TORCH

Member Benefits

Advocacy

Membership

Education

Services

Resources

Partnerships

TORCH & Affiliates

501(c)3 Affiliate

Foundation
- Scholarships/ stipends
- Grant-funded initiatives
- Scholarship Fund
- R&D

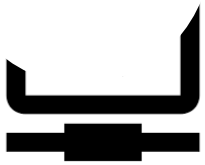
For-profit Subsidiary

TMSI
- Insurance
- Consulting services
- Executive searches
- Interim placement
- Projects, contracts
- Endorsements

TORCH IT Support Services

Email Hosting & Access

- Provide hosted email with full web and client access
- Support email account/ password creation, deletion, resetting, verification and authentication
- Provide anti-spam/anti-virus filtering and firewall protection with automatic updates



VPN/Firewall Administration

- Support and troubleshoot VPN connectivity, firewall and router
- Provide secure VPN client connectivity for remote access, support VPN client connectivity and maintain user accounts
- Provide secure LAN-to-LAN VPN connectivity for transactions b/w the hospital and its business partners and vendors: configure, manage and support L2L VPN connections
- Support, diagnose and troubleshoot the internet

Domain & DNS Management

- Provide up to three file transfer protocol (FTP) account to upload website content
- Provide secure and reliable domain hosting services (DNS management)

Access to Expert Advice, TA & IT Consulting

- Members have access to our highly experienced, professional IT staff for expert advice and general IT consulting and technical assistance on a wide-range of areas. Members can also leverage our vast network of industry partners and professionals to support your various IT needs

Helpdesk Service

- Email hosting, troubleshooting and diagnosing on the network/server level
- Internet connectivity
- VPN client remote access - setup, installation, authentication and support
- LAN-to-LAN VPN tunneling
- FTP account creation, deletion, resetting, configuration, verification and authentication
- Domain and DNS management
- General IT issues

TORCH IT Support Services

Network Support Services

- Email hosting and access
- VPN and firewall administration
- Domain and DNS management
- Access to expert advice, technical assistance and general IT consulting
- Helpdesk service

Security Services

- Security risk assessment (SRA)
- Remote monitoring management (RMM)
- Email encryption service (EES)
- Other services to come!

IT Consulting Services ("SOW"/Special Projects)

- IT consulting services
- IT/technology strategic planning
- Hospital network configuration and planning
- Server management and support
- Special projects or custom support

Security Risk Assessments

Administrative

- Gap analysis of HIPAA security policies and procedures for administrative measures for required and addressable (R&A) administrative specifications
- Interview of key staff interview(s)

Physical

- Walk-thru; assess essential physical security access controls/procedures (ex: doors, locks, cameras, workstations, server room)
- Inspect physical network access – active ports in public spaces
- Identification where e-PHI is stored/housed (ex: servers, work stations, laptops, mobile devices, removable media)

Technical

- Network vulnerability testing – complete external scan of public IP block
- Network assessment – physical setup, configuration analysis of network devices (ex: servers, edge devices, security appliances)
- Wireless security review – scenario testing for access controls and coverage; wireless encryption protocol
- Remote access assessment (RAS) security analysis
- Network diagram and inventory audit of active devices
- Identification of transmission modes of the CEHRT where e-PHI is stored
- Verification of CEHRT usage

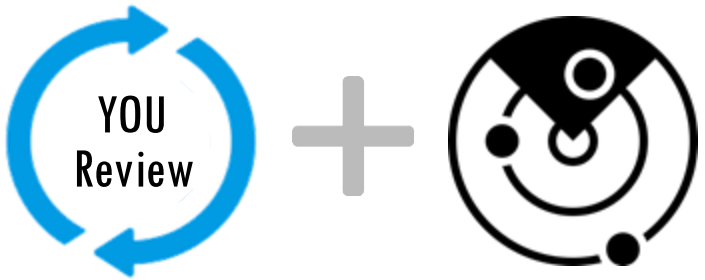
Our Recommendation

Year 1

Full Onsite SRA

Vulnerability Scan
(2/3 times a year)

Year 2



You Review
and Update

Vulnerability Scan
(2/3 times a year)

Year 3

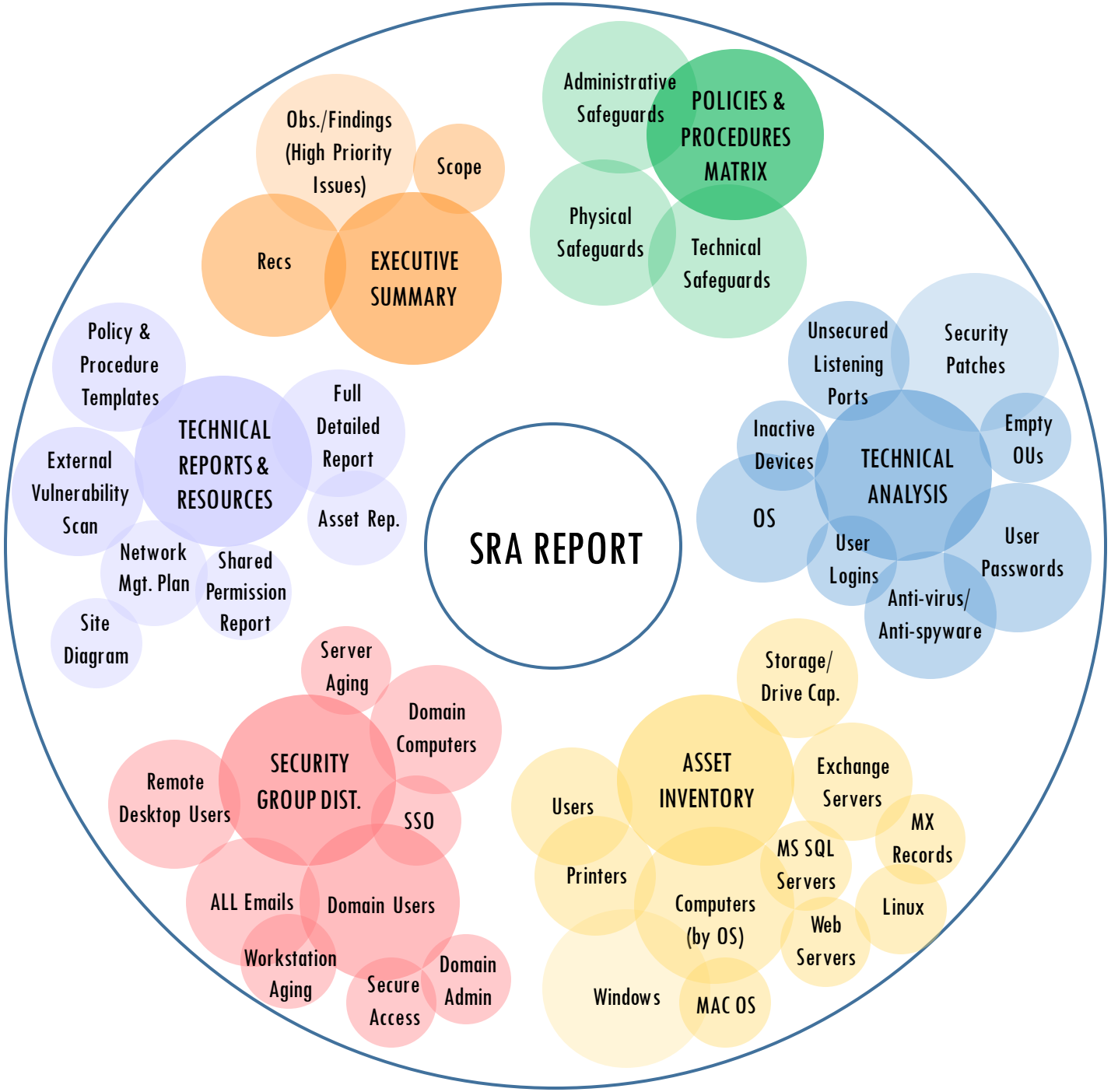
Full Onsite SRA

Vulnerability Scan
(2/3 times a year)

Security Risk Assessments

Results Document

Risk Score



Policy & Procedure Matrix (sample)

	I. ADMINISTRATIVE SAFEGUA...	Policies	Procedures	Observations/Notes
	SECURITY MANAGEMENT PROCESS §164.308(a)(1) Implement policies and procedures in place to prevent, detect, contain and correct security violations			
R	**Risk Analysis** §164.308(a)(1)(ii)(A) **Complete Assessment* Have you conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality and availability of EPHI help by the covered entity?	None in place	None in place	Had completed a risk assessment in the past by GCREC; **REC: hospital to develop written policies or procedures (P&P) to address and comply with the required risk analysis specification**
R	**Risk Management Process** §164.308(a)(1)(ii)(B) **Assess security measures, take corrective action measures as appropriate & document findings* Are security measures in place to ensure confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits?	None in place	None in place	Hospital does assess its security measures, but does not have a specific policy or procedures in place; **REC: hospital to develop written P&P to address and comply with this specification**
	Are there security measures in place that protect against any reasonably anticipated threats or hazards to the security of information?	None in place	✓	Security measures are addressed (collectively) in various existing policies; **REC: hospital to develop specific P&P to incorporate protection against threats or hazards to information**
	Are there security measures in place that protect against any reasonably anticipated uses or disclosures of information that is not permitted or required under subpart E of this part (Subpart E is HIPAA privacy)?	✓	✓	Security measures are addressed in various existing policies (ex: under Acceptable Use Policies); **REC: hospital to develop P&P to incorporate protection re: uses or disclosures of information**
	Are there security measures in place that ensure compliance by its workforce?	✓	✓	Security measures in place under various existing policies; **REC: hospital to incorporate compliance in its risk management process**
	Is your executive leadership and/or management involved in risk management and mitigation decisions? If so, who is responsible?			
R	**Sanction Policy** §164.308(a)(1)(ii)(C) Are appropriate sanction policies (progressive discipline) in place against workforce members who fail to comply with facility's security policies and procedures?			
	Does sanction policy provide examples of violations of policy and procedures?			
R	**Information System Activity Review** §164.308(a)(1)(ii)(D) Are procedures implemented to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports?			

	II. PHYSICAL SAFEGUARDS	Policies	Procedures	Observations/Notes
	FACILITY ACCESS CONTROLS §164.310(a)(1) Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed			
A	**Contingency Operations** §164.310(a)(2)(i) Have you established (and implemented as needed) procedures that allow facility access in support of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency or loss of power?	✓	✓	Hospital has P&P in place that address and comply with this specification
A	**Facility Security Plan** §164.310(a)(2)(ii) Have you implemented policies and procedures to safeguard the facility and the equipment from unauthorized physical access, tampering, and theft?	None in place	None in place	In practice, most locations have proper physical security safeguards in place (locks, cameras, badge readers), but lacking formal, written P&P; **REC: hospital to develop and implement P&P to comply with this addressable specification**
A	**Access Control and Validation Procedures** §164.310(a)(2)(iii) Have you implemented procedures to control and validate a person's access to facilities based on their role/function, including visitor control, and control of access to software programs for testing and revision?	None in place	None in place	In practice, access control and validation measures are in place; entity has Access to Hospital Information System P&P, but procedures are written in the context of new hires and are not inclusive of other cases; **REC: hospital to develop and implement P&P to comply with this addressable specification**
A	**Maintenance Records** §164.310(a)(2)(iv) Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)?			
R	**Workstation Use** §164.310(b) Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI?			
R	**Workstation Security** §164.310(c) Have you implemented physical safeguards for all workstations that access EPHI, to restrict access to authorized users?			

	III. TECHNICAL SAFEGUARDS	Policies	Procedures	Observations/Notes
	Access Control §164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to these persons or software programs that have been granted access rights as specified in §164.308(a)(4)			
R	**Unique User Identification** §164.312(a)(2)(i) Have you assigned a unique name and/or number to identifying and tracking user identity?	None in place	None in place	**REC: hospital to develop and implement P&P to comply with this required specification**
R	**Emergency Access Procedure** §164.312(a)(2)(ii) Have you established (and implemented as needed) procedures for obtaining necessary EPHI during an emergency?	None in place	None in place	**REC: hospital to implement P&P to comply with this required specification**
A	**Automatic Logoff** §164.312(a)(2)(iii) Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? [Is the automatic logoff feature activated on all workstations with access to EPHI?]	None in place	None in place	While in practice this is addressed in the hospital's Acceptable Use Policies, and that the hospital's certified EHR has this capability and is being used, hospital lack a formal P&P to comply with this specification; **REC: formalize P&P to comply**
A	**Encryption and Decryption** §164.312(a)(2)(iv) Have you implemented a mechanism to encrypt and decrypt EPHI?	None in place	None in place	The hospital encrypts its systems and workstations, but lack forma P&P; **REC: hospital to develop P&P to comply**
R	**Audit Controls** §164.312(b) Have you Implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI?	None in place	None in place	**REC: hospital to develop and implement P&P to comply with this required specification**

Remote Monitoring Management

We've partnered with SolarWinds® N-Central RMM to allow you to protect and manage your network and **identify and fix any issue with any end-point from anywhere from a single dashboard** without interrupting the user

It's a proactive approach with automated checks and notifications, coupled with advanced preventative maintenance, so you'll know about problems in your networks early and can fix them quickly

The technology is integrated with best-of-class solutions for 24x7x365 network monitoring

- Have continuous insight into your network
- Ensure optimal uptime, increase productivity, reduce business impact from IT failures and eliminate emergency downtime

Security Risk Assessments

solarwinds
The Power to Manage IT

RMM

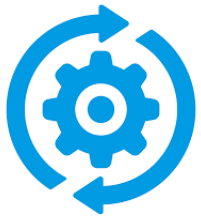
Level Up!

Patch Management

- Ensures all of your Windows servers, PCs and other vital network devices have the most up-to-date security and system patches → help functions optimally, improves reliability and minimize security risks
  - Scheduled preventative maintenance: can be scheduled for deployment, automatically, with confirmation of success or failure
  - Can customize policies to differentiate patch management for the different types of systems in your environment

Remote Monitoring

- 24x& performance monitoring of all your infrastructure to ensure all of your critical network devices are healthy and functioning reliably and optimally
  - Can support Windows, Mac, Linux and most network device manufacturers
  - With N-Central each IT FTE can support up to 400 nodes → allows staff to be more responsive, accurate, proactive, and to focus more on business IT initiatives and less on break-fix services
  - Generate alerts (email, SMS or a ticket) for specific errors to proactively resolve an issue (ex: low disk space on a server) before it becomes a downtime issue



Automation & Scripting

- The system can be used for many pre-defined automation and scripting tasks; 100+ already in the library and more tasks can be created as needed

Security Risk Assessments

solarwinds
The Power to Manage IT

RMM

Level Up!

Managed Anti-virus

Using an integrated Bitdefender anti-virus solution called Gravityzone that's directly managed by the same agent and web console as the rest of your N-Central solution allows you to see the complete health of your systems from one console

Reporting

All data and metadata collected by the system is stored and can be used to generate valuable system reports

- Executive Summary shows availability and resource usage, as well as patch and AV status for a period of time
- Examples of other reports include: device inventory, pricing, antivirus protection, backup integrity, user audits, hardware and software checkups, and more

Remote Access

Connect to a managed device (such as workstations, servers or network devices) directly from the web portal to provide support or access to it as needed; diagnostic and service tasks for workstations can be done w/out interfering with the active use of the machine

John Henderson

jhenderson@torchnet.org

Quang Ngo

quang@torchnet.org

Clay Price

cprice@torchnet.org

Peter Porter

pporter@torchnet.org