ***software-delivery-as-a-service*** options for Global Goods are important so that NGOs & govts have the substantive freedom to implement these technologies securely… **on their own terms.**

Learn more

about OpenFn, Primero, and Digital Square and our approach to security.

openfn.org

primero.org

digitalsquare.org