Recommendations from JWG7 Security Tiger Team

Purpose
A small team of security experts of JWG7 and JWG1 were tasked to provide a recommendation based on the following charter:

1. Consider how best to address security within the remit of the JWG7:
   a. Safe, effective and secure health software and health IT systems, including those incorporating medical devices
   b. Standardization in the area of health informatics and electrical equipment in healthcare where ISO/TC 215 and IEC/SC 62A have identified a need for joint standards development.
2. Consider how to leverage guidance (-2-2, -2-8 & -2-9)
3. What is directed toward the Design & Development "left" side (primary) stakeholders vs. Implementation & use "right" side (primary) stakeholders
4. Timing - 62304 and 80001-1 are both being revised and will be available before any new standard could be completed; so consider how near term updates could be included in these documents and published before any new documents - especially standards - could be completed and published.
5. Impact / use of current projects & documents: 82304-x, 62304, 81001-1, 80001-1 and 80001-2-x
6. Coordination with TC 210 & JWG1
7. Coordination with national initiatives, including in the EU, US and Asia
8. Consider recommendations to address privacy, and especially consent

The recommendations of the JWG7 tiger team is to ensure that risk management focusses equally on safety, security and privacy as each of these are all applicable, and often even mandated by (different) law and regulations, for most products.

The JWG 7 tiger team has identified a structure of 6 major topics that need to be addressed. For each of these topics a high level content and an adequate type of document is proposed considering activities and available standards both within JWG7 and by other standards groups. The results and their relations to the charter elements are summarized in the following table and presented in detail in the remainder of this document.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Document type</th>
<th>Priority</th>
<th>Charter elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Risk Management</td>
<td>Part of ISO 81001</td>
<td></td>
</tr>
<tr>
<td>1a</td>
<td>general</td>
<td>&quot;</td>
<td>High</td>
</tr>
<tr>
<td>1b</td>
<td>for manufacturers</td>
<td>Standard, or part of ISO14971 aligned with JWG1</td>
<td>High</td>
</tr>
<tr>
<td>1c</td>
<td>for operators/users</td>
<td>Part of ISO 80001 and 81001</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Security Requirements</td>
<td>Part of life-cycle standard or ISO 81001</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Consistent set of terms</td>
<td>Part of ISO 81001</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Software and System process requirements</td>
<td>TR with references to existing standards</td>
<td></td>
</tr>
<tr>
<td>4a</td>
<td>for manufacturers</td>
<td>&quot;</td>
<td>High</td>
</tr>
<tr>
<td>4b</td>
<td>for operators/users</td>
<td>&quot;</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Communication between stakeholders</td>
<td>Part of ISO 81001 and/or update of 80001</td>
<td>Medium</td>
</tr>
<tr>
<td>6</td>
<td>Data lifecycle and privacy</td>
<td>&quot;</td>
<td>High</td>
</tr>
</tbody>
</table>
Introduction

Global trends require us to make foundational changes in healthcare as consumers are increasingly engaged in their health with “Do It Yourself Healthcare”. Thanks to global connectivity and rapid development of health devices in the consumer space we are stepping in the era of “Bring Your Own Medical Device”. Value based care is shifting to lower cost settings and homes which also requires new tools used both by caregivers and customers which will further bridge professional and consumer solutions. Both the existing health IT challenges and these new trends in healthcare, require innovative solutions with a more multidisciplinary approach to be able to develop safe, effective and secure Health software and health IT systems, including those incorporating medical devices.

The older functional safety standards did not address the challenges of highly connected “systems-of-systems”. Particularly the arising security issues were not considered at this time in context of safety. Security and Privacy in an open system have become a new factor to be considered in system engineering and safety analysis. ISO/IEC 80001-1 was a first attempt to address these risks related to “systems-of-systems” but new types of solutions and a change in the threat landscape and regulatory space require a different approach.

In this report we try to provide guidance on how to extend risk management beyond safety for the new and upcoming document changes from JWG1 and JWG7. It does not provide all answers but mere guidance on how and where we need to ensure that Safety, Security and Privacy threats are considered in risk analysis and lifecycle management.

1. Security Risk management

1a. General

In this hyper-connected world all stakeholders should recognize and remain vigilant against all potential threats. Medical device manufacturers, government agencies, health care delivery organizations, health care professionals, and patients all share this responsibility.

Security is necessary to protect the safety and privacy functions of a system. We must be aware that Safety, Security and Privacy can influence each other both positively and negatively. One of the challenges for systems is to achieve the different types of requirements specified by safety, security and privacy standards in a lifecycle management. The lifecycle management requirements for security and privacy require quick responses and actions in order to deal with threats evolving continuously, while safety lifecycle management is relatively stable because the causes are random failure and systematic failure only.

Security has to be addressed across the entire lifecycle and it is about any deployed IT or device, regardless whether it is standalone, network capable, wireless or network connected!

Many existing safety and security standards focus on specific scenarios, e.g. some take an isolated device only view, and some might recognize the networked environment, while others have much more an enterprise IT focus and might not sufficiently include the safety aspect. We should recognize the specific focus some of these standards have, identify and where possible fix the gaps they have with the new types of health solutions, e.g.:

- ISO 14971 addresses safety but not security nor privacy, which should be added
- ISO 80001-2-2 does not address operational security or privacy to the extend currently required
• coordinate with other groups developing security standards, on how and where these gaps should be addressed

The next two paragraphs will discuss Security Risk Management from a manufacture and user/operator (HDO) perspective but we should recognize that these lines are blurring as more interconnected multi-vendor systems, cloud based solutions and health applications platforms are being developed and used.

Both the manufacturer and user/operator (HDO) may have to perform activities on the development (left) and operational (right) side of the “Parthenon Image”, and this should be generally address in 81001.

Deploying networked solutions will also force both the manufacturer and user/operator (HDO) to address requirements from several different regulatory and industry domains which have specific security requirements (e.g. eHealth, EMR, Telemedicine, Privacy, Critical Infrastructures, HIPAA Security Rule, SOX, PCI, etc.). Many of these have very similar security requirements so harmonization has a clear benefit.

1b. Security Risk management for Manufacturers

<table>
<thead>
<tr>
<th>What needs to be addressed</th>
<th>Risk management process for security-related risks either as part of another process (e.g. ISO 14971) or as a separate process that links well to risk management for health (e.g. ISO 14971 for medical devices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
</tbody>
</table>
| How shall it be addressed | Considering the ISO TC210 resolution to revise ISO14971 thereby taking into account security:  
1- Reach out to JWG 1  
2- Build a small team with members from JWG 1 & JWG 7  
   a) Establish a risk management architecture that either integrates safety & security or defines interfaces (see also diagram below)  
   b) Discuss consideration of non-medical health software  
   c) Identify possible need for a standard beyond ISO 14971  
   c) Propose further collaboration on risk management  
3 According to the outcomes of 2 possibly establish further risk management standard  
Basis for a separate process might be AAMI TIR 57, Parts of it in IEC62304? |
| Rationale                  | Link to safety is essential as some security-related risks have also an effect on physical/mental health and vice versa |
| Constraints/ Input/Ideas for content | Address each of the types of manufacturers (HDO, regular device manufacture, software developer, apps developer, cloud vendor, etc. that all interlink into a “system”.)  
Key in on the fact that the risk management process itself is basically the same across the board; as organizations become more complex, the amount of work to complete the process increases, but the process can be standardized.  
This does not only apply to the established medical device manufacturers but should also apply to the small app developer. |
|                           | 1. Security monitoring:  
   a. Monitor for incidents / events, e.g. complaints, coordinated vulnerability disclosures, internal problem reports, etc.  
   b. Monitor vendor performance / quality  
   c. Monitor for new vulnerabilities  
   d. Perform Infrastructure testing  
   e. Monitor for changes in the security landscape  
   f. Monitor for changes in the applicable regulatory, legal, user, product and business security requirements |
2. Incident / Event management:
   a. Analyze incident / event
   b. Perform security risk assessment

The following chart is an example showing the similarity of a safety and security risk assessment:

Regulators are calling out to assess security vulnerabilities using both safety and security risk assessments, where a quantitative risk assessment is preferred over qualitative. CVSS is one of the recognized scoring methods in the field of security:

Healthcare Product Security Risk Assessment

Common Vulnerability Scoring System
- Security industry standard for calculating risk
- Simple and direct approach to prioritize risk
- Quantitative and qualitative representation
- Supplements clinical and safety risk metrics
- Consistent view of risk across many sources
- Already available from risk sources like SCA
- Think safety, privacy, financial, operational risk

www.first.org/cvss/calculator/3.0
We should recognize that CVSS does not take into account the impact on the medical device use case (the same vulnerability of the OS might have a very different risk in a respirator or ultrasound scanner).

1c. Security Risk Management for Operators/ Users (Primarily the HDO)

| What needs to be addressed | Risk management process as it applies to the Operator and/or User of technologies (software/devices/systems/etc.) used in medical care. (In essence, the right side of the “Parthenon Image” utilized throughout the JWG7 documents.) Each of the Operators and/or Users should consider the risk management principles to safely and securely utilized the technologies used in medical care. A view of the overall “system” must be part of the technology selection process, the daily use of the technologies, etc.; a view that addresses the entire lifecycle of the use of the technologies. |
| Priority | High |
| How shall it be addressed | 1. Update use of “HDO” only on right side of the “Parthenon” and adapt for use of Operators and/or Users  
2. Standardized risk management process for both the manufacture and Operator and/or User (HDO). While every step of the risk management process should be addressed by the manufacturer and operator/user, but the level of effort, responsibility for implementing, etc. will be different each “entity”. For example: In some cases an “entity” will be doing the design/implementation of security controls, while another “entity” may only be asking the question, “did you implement a security control and how did you do it?”.  
3. Discuss and add examples of successful implementation and/or regulations/standards/etc.  
4. Discuss and add examples of successful implementation of risk management process for Operator and/or User (HDO). These can range from implementation of a formalized risk management process to more simplified SLAs which could be used to ensure security controls addressed & who responsible “entity” would be.  
5. As with notes in section 1b. (Security and Risk Management for Manufacturer), should point to existing standards such as 80001, 27000, 27034-2, 31000, etc.  
6. Follow similar process/notes under section 1b. (Security and Risk Management for Manufacturer)... |

Rationale

Technologies and organizational structures used today and into the future are more complex. Understanding the risk management process, including links with safety and security, is key to providing healthcare now and into the future. Managing risk by addressing both safety and security is the responsibility of the manufacture and Operators and/or Users.

As we rewrite/write new standards, these changes need to be taken into account. Of key importance and possible change to other JWG7 documents, pointing simply to an HDO as the only entity on the right side of the “Parthenon Image” is short sided. If we continue to use the term HDO, we have to adjust definitions to include anyone who has input of output in any workflow, regardless if they are employed by the HDO. The reality is, the right side of the “Parthenon Image” really refers to the Operator and/or User of technologies used in medical care. The Operators and/or Users can be part of an HDO, a patient utilizing the technologies at home, research facilities, etc.
Operators and/or Users need to understand the risk management process, be able to evaluate if appropriate steps have been taken by manufactures, technology providers, etc. to provide safe and secure medical technologies AND be able to develop & implement policies/processes/controls where gaps exist.

### Constraints/Input/Ideas for content

1. Level of effort to update/change HDO to Operator and/or User
2. Complexity of organizations and determining who is responsible to do the risk management process and align with safety & security processes/controls/requirements.
3. For international standards, the common issue of the application/existence of specific country Guidelines/Requirements/Regulations.
4. Availability of good examples of Operator and/or User application of risk management (with inclusion of safety & security concepts included).
5. Similar constraints and notes as listed in section 1b. (Security and Risk Management for Manufacturer)...
6. Standards should recognize the increased complexity of integrated solutions which can consist of a mix of home grown and vendor (cloud) solutions, e.g. the HSPC/Cognitive Medical solution demonstrated at HIMMS’16. Especially when using cloud type solutions and looking at agile / continuous development processes and secondary use, the manufacturer and HDO can have the developer, operator and user roles. Who is responsible for risk assessments might not be as obvious and using SLA’s as the only construct might not be the correct instrument for dealing with appropriate risk management.

The simplistic scenarios below try to capture some of these responsibilities are shown in the tables below.

### Scenarios, a simplistic view:

The tables below are a very simplistic and incomplete view the responsibilities of several stakeholders in different types of solutions. The tables do not contain all possible scenarios and new challenges such as “Bring Your Own Medical Device”, it is intended to trigger discussions on this topic.

Note that not all roles are shown in the tables below, e.g. the patient, family of the patient and other users as they usually will not have a direct responsibility for the security features and controls in development or operational activities. Note that these users will however impose requirements on the system, e.g. how to handle multi-factor authentication for access by patients.

<table>
<thead>
<tr>
<th>Responsible for security REQUIREMENTS LEFT-SIDE HOUSE</th>
<th>Manufacturer (provider of the service Platform and applications)</th>
<th>HDO*</th>
<th>Integrator</th>
<th>Operator</th>
<th>Optional third parties used in infrastructure chain (by Manufacture and/or HDO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-networked Medical Device</td>
<td>Technical</td>
<td>Physical</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Networked Medical Device</td>
<td>Technical</td>
<td>Physical and Network</td>
<td>Network</td>
<td>Network</td>
<td>-</td>
</tr>
<tr>
<td>On Premise Health Software</td>
<td>Technical</td>
<td>Physical and Network</td>
<td>Network</td>
<td>Network</td>
<td>-</td>
</tr>
</tbody>
</table>

Note: The tables above show the responsibilities of different stakeholders in different types of solutions. The tables do not contain all possible scenarios and new challenges such as “Bring Your Own Medical Device”, it is intended to trigger discussions on this topic.
Cloud based Health Software or App
- Technical + Physical + Network + manages third parties
- Physical and Network
- Network
- Network
- Technical + Physical + Network + manages third parties

Remote service
- Technical + Physical + Network + manages third parties
- Physical and Network
- Network
- Network
- Technical + Physical + Network + manages their third parties

Health App’s (combined of dev + app)
- Technical + Physical + Network + manages third parties
- Physical and Network
- Network
- Network
- Technical + Physical + Network + manages their third parties

*) Note that HDO can mandate technical requirements in procurement process; also the HDO manages third parties such as external integrators/operators and infrastructure suppliers; Also note that certain requirements could be defined through local regulations, national infrastructure requirements, etc.

<table>
<thead>
<tr>
<th>Responsible for security MAINTENANCE RIGHT-SIDE HOUSE</th>
<th>Manufacturer</th>
<th>HDO*</th>
<th>Integrator</th>
<th>Operator</th>
<th>Optional third parties used in infrastructure chain (by Manufacture and/or HDO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-networked Medical Device</td>
<td>Yes</td>
<td>(Yes - physical)</td>
<td>(Yes)</td>
<td>(Yes)</td>
<td>-</td>
</tr>
<tr>
<td>Networked Medical Device</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>On Premise Health Software</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Cloud based Health Software</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*) Note that HDO can be responsible for patching certain systems depending on the agreements with the manufacturer; but this could even be outsourced back to the same vendor or another third party.

Overviews like this should demonstrate that security is the responsibility for everyone!

2. Security Requirements to be met by the device/software

<table>
<thead>
<tr>
<th>What needs to be addressed</th>
<th>The manufacturer shall determine the security requirements for the product taking into account legislation and the environment of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
<tr>
<td>How shall it be addressed</td>
<td>Could be a requirement in IEC 82304-1, (IEC 62304), IEC 60601-1, (ISO 81001) Is not worth to have an own standard for this</td>
</tr>
<tr>
<td>Rationale</td>
<td>There are a lot of security requirements out there. They depend on local legislation and may also come from “non-medical” legislation. We cannot provide an up-to-date list of security</td>
</tr>
</tbody>
</table>
requirements. Therefore, it is important to require the manufacturer to have a process available ensuring that all applicable security requirements are captured. This is an important topic with the increasing call for certification!

<table>
<thead>
<tr>
<th>Constraints/Input/Ideas for content</th>
<th>Constraint:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• It is not about how a security requirement is addressed</td>
</tr>
<tr>
<td></td>
<td>• It is not about to define security requirements*</td>
</tr>
<tr>
<td></td>
<td>• It may list sources for security requirements</td>
</tr>
<tr>
<td></td>
<td>• It may expand on how to determine security requirements</td>
</tr>
<tr>
<td></td>
<td>• List a number of standards that could be used as a source for security requirements</td>
</tr>
</tbody>
</table>

*: **JWG7 shall avoid adding new specific security requirements, first check if well-established standards (e.g. 27000 series) suffice.**

Privacy requirements need to be included, especially when developing services but also for remote service.

Sources for requirements are IMDRF, European requirements (e.g. GDPR, MDR)

Potential standard sources for security requirements: 80001-2-2, 80001-2-8, 80001-2-9, 62443 / 27000 series / NIST 800-53

The capabilities as listed in 80001-2-2 are high level requirements, note that these are insufficient as we need to include infrastructure and privacy.

Any list of sources (laws, regulations, standards,..) cannot be exhaustive, the manufacturer has to determine the influence from the specific regulations.

Don’t take if very far and keep it to a couple of bullets explaining what we think that the (high level) requirements are.

Monitoring of sources for security requirements for the whole lifecycle of the device (and data?)

When looking at the overall picture it is not just medical we have to deal with. In many countries one would have to comply with privacy related security requirements, medical data security requirements, national infrastructure requirements, critical infrastructure requirements and requirements stemming from other areas such as SOX, PCI, etc.

We have to explain that when dealing with a networked infrastructure many different systems interconnect and each have multiple sets of requirements that have to be complied with. This is for anyone operating an infrastructure and could be the manufacturer, the HDO, both and of course any sub-contractors that they would use.

Security requirements can originate from regulatory, contractual and business requirements.

Also the user/operator can use these manufacturer processes to determine security requirements for the use of the system.
3. Consistent set of terms

<table>
<thead>
<tr>
<th>What needs to be addressed</th>
<th>Set of terms for security that is consistent with the terms in the “Safety” domain as used by medical device manufacturers: harm, hazardous situation, safety, security, cyber security, vulnerability, threat and exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
</tbody>
</table>
| How shall it be addressed  | Terms should be defined in new standard IEC 81001-1  
Invite JWG 1 for collaboration  
Align with revision of ISO 14971, address potential changes of ISO 14971 terms |
| Rationale                  | This is already part of the JWG 7 work program  
There are already diverging definitions of “harm” and “security” in JWG 7 standards |
| Constraints/In put/Ideas for content | All standards should recognize that:  
• HDO should be expanded to user / operator  
• Manufacturer can also be users / operators  
• Users/operators can be Manufacturers  

As stated in topic 1a, any infrastructure needs to comply with different standards. Perhaps, as part of IEC 81001-1, a table shall be created that compares security-related terms for some commonly used standards, point out the differences.  

We need to ensure we use the proper term “security” vs “cybersecurity”  

Also see [https://www.enisa.europa.eu/publications/definition-of-cybersecurity](https://www.enisa.europa.eu/publications/definition-of-cybersecurity) as a reference and for recommendations|

4. Software and System process requirements

Secure Software Development Life Cycle (SSDLC) processes should be used in development and sustained engineering to address the required process tasks and deliverables. ISO/IEC/IEEE 15288 Systems and software engineering — System lifecycle processes, defines a framework for systems and software engineering. NIST Special Publication 800-160 Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, used this standard to map security activities to each of these processes. The image below, taken from NIST SP800-160, is a good example of an overview of security relevant processes.
4a. Software and System process requirements for Manufacturers

| What needs to be addressed | Throughout the product development lifecycle there are essential activities and considerations for manufacturers to evaluate in order to prevent and remediate security related risks. Mapping these security activities to various phases of development is necessary to illustrate the scope of activities, when they are performed, which are iterative and/or incremental, as well as why they are essential. |
| Priority | High |
| How shall it be addressed | 1. Standardize the list of security related activities for software and system security engineering and point to existing authoritative sources (e.g. ISO/IEC 21827, NIST SP 800-160, OWASP SAMM, and Security by Design with CMMI) in a TR or TS.  
2. Discuss and add an example development process with security activities incorporated along with differences for proprietary software and software of uncertain provenance.  
3. Compile and align software and system design-level requirements with other standards (e.g. ISO 27034 and IEC 62443)  
4. For language-agnostic secure coding standards reference OWASP and SEI CERT  
5. For system hardening standards reference NIST Checklists, DISA STIGs, NSA Guides, and CIS Benchmarks.  
6. Discuss and add an example vulnerability and patch management procedure that includes itemizing system and software components, monitoring vulnerability repositories, prioritizing, testing, deploying, and reporting (e.g. NIST SP 800-40) |
7. Outline security testing methodologies and when they are performed that includes dynamic, static, and manual code analysis, robustness and negative testing, vulnerability scanning, and penetration testing.

8. Define the proper security documentation that is produced out of development (e.g. system architecture and network diagrams showing data flow) that ultimately feed into customer-facing documentation for installation, use, and decommissioning.

9. Evaluate applicability of process under section 1c (Security and Risk Management for Manufacturer) for continuous risk assessment methodology used to prioritizing security defects.

10. Coordinated vulnerability disclosure (ISO/IEC 29147 and 30111)

**Rationale**
Manufacturers are today moving towards more agile and rapid development lifecycles. Security activities require better definition and precision in order to achieve a faster and more nimble development process. Otherwise, developers avoid or abbreviate these security practices. Without clear explanation, Manufacturers may inadvertently focus on late-phase risk identification rather than preventing risk from enter product design in earlier phases.

**Constraints/Input/Ideas for content**

1. Expertise and cost of penetration testing in-house and through contractors for smaller Manufacturers
2. Beyond referencing high-level components of development process such as Design Input, Design Output, Verification, and Validation the more granular variations in software development processes make it challenging to create one comprehensive yet prescriptive placement of security activities that would apply to both agile, v-model, and waterfall methodologies.
3. Note there is a link of the structure of 62304 to the NIST SP800-160 and underlying ISO/IEC standards

---

**4b. Software process requirements for Operator/User (primarily the HDO)**

<table>
<thead>
<tr>
<th>What needs to be addressed</th>
<th>Operators or Users that interact with medical technologies possessing software must understand the practices and considerations necessary to ensure security risks are properly managed during procurement, installation, use, maintenance, and decommissioning.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
</tbody>
</table>

**How shall it be addressed**

1. Outline the security related activities with product lifecycle phases for software and system security operation and maintenance. Point to existing authoritative sources (e.g. ISO 27001, NIST SP 800-53 )
2. Discuss and define the different capabilities with various user types (e.g. consumer, HDO) to manage security
3. Discuss and provide examples of using security documentation provided by Manufacturers and questionnaires for a basis of assessment during procurement through decommissioning
4. Standardize process for customers to report security risks to Manufacturers and monitor for new security risks
5. Establish the responsibility agreement process based on ISO TR 80001-2-6 and discuss updates that further clarify specific components such as application of patches, network monitoring, antivirus updates, managing access with authentication and authorization controls.
### Rationale

Security by design does not completely address security risks for medical technology. Ultimately, there is a shared responsibility between Manufacturers and Operators or Users to ensure that security for medical technology is also appropriately provisioned and maintained. Users and Operators must understand the security capabilities of the system in order to make decisions during procurement or to take action during installation and use such that security risks are avoided or reduced.

A well-defined mechanism for reporting security risks to Manufacturers is critical to ensuring prompt assessment, escalation, resolution, and communication to other Operators and Users. Inversely, Operators and Users should be aware of documentation available that explains the systems security and how to monitor for new security risks.

### Constraints/Input/Ideas for content

- Technical proficiency and capabilities of the Operator or User to perform these tasks especially for consumer-based products
- The complexity of interpreting security notifications from Manufacturers
- Maintaining the same level of standardization for second-hand operators and users

**Standards:** [https://www.enisa.europa.eu/publications/standardisation-for-smes](https://www.enisa.europa.eu/publications/standardisation-for-smes)

### 5. Communication between stakeholders

**What needs to be addressed**

Manufacturers should evaluate what forms of communication are necessary for on security risks and remediation while considering the various sources for this information to be reported from such as Users, Operators, Manufacturer Testing, Security Researchers, or other third-party entities. Establishing a review process and cadence of communication ensure that information provided is accurate and helpful.

**Priority**

Medium

**How shall it be addressed**

1. Standardize mechanisms for Security Researchers, Users, Operators including HDOs to report security risks to Manufacturers
2. Define the various stakeholders in the process for evaluating, developing, and delivering security communications (e.g. regulatory and government agencies, ISAOs, media outlets, Security Researchers, Users, and Operators)
3. Standardize the types of security communications from Manufacturers including security documentation during procurement (e.g. MDS2), security notifications for patches and emerging threats, communication during incident response to all stakeholders
4. Discuss and provide examples for these various types of security communications with common components that describe and prioritize risk
5. Discuss and outline criteria for deciding the communication audience, priority, and timing of communication

**Rationale**

Establishing clear mechanisms for communication between Manufacturers and Operators or Users provide awareness to new and emerging threats, patches or compensating controls that reduce or mitigate security risks, as well as establish best practices and considerations when using medical technology.
### Constraints/Input/Ideas for content

- A dynamic environment where industry groups are rapidly emerging and information sharing is in its infancy
- Ensuring that the proper balance of transparency and focus is achieved in these communications
- Evaluating a more unified representation of security risks such as the Common Vulnerability Scoring System
- Consider recommendation on documents to be shared, e.g. policies, requirements, pen test results, etc. Is this something we push back on want to extend and if so would this be different for products and services?

### 6. Data lifecycle and privacy

| What needs to be addressed | New technologies are leading to an exponential increase in the volume and types of data available. This is particularly applicable to health data, resulting in an unprecedented potential to transform healthcare and enable better healthcare at a lower cost. The move to EHR/MDR, big data analytics and the inclusion of personal health data also raises concerns about:
- Availability (e.g. immediate access to information in emergency situations)
- Interoperability
- Good data stewardship
- Compliance to the many new and upcoming generic and eHealth specific privacy regulations across the globe (e.g. GDPR and HIPAA)

We should recognize that we are dealing with an increasing number of multi-vendor solutions (e.g. clinical decision systems) where data subject information is stored in different formats by different vendors using different storage locations and techniques (e.g. private, public and hybrid cloud solutions).

The ability for researchers to access large sets of data is perceived to advance medicine, persistence of and access to these data sets are key which will require good data stewardship and the recognition of data as a separate asset with its own lifecycle management, not coupled to systems.

The sometimes very restrictive regional requirements related to the collection, use and storage of health data has serious impact on the solutions that can be offered.

Implementing privacy principles without looking at safety (e.g. consent and notification) might introduce safety risks. |
| Priority | High |
| How shall it be addressed | Good guidance on the data lifecycle, the privacy principles and privacy by design in standards could help to build confidence by HDO’s, regulators and patients in health IT solutions and help to establish a more harmonized global approach. |
The documents created by JWG7 should address data lifecycle and the privacy principles (collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation and accountability), mention privacy by design.

The documents created by JWG7 should also recognize that risk management is necessary for safety, security and privacy. They need to provide good rationale to explain the overlap and differences between these three.

These documents should also emphasize areas where privacy can impact safety or security. As an example consent/data access models should recognize safety risks if medical staff is unable to access information during calamities. For instance a consent framework must be able to support that or provide break-glass functionality similar to the security controls.

Interoperability was recently discussed within JWG7 and perceived as an element of availability. Although this positioning is fine it is advised to provide enough guidance on interoperability from a safety, security and privacy perspective.

Especially the framework document should provide guidance on data stewardship to build the recognition for the data lifecycle which is more than “just” privacy. E.g. how to protect gnome data over a lifespan of 50 years and more. Or how to address interoperability across systems and during the data lifespan, which tends to be forever when pertaining health data.

### Rationale

Privacy as a another risk management area should align with safety and security risk management as controls established for privacy might introduce safety concerns.

The uncertainty from organizations on how to implement the security and privacy requirements result in restrictive behavior which impacts the advantage benefits of new types of solutions such as better security, interoperability, quicker innovations and a reduction in cost.

### Constraints/Input/Ideas for content

HDO’s and vendors should have a strategy on the data lifecycle, including risk assessment on data sets for safety, security and privacy. This strategy should further include details on items such as access management, storage (cost), backups, disposition, encryption, data formats, business continuity management, etc. Although most of these requirements are called out through privacy and or security regulation this might not be enough when looking at all stakeholders, types of solutions and cross border issues.

There needs to be a process by which "patients" and "providers" know all IT & devices that interlink and could possibly store privacy/patient data. Tracking this would be part of a MOU/data map/etc. that would be updated as new IT/devices are added or removed from the overarching "system". As part of the terms of use/registration a patient or provider has at any entry point into the overarching "system", the list of IT that processes or stored privacy/patient data would be revealed and approved via electronic signature. In a well-established electronic consent proves patients or providers should be able to "opt out" any portion of the interconnected "system". For my comments here, "provider" means anyone using the systems that is not the patient and "system" refers to all the interconnected hardware/software/etc. Also, for the providers their part of an informed consent is really the signing off that they have need to see or use the privacy/patient data. (This takes us on
another rabbit trail as the providers would already be limited in what they can see/use based on each part of the "system" having its own access lists.

References to standards such as:
- 29100 Information technology - Security techniques - Privacy framework
- 29101 Information technology - Security techniques - Privacy architecture framework
- 17975 Health informatics - Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
- 25237 Health informatics - Pseudonymization
- 27018 Information technology - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Privacy by design strategies:
Strategies by data protection legislation actors


Data Sources | Data Users | Data Uses
--- | --- | ---
Hospital | Hospital | Discharge Summary
Physicians | Physicians | Office Visits
Person/Patient | Person/Patient | Personal Health Record
Labs | Labs | Test Results
Public Health | Public Health | Communicable Disease Reporting
Payer | Payer | Benefit Checking, Claims, Quality Audits
Researchers | Researchers | Research Studies