Supporting Innovation through the Evolution of Health IT "Business Standards"

A Together.Health Security Assessment Template (THSA) for Working with Startups

ONC Annual Meeting, Washington, D.C.

January 27th, 2020

The Office of the National Coordinator for Health Information Technology

Breakout Session Panelists

Stephen Konya (Moderator)

Office of the National Coordinator for Health Information Technology

@ONC_HealthIT

@StephenKonya

Hayley Hovious President

Nashville Health Care Council

@NashHCC

Nick Dougherty Managing Director

MassChallenge HealthTech

@MassChallengeHT

@TheMailboxMan

Christina Mazzone Cyber Security Risk Officer

PTC

@PTC

Adam Landman Chief Information and Digital Innovation Officer, Emergency Physician

Brigham and Women’s Hospital

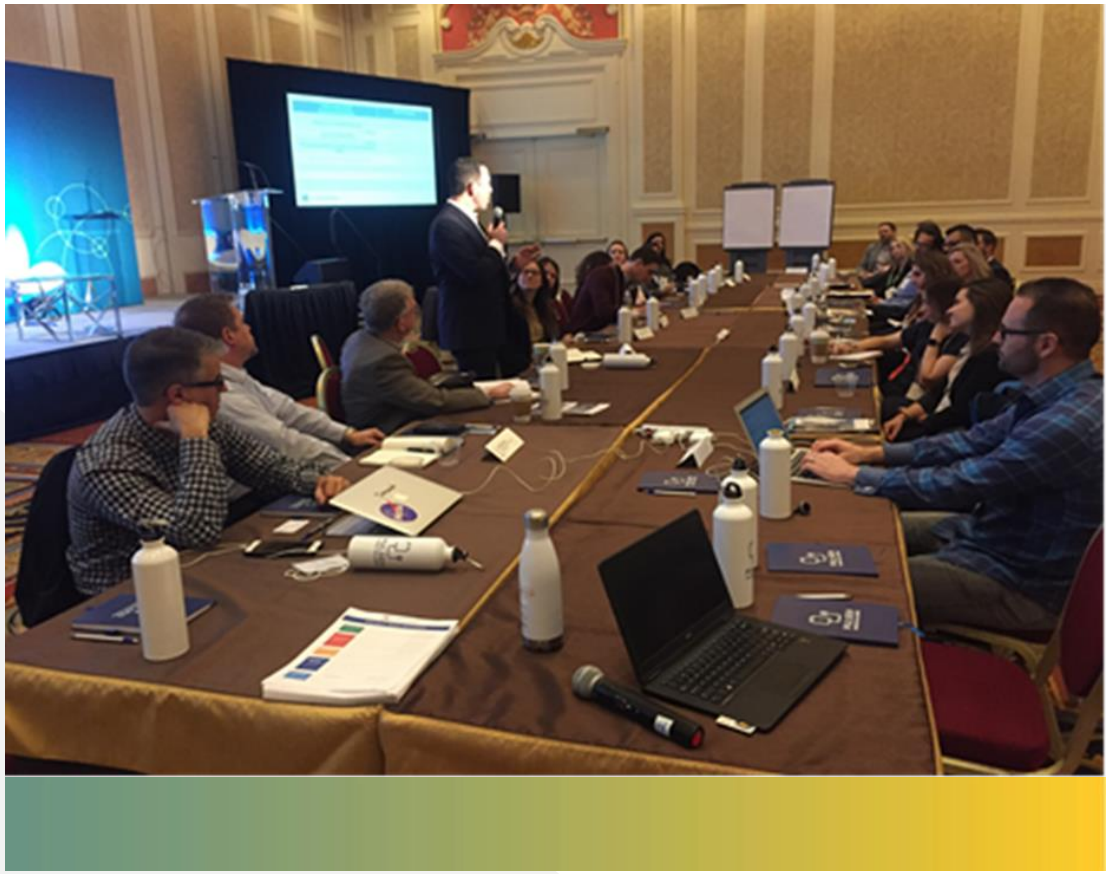
@BrighamWomens

@landmaad

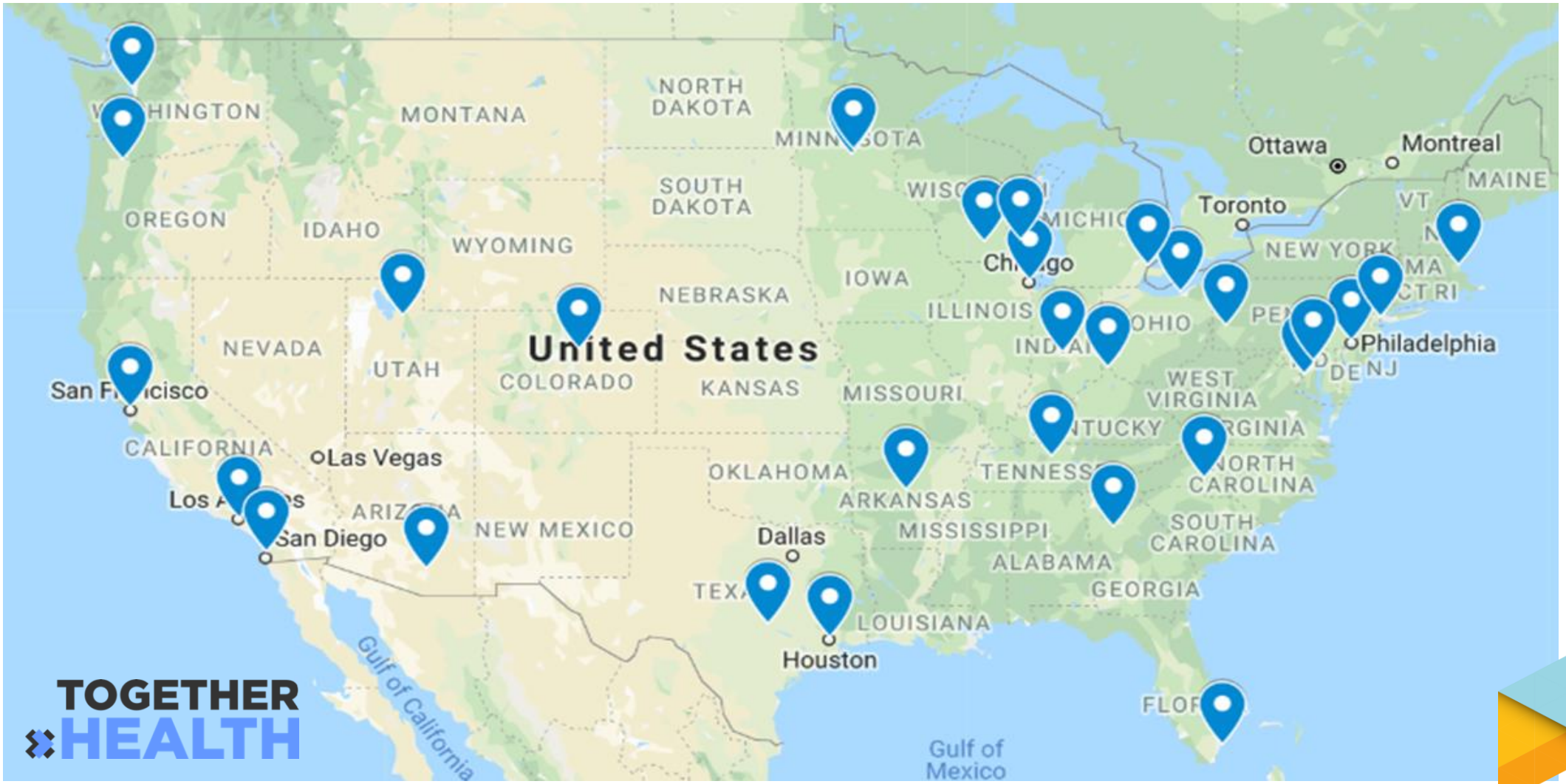
TOGETHER HEALTH

Mission

To bring organizations together, to work collaboratively to **share** best practices, **inform** stakeholders and **leverage** existing resources to fuel the **creation** and **adoption** of digital health innovation.



A National Collaborative of 30+ Regional Innovation Ecosystems



TOGETHER HEALTH

- A national, open collaborative
- 40+ digital health ecosystem partners (incubators, accelerators, associations, networks, etc.)
- 30+ regions / cities represented
- Semi-Annual Gatherings (Spring and Fall Summits)
- Projects launched;
  1. Standardizing security risk assessments
  2. Measuring the ROI of innovation & digital health solutions
  3. Common Curriculum
  4. Mapping the nation's digital health ecosystems

For more information, please visit: www.Together.Health

Building a National Standardized Security Assessment

MASSCHALLENGE HEALTHTECH

MeHI MASSACHUSETTS eHEALTH INSTITUTE

TOGETHER HEALTH

“Piloting with health systems is like being dragged out into the middle of an ocean & being abandoned.”

Startup CEO

“They [startups] don’t understand that we can’t just spin something up just because we are a big system.”

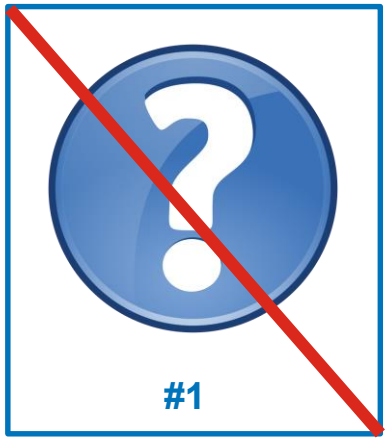
Health System CIO

So What Do We Know…

- We need to mitigate risk and protect patient data.
  - However, Business Associate Agreements and Security Assessments are a barrier to innovation.
    - They create major delays, cost legal and technical capital, and are inconsistent.

OUR CONTRIBUTORS

TOGETHER.HEALTH SECURITY ASSESSMENT (THSA) GOALS



#1

NO NEW QUESTIONS

Use existing questions and frameworks whenever possible

#2

USE THE BEST IN CLASS FOR SECURITY

Don’t just build for healthcare, build for security

#3

SIMPLIFY THE PROCESS

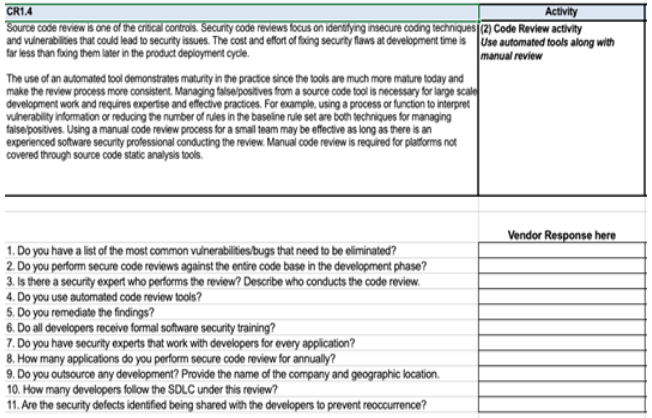
Don’t create a process so burdensome it’s impossible to adopt (i.e. don’t make a slow process slower)

#4

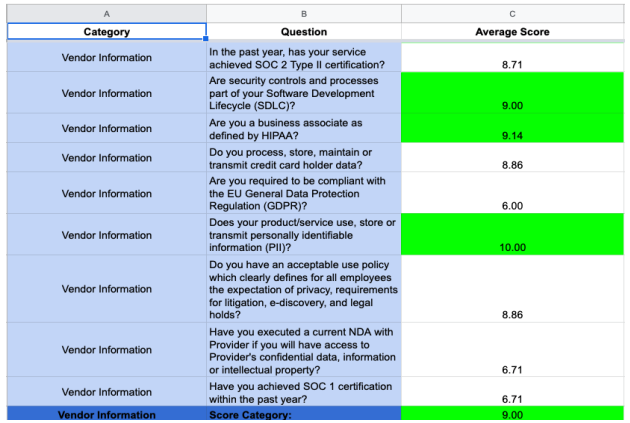
EDUCATE

Help covered entities, vendors, and other health ecosystem stakeholders understand how to prepare for and meet the standards

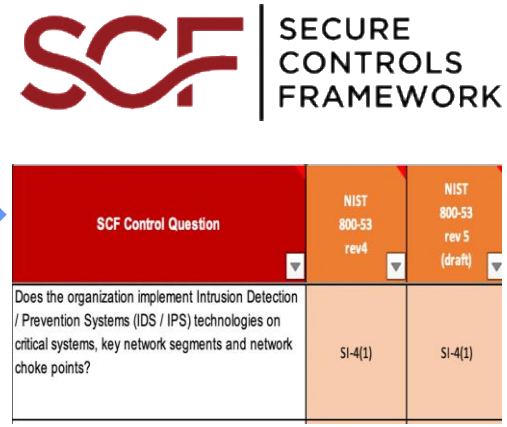
OUR WORK



CR1.4	Activity
Source code review is one of the critical controls. Security code reviews focus on identifying insecure coding techniques and vulnerabilities that could lead to security issues. The cost and effort of fixing security flaws at development time is far less than fixing them later in the product deployment cycle. The use of an automated tool demonstrates maturity in the practice since the tools are much more mature today and make the review process more consistent. Managing false/positives from a source code tool is necessary for large scale development work and requires expertise and effective practices. For example, using a process or function to interpret vulnerability information or reducing the number of rules in the baseline rule set are both techniques for managing false/positives. Using a manual code review process for a small team may be effective as long as there is an experienced software security professional conducting the review. Manual code review is required for platforms not covered through source code static analysis tools.	**(2) Code Review activity** ***Use automated tools along with manual review***
	Vendor Response here
1. Do you have a list of the most common vulnerabilities/bugs that need to be eliminated?	
2. Do you perform secure code reviews against the entire code base in the development phase?	
3. Is there a security expert who performs the review? Describe who conducts the code review.	
4. Do you use automated code review tools?	
5. Do you remediate the findings?	
6. Do all developers receive formal software security training?	
7. Do you have security experts that work with developers for every application?	
8. How many applications do you perform secure code review for annually?	
9. Do you outsource any development? Provide the name of the company and geographic location.	
10. How many developers follow the SDLC under this review?	
11. Are the security defects identified being shared with the developers to prevent reoccurrence?	



	A	B	C
	Category	**Question**	**Average Score**
	Vendor Information	In the past year, has your service achieved SOC 2 Type II certification?	8.71
	Vendor Information	Are security controls and processes part of your Software Development Lifecycle (SDLC)?	9.00
	Vendor Information	Are you a business associate as defined by HIPAA?	9.14
	Vendor Information	Do you process, store, maintain or transmit credit card holder data?	8.86
	Vendor Information	Are you required to be compliant with the EU General Data Protection Regulation (GDPR)?	6.00
	Vendor Information	Does your product/service use, store or transmit personally identifiable information (PII)?	10.00
	Vendor Information	Do you have an acceptable use policy which clearly defines for all employees the expectation of privacy, requirements for litigation, e-discovery, and legal holds?	8.86
	Vendor Information	Have you executed a current NDA with Provider if you will have access to Provider's confidential data, information or intellectual property?	6.71
	Vendor Information	Have you achieved SOC 1 certification within the past year?	6.71
	Vendor Information	**Score Category:**	9.00



SCF Control Question	NIST 800-53 rev4	NIST 800-53 rev 5 (draft)
Does the organization implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points?	SI-4(1)	SI-4(1)

SECURE CONTROLS FRAMEWORK

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

FedRAMP

Collected hundreds of questionnaires from health systems, payors, pharma, and more to build a common question set

Created a common set of questions and tested in multiple focus groups

Mapped tested questions to existing standard (NIST 800-53 and FedRAMP Tailored) using SCF (Secure Controls Framework)

OUR ALPHA-BUILD

Health systems map their existing questionnaires to SCF, an open-source framework that connects best-practice security controls with the top frameworks like HIPAA, NIST 800-53, SOC 2, etc.

SCF SECURE CONTROLS FRAMEWORK

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	SCF Control Question	NIST 800-53 rev4	NIST 800-53 rev 5 (draft)	US FedRAMP [moderate]	HIPAA - HICP Small Practice	HIPAA - HICP Medium Practice	HIPAA - HICP Large Practice
Monitoring	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	Does the organization implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points?	SI-4(1)	SI-4(1)	SI-4(1)	6.S.C	6.M.C	6.M.C 1.L.A

Together.Health updates Security Assessment guidelines based on most commonly mapped questions in SCF

Vendors prepare their solutions to meet Together.Health guidelines

ADOPT the “THSA”
THE TOGETHER.HEALTH SECURITY ASSESSMENT

OUR ASK Bring THSA back to your ecosystem and recruit health systems and vendors to conduct assessment mapping and adopt!

VISIT https://together.health/security-assessment

Breakout Session Panelists

Stephen Konya (Moderator)

Office of the National Coordinator for Health Information Technology

@ONC_HealthIT

@StephenKonya

Hayley Hovious
President

Nashville Health Care Council

@NashHCC

Nick Dougherty
Managing Director

MassChallenge HealthTech

@MassChallengeHT

@TheMailboxMan

Christina Mazzone
Cyber Security Risk Officer

PTC

@PTC

Adam Landman Chief Information and Digital Innovation Officer, Emergency Physician

Brigham and Women’s Hospital

@BrighamWomens

@landmaad