Meeting report from the workshop on 13th September 2018

Workshop Focus: GDPR Compliance and the International Patient Summary (IPS)

Author: Stephen Kay CEN IPS Project Team Leader

Executive Summary

The CEN IPS Project Team, in cooperation with CEN/TC 251 Working Group 1, brought together a range of experts to consider the General Data Protection Regulation (GDPR) in relation to the International Patient Summary (IPS). The focus of the meeting was to understand better what GDPR compliance means for the International Patient Summary (IPS), both now and in the future, in Europe and beyond.

The current landscape is filled with patient summary initiatives, but the joint work of CEN and HL7 offer the first international standards in this space that could harmonize efforts and thereby provide a consistent and safer exchange through conformant IPS implementations. Although the IPS is not a comprehensive EHR, the IPS work offers a starting point and contribution for a common EHR exchange format.

The IPS is an extract that provides a snapshot of the patient's clinical and non-clinical history, restricted to a standardised core dataset. It is a collection of standardised core data elements, that may or may not be complemented by other data. The IPS comprises a communication, produced and consumed by healthcare providers, in different jurisdictions to facilitate better continuity and coordination of care. The IPS can be implemented in a variety of ways, and although CDA and FHIR examples of use are given, these are not the only means of IPS exchange. The IPS Dataset in the domain model is implementation-independent.

The main task of the workshop on GDPR was to improve the current IPS implementation guidance being prepared for Europe. A secondary, but important task was to consider whether the workshop could produce outputs that might be relevant to extensions of the current IPS scope.

It was noted that separation of the data from the process is key to understanding conformance; the method of linking the data (e.g. defined as constituting the IPS) to processing of that data is essential on how the GDPR is operationalised.

The outputs of the meeting are presented in the 'Conclusions and Observations' of this report. However, it is recognised that GDPR will continue to have implications for the design and implementation of the IPS, and in that sense, this report should be regarded as an interim document, with others to follow over time as both mature.

Meeting report from the workshop on 13th September 2018

Workshop Focus: GDPR Compliance and the International Patient Summary (IPS)

Author: Stephen Kay CEN IPS Project Team Leader

Introduction

The aim of GDPR is to harmonise data protection regulation across the European member states (MS); the meeting attendees appreciated that GDPR was applicable for all business sectors, and that healthcare within Europe was just one consideration amongst many. It would be an added benefit if other countries in and beyond Europe accepted and adopted its principles.

The International Patient Summary Standards are targeted at a global application and were developed exclusively for the healthcare sector. By contrast, GDPR addresses all sectors and is essentially regional in its scope. IPS development is built on the premise that ill health recognises no boundaries and therefore it is logical to produce generic solutions; i.e., better coordination and continuity of care are requirements that reach beyond local, national and regional applications.

GDPR is now European law but it is still maturing and is still susceptible to mis-interpretation. It is therefore possible that these different interpretations lead to different policies and implementations within individual jurisdictions of Europe, hindering interoperable solutions for health data exchange. Note, because of subsidiarity, a country can define additional requirements upon GDPR.

The CEN IPS Standards Project proposal "SA/CEN/GROW/EFTA/000/2015-6 <<< International Patient Summary">>> was funded with eHN and EC approval; the aim of this work was to "participate in the creation of an International Patient Summary specification, at a global level, and turn this into a European Standard, in line with the Guidelines on Minimum/Non-exhaustive Patient Summary Dataset for Electronic Exchange as adopted by the eHN". The CEN IPS project formally began in May 2016 and was targeted for completion in March 2019. It collaborates closely with HL7 in a joint production. The products of CEN IPS, or IPS for short, are the focus of this document.

The strategic goal for IPS is to provide a harmonised specification i.e., a formal, coherent and consistent, specification that builds upon existing European work, contributes to the global activity and benefits the on-going European efforts to establish better continuity and coordination of care.

The tactical aim for IPS is to support this strategy by realising two main objectives:

- 'Participation', recognising that an International Patient Summary necessarily requires working closely with a global community, and
- 'Assurance', requiring that any international deliverable will be both faithful to existing European work and refined such that it is relevant to the rich European context and culture but capable of satisfying emerging requirements.

The first IPS Standard is reaching its first iteration of formal ballot and will become an open International standard but it is currently at a draft stage. The CEN IPS is also tasked with providing guidance for a European implementation of this international standard and therefore seeks to understand how GDPR might affect such implementations. ***The main task of the workshop on GDPR was to improve the current IPS implementation guidance being prepared for Europe.***

Meeting report from the workshop on 13th September 2018

Workshop Focus: GDPR Compliance and the International Patient Summary (IPS)

Author: Stephen Kay CEN IPS Project Team Leader

Format and Outline of IPS/GDPR Workshop

Prior to the workshop, attendees were given:

- Access to the first IPS Standard (i.e., the global domain model which is the draft prEN17269, and is currently out for ballot until the middle of October).
- An extract from the 2nd IPS Standard (focusing on regulation and GDPR) i.e., the DTS17288, the technical specification providing guidance for European implementation of prEN17269.
- An agenda with the focus, set of speakers, suggested questions and expected outputs.

The attendees are named in the appendix.

The morning session comprised an introduction and welcome from Stephen Kay, Vice Chair of CEN/TC251 and CEN IPS Project Team Leader.

A series of presentations from 5 experts from different persuasions was given next; each had 10 minutes and the purpose was to set the scene provide a context and basis for discussion.

The following presentations were given and are available on the CEN/TC251 website:

a.	GDPR: Present state:	Matthias Pocs, Convenor of CEN/TC251-WG1
b.	Sharing Clinical documents:	Stéphane Spahni, HUG & IHE-Europe co-chair
c.	Status of the IPS standards:	Giorgio Cangioli, Hl7 International
d.	HL7 GDPR on FHIR:	Prof. Alexander Mense, HL7 (Austria)
e.	H2020 SHiELD Overview:	Ed Conley, AIMES

After lunch, the workshop took the form of a facilitated group discussion, considering the IPS Use Case and the IPS Scenarios.

Meeting report from the workshop on 13th September 2018

Workshop Focus: GDPR Compliance and the International Patient Summary (IPS)

Author: Stephen Kay CEN IPS Project Team Leader

Presentation Summaries

The actual slide presentations are part of this report but a brief summary of each is given here:

GDPR: Present state: Matthias Pocs, Convenor of CEN/TC251-WG1

- Data Protection Principles listed and applied to healthcare
  - Lawfulness including 'consent'
  - Data must be accurate (and regularly updated)
  - Purpose Limitation… data processed for specified and non-incompatible purposes
  - Data Security and appropriate levels, e.g. role-based access control
  - Data Subject Rights
  - Data Portability
  - Data Minimisation
  - Responsibility
- New Risk based approach
- New Accountability… controllers must be able to demonstrate compliance
- New Certification
- New Data Protection by Design, e.g. design-time documentation and changes to design as well as operational implementations.

Sharing Clinical documents: Stéphane Spahni, HUG & IHE-Europe co-chair

- National Contact point for cross-border exchange supporting reliable exchange of information between countries (bi-directional gateway in each country)
  - Including transcoding and translation of documents
  - Without intervening into national infrastructure
  - Through the establishment of a circle of trust between the countries
- Patient Information Notice provides detailed privacy information for the patient
  - Information consent and personal data protection obtained before care takes place
  - Traceability and Accountability by Audit Trail and Node Authentication (ATNA) Logs at both Country A and Country B addresses who is accessing 'what' and 'when'.

Meeting report from the workshop on 13th September 2018

Workshop Focus: GDPR Compliance and the International Patient Summary (IPS)

Author: Stephen Kay CEN IPS Project Team Leader

Status of the IPS standards: Giorgio Cangioli, Hl7 International

- What is the IPS? Definition from SOURCE: ISO/TR 12773-1:2009 (en) Business requirements for health summary records — Part 1: Requirements].
- Fundamentally the IPS is structured as a document with required and optional sections, that can be extended to meet specific needs. The IPS is characterised as being Minimal and non-exhaustive, specialty-agnostic, condition-independent, implementation-independent yet still clinically relevant.
- It is not an EHR
- The IPS Project is a collaboration between CEN TC251 and HL7 and delivers 4 standards, two from CEN IPS and 2 from HL7 IPS project teams.
- Balloting and draft use of the 4 standards; first iteration expected to be complete by 2020

HL7 GDPR on FHIR: Prof. Alexander Mense, HL7 (Austria)

- HL7 Work in progress on FHIR Security and Privacy artefacts
- Components supporting the implementation of security and privacy include CDA elements and FHIR components, e.g. resources, guidance and vocabulary
- FHIR resources include 'consent', 'provenance', Audit event based on IHE-ATNA
- Implementation Guidance include Security Labels attached to a resource or bundle that provide security metadata about context and purpose of use and data sensitivity
- The general principles are focused on FHIR/ technical level, requiring no specific polices or making no legal assumptions.
- Creating a Whitepaper and the work in progress maps the requirements of GDPR to the existing components, identifying gaps and provide simple examples.

H2020 SHiELD Overview: Ed Conley, AIMES

- The SHIELD project is a H2020 Project focused on European Security in Health Data Exchange
- It proposes an open and extendable security architecture (OpenNCP) enhanced with security mechanisms, privacy-by-design modelling and analysis tools.
- Its use case is the storage and exchange of health data across European Borders.
- It considers the idea of transforming a national PS to the IPS and then using the epSOS based architecture to support the secure exchange
- It has 3 use cases: of which 'Break Glass' (unscheduled emergency of Stroke) is close to the primary IPS scenario, as-is 'Surgical Intervention' requiring a shared medical history and is a scheduled cross-border use case.
- SHiELD has a number of high-tech solutions to make the GDPR compliance less onerous

Conclusion and Observations

The following items form the main outputs of the workshop (Note, these are ordered according to the given extract of DTS17288, but add and complement rather than replicate what has already been written in the current version of that document):

1. Data Protection by Design:
    a. A new feature of GDPR, it brings attention to Data Protection by Design, e.g. design-time documentation and changes to design as well as operational implementations. This has direct relevance for writing and maintaining a standard intended for implementation. This may require considerations for standardised processes for "effectiveness" and "integration" of privacy design strategies. Further guidance is given in GDPR Article 25 and its Recital 78.
    b. Purpose Limitation is a related requirement in that care must be taken to be precise in a Standard's normative sections. Whereas this is obviously good practice for any SDO, these requirements strengthen the need; in particular, attention must be given to ensure that the personal data cannot be processed for both specified and non-incompatible purposes.
        - The distinction between use case and use case scenarios and their level of detail is important with respect to 'purpose limitation' (see the Minimisation principle discussion below.)
        - In order to be able to enforce minimisation and purpose limitation by automated means, this may require creating an additional data field for "coded" processing purposes (e.g. 0 = clinical care, 1 = administration of care, 2 = clinical research, 3 = patient control, etc.).
    c. Separation of the data (as in prEN17269) from the implementation (and associated guidance, e.g. DTS17288) is seen as a key design feature. The approach taken by CEN IPS, enables the domain model (IPS Dataset) to be implementation-independent, facilitating harmonisation and encouraging wide-spread use. Critically, it also focuses attention on the quality of the data, in light of the availability and accuracy principles, and permits the legal view of it as a 'file', minimising impact of GDPR yet using its principles to ensure better healthcare.
    d. Considerations should be given to the element of pseudonymisation included in the new legal obligation. This may require the creation of a pseudonymised variant of the IPS Dataset model, to help controllers implement GDPR Article 25.
2. Information and Consent:
    a. Consent is of the legal basis that makes sharing of (health) data possible. It's important to separate the consent to the treatment (in most countries this is handled by other health related legislation) from the sharing of the data. The KONFIDO project has created use cases which are compliant to the GDPR. The

OpenNCP of SHiELD indicate one way of sharing that is GDPR compliant. The activity of sharing (health) data cross borders brings GDPR into the discussion; not the IPS Dataset itself, rather the quality of data that populates it when it is exchanged.

b. Given the fact that IPS is constructed of discrete data elements, based on a modular design, the IPS gives the opportunity to see whether there are different GDPR requirements for each 'building block'; conversely, it is possible to consider the IPS as a single communication. The former lends itself towards security tagging based upon the sensitiveness of a specific data element and the degree of consent. This may be provided by the HL7 security labelling, but this is still a work in progress at this point in time vis a vis the mapping of such labels against GDPR. The alternative to treating the IPS Snapshot as a single artefact is for optional items in the IPS dataset to dropped from the exchange so as to avoid some of the difficulties raised by non-legitimate user's inferring something from missing data.
c. The Patient Information Notice (PIN) is something that should be used in conjunction with the IPS as it requires Information consent and personal data protection obtained before care takes place; however, it was noted that the template would be customised by local authorities, and the IPS may be constructed from a variety of sources, which might pose inconsistencies. For example, the eHDSI ITF gathers input on PIN implementation.[1]
d. It was noted that the IPS use case, in part because a core dataset was being used that was intended to be relevant in all scenarios and also implementation-independent, did not exercise the GDPR to a great extent (arguably a good thing from the SDO/designers' perspective) as GDPR was more about use and activities and so little was likely to be changed to the 'file'. However, if the security tags became the way of providing 'Privacy by Design' these would have to be included in future iterations of the IPS dataset.
e. 'Access' as part of information governance is often controlled with schemes such as Role Based Access Control schemes (RBAC). In RBAC, 'roles' are problematic as these are not agreed or standardised - apart from individual cases[2] - across Europe (and certainly not on a global scale), there may be a need to map the different roles in play to allow legitimate use with respect to consent and access, related to the activities.

[1] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Gather+input+on+PIN+Implementation+in+MS , last update 15 October 2018.

[2] Such as the OpenNCP case: according to epSOS architecture (see epSOS deliverable D3.A.7 v1.1), roles includes DOCTOR, PHARMACIST or ADMINISTRATIVE_STAFF and their functions (POE-006, PRD-003, PRD-004, PRD-005, PRD-006, PRD-010, PRD-016, PPD-032, PPD-033, PPD-046). However, as there is no agreement for what a "doctor" can do across Europe, those roles agreggate a variety of those functions.

3. Minimisation:
    a. This is assumed to be covered in that IPS is foremost a Summary. However, the Use case is intended for the purpose of improving continuity of care (essentially a clinical purpose) and improving Coordination of Care (essentially a non-clinical task). This dual purpose means that the IPS Dataset carries both administrative and clinical data elements. This may require the reduction in the amount of data exchanged dependent on which one of the purposes is intended.
    b. The scope of the IPS standard currently excludes specifics on how a PS is constructed (i.e., IPS Production) and accessed (i.e., IPS Consumption). Consequently, the impact of GDPR is minimised for the Domain model and is more relevant to the Implementation guide.
    c. 'Consent details' and 'Patient Information Notices' are not a part of the IPS Specification, but given that a defining property of IPS is the sharing of both personal data and person identifiable data, provision in an implementation must be made.
    d. An IPS may or may not persist after presentation to the attending clinician at the point of care (depending on jurisdictional requirements and organisational policies) but an audit of its use (without clinical content being retained) will be necessary both in the producing and consuming systems to show transparency.
4. Accuracy
    a. Data must be accurate and regularly updated. Different jurisdictions have different rules for storage of an IPS. Some prohibit the *update* of any IPS, considering the IPS as a one-off snapshot and requiring a new IPS to be generated on the fly.
    b. Although construction of the IPS is beyond the scope of the current standards, it should be noted that the IPS might be generated from multiple heterogenous sources and the possibilities of duplicate and misplaced data will exist until formal agreement is reached upon the classification of document types and their associated components.
    c. IPS is not intended to be a comprehensive EHR; EHR Systems design should deal with much of the GDPR requirement and, in many cases, demands of GDPR on IPS are addressed by the general principles regarding any health data exchange.
    d. The issue of relevance and the quantity of data actually exchanged can be considered, in part, with reference to the presentation layer of systems which should not be confused with the exchange itself.

5. Portability
    a. The IPS standards dataset needs to be worked on until it is possible to write an "IPS file", which software from another vendor could read and use seamlessly. The current implementation guides under preparation will attempt to bring the IPS standards family that far. This requires that decisions need to be made regarding the coding schemes used for coded entries.
    b. The possible different types of IPS implementations (e.g. citizen mediated, NCP infrastructure, portals etc.) will be different mechanisms and each will need to consider how relevant GDPR principles are for their compliance.
6. Risk Assessment
    a. A new requirement; this should be included within the European implementation Guide, DTS17288 as it takes place in an operational context. Note, it is not in the current version.
    b. Disease and patient register guidelines that are under construction need to consider the impact of GDPR, eIDAS, and NISD; an action taken is to consider the implications of these for the IPS implementation guide.

Full compliance with GDPR requirements is still a work in progress, but it is critical that new revisions of the IPS Standards, and the increasing clarity of the regulation, are constantly kept in step. IPS provides a base standard which can influence the whole subject of health data exchange within the healthcare domain.

Given that potential, it is critical that IPS implementations do no harm. It is very important to ensure that the IPS standards, and their associated conformant implementations, are considered trustworthy and safe; it is important and necessary that they also demonstrate these qualities. Such an outcome will gain and keep the confidence of the stakeholders and thereby the IPS will be accepted and adopted as good, leading practice that will benefit all people and organisations alike.

Acknowledgements

The IPS project team wishes to thank all the attendees for their participation. The different disciplines, especially the legal and technical ones, provided valuable perspectives that complemented each other well and contributed to the overall success of the workshop.

My thanks go to Matthias Pocs, convenor of CEN/TC251 Working Group 1, who presented and helped organise the meeting; he also contributed to the final report. My sincere thanks too, to the other invited speakers: Stéphane Spahni, Giorgio Cangioli, Alexander Mense, and Ed Conley.

Finally, my thanks go to my IPS Project Team members, Shirin Golyardi, Giorgio Cangioli, Karima Bourquard and Vincent van Pelt for their contributions to this final IPS/GDPR report.

Appendix: Attendee List and mode of participation

The attendees name, affiliation and attendance detail either in person or by phone

(October 2014)

Assignment of Exploitation Rights

Including the 'List of Participants'

Date(s) of meeting: 2018-09-13

Place of meeting: CEN-CENELEC meeting centre, Brussels

*** CEN/TC251 Health informatics / IPS project workshop on IPS-GDPR**

Secretary: Shirin Golyardi **NSB: NEN**

Foreword **

In order to secure the legal protection of the documents elaborated collectively by the participants (i.e. delegates of CEN Members and other experts in CEN's standardization work), you are asked to accept the following terms and conditions for the assignment of the exploitation rights of your contributions to European standardization by signing the list of participants. For convenience of use, this statement of assignment may also be used as the list of participants for meetings.

EXPLOITATION RIGHTS ASSIGNMENT STATEMENT

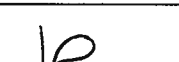
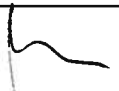
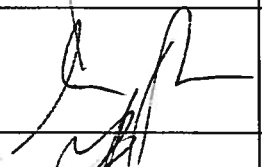
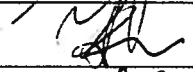
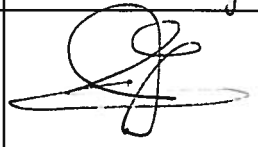
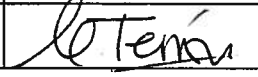
1. In the framework of the Berne Convention for the protection of literary and artistic works:
   (a) By signing the attached list, I assign solely, exclusively and irrevocably to the European Committee for Standardization (CEN) for the benefit of its national Members the exploitation rights of my intellectual contributions, as are reproduced in the publications resulting from the technical deliverables of CEN, as defined in paragraph 1.2 of CEN/CENELEC Internal Regulations Part 2.
   (b) I agree that CEN deliverables containing all or part of my contributions may be published without mention of my name.
   (c) For the total duration provided for by law, I accept that exploitation will take place without mention of my name.
   (d) I accept that this assignment does not preclude me from continuing to exploit my own copyrightable contribution for my own purposes, provided that such exploitation does not adversely affect the exploitation of the publications specified in (a) above.
2. Should I offer intellectual contributions for which I do not personally hold the copyright, I undertake to do the necessary to declare this to the appropriate CEN officer with regard to this Statement, or to any other relevant CEN body and to name the holder of the copyright if known to me, in view of securing the assignment of its exploitation rights to CEN.
3. The assigned exploitation rights are granted free of charge worldwide and cover all languages and all forms of exploitation known at present, in particular and non-restrictively: publication, reproduction and adaptation by all means and all graphical support systems, by print, press, photocopy, microfilms, and via all magnetic, electronic and numerical support systems, memory cards, CD-ROMs, DVDs, Blu-Rays, films, photographs, slides, teledistribution, cable, satellite, web applications and on-line document servers and networks, distribution, sub-distribution, translation, derive revenue from duplication, communication to the public in total or in part, in summary or with comments, transfers of exploitation licences to third parties.

** The exploitation rights of contributions made by individuals from the UK government are covered by a separate agreement 'CEN/HMSO Licence Agreement' dated 26 July 2000.

CEN/TC 251 IPS project.
Date: 2018-09-13 Place: Brussels.

List of assignees

By signing this list of participants, I accept to assign the exploitation rights to CEN in accordance with the Exploitation Rights Assignment Statement

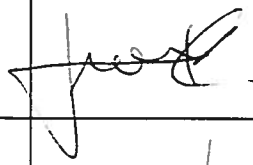
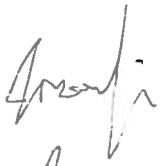
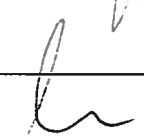
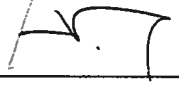
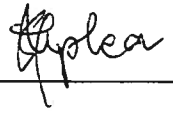
Name	Initials[1]	Signature	Date	Nominating organization[2]	Role[3]	Country	Employer[4]	Sponsor[5]
Stephen Kay				CEN	IPS project leader	UK		
Giorgio Cangioli				CEN/HL7 international	IPS project member & HL7 IPS	IT	(HL7 EUROPE)	
Karima Bourquard				CEN/IHE	IPS project member	FR	(IHE-EUROPE)	
Matthias Pocs				CEN	CEN/TC 251/WG1 convenor	DE		
Catherine Chronaki				HL7 international	Trillium II	GR		
Ed Conley				AIMES		UK	AIMES	
Jos Dumortier				~~Law KU Leuven~~ ~~Timelex~~ KONFIDO	Honorary Professor / Partner Timelex	BE	Timelex	
Marta Terron Cuadrado				EC eHealth systems	semantics		FUJITSU TB	

[1] Initials will be used in the meeting report
[2] Nominating organization = Name of the CEN Member (National Standards Body), Liaison organization , Partner organization, or other organization represented.
[3] Role = please indicate what you are representing i.e. delegate of a CEN Member (TC and SC meetings), expert appointed by a CEN Member (WG meetings), representative of an organization granted observership, Consultant, TC or SC Secretary, TC or SC Chair, WG Convenor ,WG Secretary
[4] Employer = Organization of which the expert is an employee.
[5] Sponsor = Organization funding the expert in this standardization activity. If the sponsor is the same as the employer, please write 'SAME'.

CEN/TC 251 IPS project.
Date: 2018-09-13 Place: Brussels.

List of assignees

By signing this list of participants, I accept to assign the exploitation rights to CEN in accordance with the Exploitation Rights Assignment Statement

Name	Initials[1]	Signature	Date	Nominating organization[2]	Role[3]	Country	Employer[4]	Sponsor[5]
				implementation	expert			
Karlien Erauw			13/9/18	AGORIA NBN	Expert - standardization BE secretary	BE	Agoria	
Jason Gavin				EC/DG SANTE	ERN Clinical Patient Management System Team			
Alexander Mense				HL7 Austria		AT		
Reza Razavi				EC/DG CONNECT	Policy officer			
Stéphane Spahni by remote access				HUG & IHE-Europe co-chair				
Simona Tiplea				EC eHealth systems implementation	Business analyst			
Jeremy Thorp				NHS Digital / Implementation and the Digital Environment	Associate Director	UK		
Charalampos Tsitlakidis			13/9/2018	EC/DG CONNECT	Policy officer			

CEN/TC 251 IPS project.
Date: 2018-09-13 Place: Brussels.

List of assignees

By signing this list of participants, I accept to assign the exploitation rights to CEN in accordance with the Exploitation Rights Assignment Statement

Name	Initials[1]	Signature	Date	Nominating organization[2]	Role[3]	Country	Employer[4]	Sponsor[5]
Antoine Chaudières (by remote access)		✓		ASIP Santé	consultant	FR		
Florence Eon (by remote access)				EC/DG SANTE				
Rob Hausam (by remote access)				HL7 international	HL7 IPS	US		
Angélica Cavalcante Galvão (by remote access)		✓		ASIP Santé	Project manager	FR		
Violaine Margueron (by remote access)		✓		ASIP Santé	consultant	FR		
Thomas Penzel (by remote access)				Charite - Universitätsmedizin Berlin	DIN expert	DE		
Alpo Värri (by remote access)		✓		Tampere University of Technology	Associate Professor, CEN/TC 251/WG2 convenor	Fi		
Shirin Golyardi				NEN	CEN/TC 251 secretary	NL		