IHE SERVICES

Building trust
in eHealth
interoperability

Cybersecurity for Health Information Exchange

IHE–Europe Symposium

Rennes - April 9th, 2019

Charles Parisot, Chair IHE-Services and Principal at InteropEhealth

Priority on Cybersecurity

- Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing any country’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects an organization’s bottom line or the credibility of a government’s institutions. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate, to gain and maintain trust of its citizens or customers.
- Approaching cybersecurity is mainly undertaken as a set of risk management activities. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

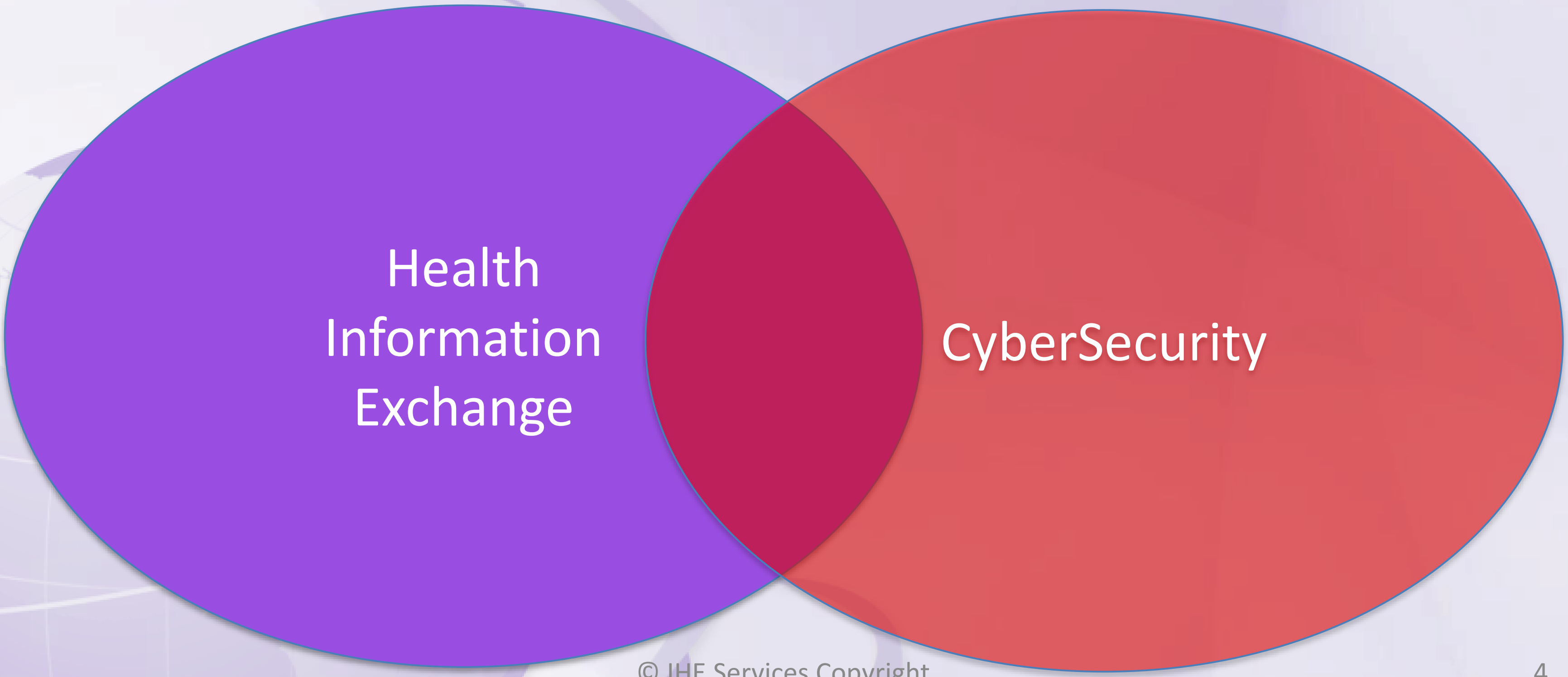
Cybersecurity in Health

- Cybersecurity, a key priority for all entities creating and managing health data. The concerns to remove cyber vulnerabilities apply both within the health delivery organizations such as hospitals, and in the platforms for health information exchange serving the regional, national and cross-border levels.

- For over 10 years IHE has enabled vendors to address security risks for health data exchange in standard-based ways. 2019 is the year where the digital health technology community wants to deliver much stronger Cybersecurity protection than was previously available.

Cyber Security and IHE - Focus

- Cybersecurity is a broad field that covers many aspects of the digital world
- IHE has a clear focus on the exchange of health information



IHE’s Role in Cybersecurity (1)

IHE’s objective -- to facilitate interoperability -- does not put IHE at the center of Cybersecurity Risk Management activities, except on the dimension of protecting health information whilst in transit. This includes:

- Establishing secured communication pathways using cryptographically strong authentication, so that individuals and systems authentication prevents unauthorized access to systems or devices functions
- Encrypting information exchanged between mutually authenticated systems

IHE’s role in Cybersecurity (2)

- Vendors of a wide range of health IT systems and devices products affirm their support for such enhanced Cybersecurity by implementing the relevant IHE profiles and testing their products in the world’s largest health interoperability events – the IHE Connectathons.

- IHE takes this challenge very seriously and now offers its support for an important next step. In 2018, IHE approved a major increment in its security specification step (Audit Trail and Node Authentication Profile (ATNA).

→ Goal is to enables users that want to deploy or use these products to witness the readiness of their technology partners.

IHE's role in Cybersecurity (3)

- IHE IT Infrastructure domain recently published three new Options to the IHE ATNA (Audit Trail and Node Authentication) Profile, it is now easy for vendors to claim compliance to the IETF most current Cybersecurity best practice (BCP 195 – Support of TLS1.2 and stronger cypher suites, and certificate validation).
- With these Options, users and vendors are offered the best balance between flexibility and guaranteed interoperability.
- Testing of these three Cyber protection options at the IHE Connectathons in 2019 has been important:
  - Vendors have confirmed their product readiness and are assessed positively as part of the official IHE Connectathon results.
  - Users had an opportunity to assess that interoperability is achieved with the highest level of Cyber protection available in 2019.
  - For the public authorities they know that a stronger level of cyber protection for health information exchange is now established for policy making.

The three new ATNA Options (1)

1-BCP195 TLS Secure Transport Connection – All TLS versions

- *Higher level of protection for the TLS-protected communication channel by adopting the IETF Best Current Practice (BCP195)*
- *But includes backward compatibility requirements to maintain interoperability with systems that do not support BCP195, by down-grading to TLS Version 1.1 or Version 1.0 and/or cypher suites under specific conditions that are allowed by BCP195.*

➔ *Maintains interoperability as appropriate with existing ATNA implementations.*

2-BCP195 TLS Secure Transport Connection - TLS 1.2 Floor

- *Guaranteed highest level with additional requirement by:*
  - *a) not allowing any TLS protocol lower than TLS 1.2*
  - *b) making mandatory some newer cypher suites that are only recommended in BCP195.*

Both options are compatible with similar options present in Digital Imaging and Communications in Medicine (DICOM), thus ensuring that DICOM transactions tested in IHE Profiles meet the requirements of DICOM Supplement 204 – TLS Security Profiles.

These above two ATNA options are also being included in the IHE international Conformity Assessment program (ISO/IEC 17025 accredited laboratories) for release in January 2019.

The three new ATNA Options (2)

3-FQDN Validation of Server Certificate.

- *Enables the verification that the digital certificates used have been issued by a trusted authority to the fully qualified domain name (FQDN) of the server to which the request or submission has been addressed.*

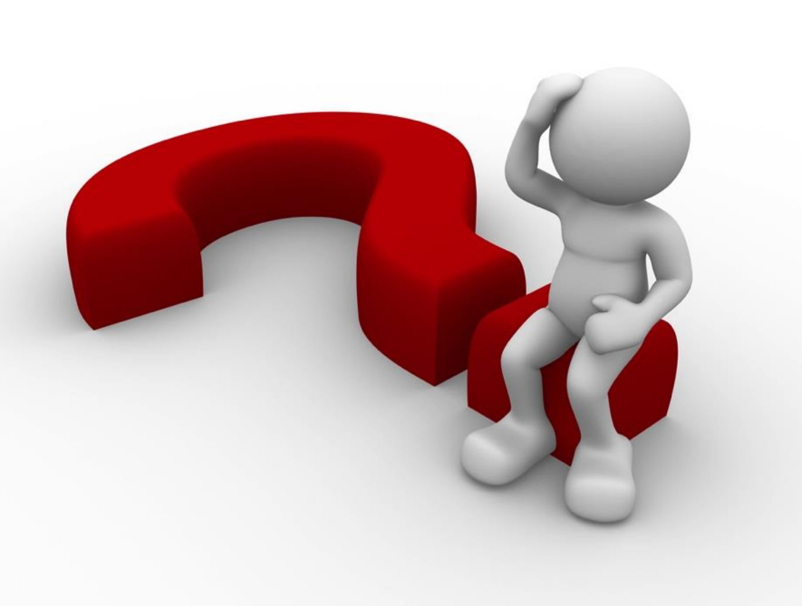
It allows for the prevention of traffic interception by a malicious attacker (man-in-the-middle attacks). These are significantly more dangerous over the public Internet, since more methods exist. Many of these methods are widely known; this is why RFC 6125 requires server certificate verification for all TLS traffic.

Is IHE qualified to address this facet of Cybersecurity?

- IHE is multi-stakeholder, non-profit organization dedicated to improving standards-based interoperability in healthcare (www.ihe.net and www.ihe-Europe.net).
- Security and Privacy are core elements included in that mission. Its mission is to identify and profile standards (widely adopted internationally) for effective interoperability in support of user selected use cases.
- One such profile, widely used world-wide in eHealth, is the current IHE ATNA (Audit Trail and Node Authentication) Profile:
- It is one of the 27 IHE Profiles formally recognized by the European Commission (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_199_R_0011).
- It is listed in the Interoperability Standards Advisory (ISA) publication issued annually by the US Department of Health and Human Services (http://www.healthit.gov/isa/ISA_Document/Appendix_I)
- It is used in a large number of eHealth deployments in Europe, the USA, and around the world.

➔ Health IT applications and devices products from 320 vendors world-wide have been recorded for support of the original ATNA Profile at IHE Connectathons. https://connectathon-results.ihe.net/.

Any Question ?



www.ihe-Europe.net