Tool-supporting Data Protection Impact Assessments with CAIRIS

Joshua Coles
Bournemouth University
Poole, UK
josh-coles@hotmail.co.uk

Shamal Faily
Bournemouth University
Poole, UK
sfaily@bournemouth.ac.uk

Duncan Ki-Aries
Bournemouth University
Poole, UK
dkiaries@bournemouth.ac.uk

***Abstract*—The General Data Protection Regulation (GDPR) encourages the use of Data Protection Impact Assessments (DPIAs) to integrate privacy into organisations' activities and practices from early design onwards. To date, however, there has been little prescription about how Security & Privacy Requirements Engineering processes map to the necessary activities of a DPIA, and how these activities can be tool-supported. To address this problem, we present a tool-supported process for undertaking DPIAs using existing Requirements Engineering approaches and the CAIRIS platform. We illustrate this process using a real-world case study example where it was used to elicit privacy risks for a prototype medical application to support chemotherapy treatment.**

***Index Terms*—GDPR, Privacy, Risk, Requirements Engineering, CAIRIS.**

I. Introduction

The protections afforded to EU citizens' data privacy by the General Data Protection Regulation (GDPR) have led many organisations to rethink how they collect, process, and manage personal data. GDPR requires organisations to integrate data protection into processing activities and business practices from early design through the product or service lifecycle [1].

To satisfy this requirement, the regulation encourages organisations to undertake a Data Protection Impact Assessment (DPIA) to identify and minimise data protection risks as the initial step of any new project. Depending on the approach adopted, DPIAs should be relatively cheap to implement with sufficient resources and tools. However, while there is advice on the legal requirements for DPIA and the elements of *what* practitioners should do to undertake a DPIA [2], there is less prescription on *how* they should do it.

An evaluation of existing Privacy Requirements Engineering approaches [3] has found that existing approaches capture the elements that would be needed by a DPIA. For example, PriS [4] supports the ability to capture business and privacy goals, while LINDDUN [5] supports the flow of information, and threat modelling activities conducive to assessing privacy risks. However, two barriers need to be overcome before such approaches are ready for security and practitioners to use in DPIAs. First, more prescription is needed to indicate what tools and techniques map to different stages of a DPIA. Second, such steps need to be adequately tool-supported, such that data input in one step can be used to support reasoning and analysis in others.

IRIS (Integrating Requirements and Information Security) is a process framework for devising processes for designing usable and secure software [6]. It is complemented by CAIRIS (Computer Aided Integration of Requirements and Information Security): an open-source platform that can be used with an IRIS process [7]. Although not initially designed with privacy in mind, the framework illustrates how commonly used Security, Usability, and Requirements Engineering techniques can be orchestrated as tool-supported processes.

CAIRIS [7] has been used in a variety of case studies, ranging from the creation of user-centred security policies in critical infrastructure, to the design and development of a secure and privacy preserving web middleware platform [6]. Based on these experiences, we believe CAIRIS supports the concepts required by a tool-supported DPIA process as well. To explore this possibility, we present a tool-supported DPIA process using CAIRIS. The DPIA process orchestrates concepts from the IRIS meta-model, while CAIRIS acts as tool-support for each stage of the process. We consider the background for our approach in Section II, before presenting the approach itself in Section III. We illustrate the approach by describing its use in assessing the privacy implications of a mobile medical application in Section IV, before considering the implications of our work in Section V.

II. Background

A. Supporting GDPR with Requirements Engineering

To comply with GDPR, data processing should adhere to seven principles: (i) Lawfulness, fairness and transparency, (ii) Purpose limitation, (iii) Data minimisation, (iv) Accuracy, (v) Storage limitation, (vi) Integrity & Confidentiality, and (vii) Accountability [8]. The regulation also identifies three roles with a stake in personal data processing:

- *Data Controllers* control the purposes and means of processing personal data;
- *Data Processors* are responsible for processing personal data on behalf of a controller;
- *Data Subjects* are people whose personal data is processed by a controller or processor.

From these principles alone, it is apparent the role that Security & Privacy Requirements can play in evaluating the privacy impact of an initial system design. For example, the

role of requirements in expressing lawful, fair, and purpose limited processing is well explored [9], and recent work by Hosseini et al. [10] illustrates how Requirements Engineering approaches can also be used to reason about transparency.

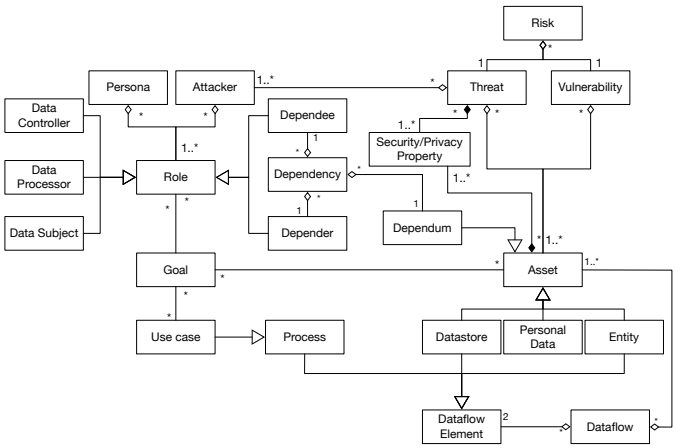

Fig. 1. UML class diagram of IRIS meta-model elements necessary for a DPIA

B. Capturing DPIA concepts with IRIS and CAIRIS

To assess the impact of privacy on some product, design, or service, the Information Commissioner's Office (ICO) in the United Kingdom recommends several requirements for an effective DPIA. These are required to:

- Ensure the need for a DPIA;
- Describe the data processing;
- Consider consultation;
- Assess necessity and proportionality;
- Identify and assess risks;
- Identify measures to mitigate risks;
- Sign off and record outcomes;
- Integrate outputs into a project plan;
- Keep under review.

The data that needs to be elicited as part of a DPIA pertains to Security & Privacy Requirements Engineering, but it is also relevant to Usability Engineering. For example, modelling people and the contexts within which they work are important when justifying the need for processing, or the impact that privacy risks might have on the work associated with this processing. To capture the impact of people on security and requirements, the IRIS meta-model was devised to capture the relationships between security, usability, and requirements engineering concepts [6], and provides the foundations upon which CAIRIS is based.

Although CAIRIS was designed to illustrate the form that tool-support for specifying usable and secure software might take, the sub-set of IRIS concepts in Figure 1 suggests CAIRIS may be able to specify the elements necessary for a DPIA too. For example, although the IRIS meta model was not originally designed to capture the flow of information, an important element when describing data processing, modest extensions to the IRIS meta-model made it possible to model Data Flow Diagrams (DFDs) by leveraging the idea that use cases can capture data processes, and different types of asset can capture entities and data stores [6].

III. Approach

We have devised an approach for conducting a tool-supported DPIA of some system. This entails applying Usability, Security and Requirements Engineering techniques associated with IRIS, and – by using CAIRIS to specify the data collected from these techniques – modelling the system assets and goals, its data flows, and privacy risks.

Although this approach does not explicitly address all requirements desired for recording outcomes, sign-off, and the integration of outputs into a project plan, CAIRIS can still help keep the DPIA under review. For example, CAIRIS can generate documentation that can assist the process. Moreover, as multiple stakeholders can use a running instance of CAIRIS, and traceability is supported between model elements, it is easy to keep the DPIA under review, and shared for discussion with other stakeholders.

A. Data Collection

To establish the need for a DPIA and to collect the data necessary to describe the data processing, the approach begins by gathering any available documentation that describes the practice, process, or system with privacy implications. This can be supplemented with stakeholder interviews to understand the relevant context of use, the nature of the personal data, the processes and people interacting with it, and justification for any data processing. The data collected forms the basis of the subsequent steps.

B. Define Contexts of Use

The contexts of use that the product, service or practice under evaluation needs to operate in are made explicit. These are necessary to put the data processing to be described in context. For example, a processing activity during business hours may be different to the same process that takes place out-of-hours.

C. Define Roles and Personas

Roles correspond with actors that the evaluated system is defined for, while personas are narrative descriptions of archetypical users. Roles are typed based on whether they are data subjects, data controllers, or data processors. These roles form the basis of actors in use cases. Roles may also be fulfilled by potential attackers.

Personas that represent archetypical users [11] are also defined at this stage. As these are grounded in the information collected during the data collection stage, these may be based on assumption-based data. Nonetheless, by acting as a specification of intended users, they encapsulate assumptions made about users, their activities, attitudes, aptitudes, motivations, and skills.

D. Asset Modelling

Before personal data processing can be defined, the data itself needs to be defined. Asset Modelling involves identifying information assets of value within the system, mapping the relationship between system and information assets, and determining the security (Confidentiality, Integrity, Availability, Accountability) and privacy (Anonymity, Pseudonymity, Unlinkability, Unobservability) properties of the assets that need to be preserved [12]. As this information is captured by CAIRIS, asset models – which are based on UML class diagrams – can be automatically generated.

At this stage, we also consider consultation to distinguish personal data from information assets. We do this by making explicit that consent has been provided by a data subject to a data controller for processing it. Because the data controller depends on the data subject for consent, we model this relationship by indicating that the data controller *depender* depends on a data subject *dependee* for an asset *dependum*. This dependency relationship – which corresponds with authorisation relationships in STS-ml [13] and dependency relationships in several social goal modelling languages, e.g. [14] – is defined as follows:

$$
\begin{array}{|l}
Role ::= DataSubject \mid DataController \mid DataProcessor \\
depender\_dependum : Role \pfun Asset \\
dependum\_dependee : Asset \pfun Role \\
\hline
\forall x : Role;\ y : Role;\ a : Asset \bullet \\
\quad x \mapsto a \in depender\_dependum \land \\
\quad a \mapsto y \in dependum\_dependee \land \\
\quad x = DataController \land y = DataSubject
\end{array}
$$

Consequently, personal data can be defined as the set of asset dependums in dependency relationships between data subject dependees, and data controller dependers:

$$
\begin{array}{|l}
Personal\ Data : \mathbb{P}\, Asset \\
\hline
\mathrm{dom}\, depender\_dependum = \{DataController\} \land \\
\mathrm{ran}\, dependum\_dependee = \{DataSubject\}
\end{array}
$$

The depender would typically be a data controller who has received consent from the data subject dependee to process the personal data. However, the dependee may not be the data subject, but acting as a proxy for the data subject. For example, if the data controller has received consent from the data subject to share the personal data with a third party, this third party would fulfil the role of a data controller where the data subject is the original data controller. Because the third party has obligations for protecting this data on behalf of the data subject, they are treated synonymously in our model.

E. Define Processes and Goals

To describe data processing, we rely on use cases and goals to specify processing, and the basis of this processing respectively. Use cases capture sequences of actions a system performs when carrying out personal data processing with an observable result. Goals represent prescriptive statements of intent the system needs to satisfy. Our approach for modelling system and privacy goals is not dissimilar to the approach taken by PriS [4]. Goal models in CAIRIS are based on KAOS goal models [15]; PriS goals are explicitly associated with security or privacy properties. In CAIRIS, these properties are associated with assets where these need to be preserved, or threats where an attacker wishes to exploit them for his or her own ends. Nonetheless, because goals in CAIRIS can be concerned with assets, it is possible for goals to be associated with security and privacy properties by virtue of the properties of their associated assets.

To help assess necessity and proportionality, we rely on the traceability between CAIRIS model elements. As Figure 1 indicates, goals in CAIRIS can be operationalised by use cases. Defining these operational relationships provides an indication that data processing is lawful if the use case actor is a data processor or controller, and necessary because the processing is linked to a goal. Figure 1 also shows that assets can also be associated with goals and, when they are, this helps indicate compliance with GDPR's Purpose Limitation principle by indicating that the purpose pertains to the personal data asset processed within the associated use case.

F. Define Data Flows and GDPR non-compliance checks

Taking inspiration from LINDDUN [5], we use Data Flow Diagrams to model the flow of personal data between external systems and people (entities), the use cases that carry out personal data processing (processes), and systems that store persistent data (data stores). Data flows in CAIRIS are labelled, and carry one or more items of personal data. At this stage, the assets that constitute entities and data stores should already have been defined, together with the use cases that describe data processing.

Once these data flows have been defined, it is possible to carry out simple GDPR non-compliance checks based both on the data flows and the information captured in previous steps. For example, consider the GDPR principles that *Personal data must be processed lawfully, fairly, and transparently*, and *Personal data can only be collected for specified, explicit and legitimate purposes*. We defined data flows as fair and lawful if, and only if processing is undertaken by a data processor, data controller, or data subject, and processes have been operationalised by necessary goals that specify or constrain data processing, e.g.

$$
\begin{array}{|l}
necessary\_goals : Process \pfun \mathbb{P}\, Goal \\
process\_actors : Process \pfun \mathbb{P}\, Role \\
lawful\_dataflow : Entity \pfun Process \\
\hline
\forall x : Entity;\ y : Process \bullet \\
\quad x \mapsto y \in lawful\_dataflow \land \\
\quad (DataController \in process\_actors(y) \\
\quad \lor\ DataProcessor \in process\_actors(y) \\
\quad \lor\ DataSubject \in process\_actors(y)) \land \\
\quad y \in \mathrm{dom}\, necessary\_goals
\end{array}
$$

While such checks are not sufficient to prove that an emerging design is fully compliant with GDPR, they are a

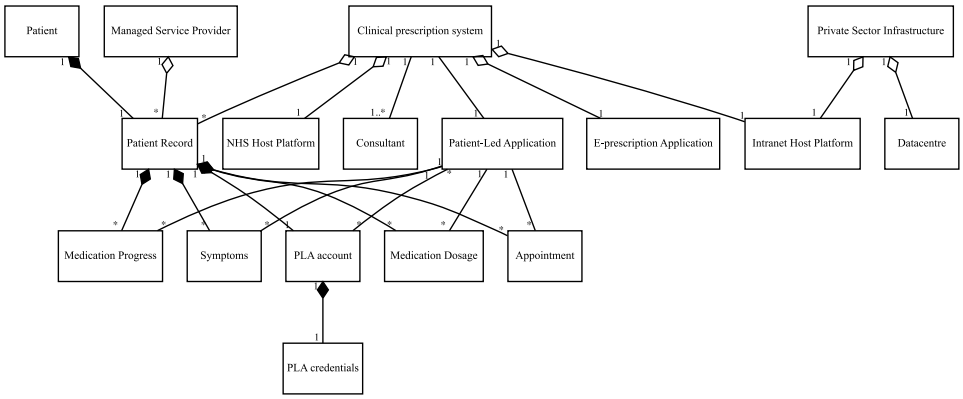

Fig. 2. Final asset model of PLA assets

useful sanity check for identifying when some element of a design might *not* be compliant. These GDPR non-compliance checks have been implemented in CAIRIS; further details of these checks can be found in [16].

G. Privacy Risk Analysis

Privacy risk analysis identifies measures to mitigate risks. Using previous stages as input, we define vulnerabilities identified while describing the data processing, and considering necessity and proportionality. We also define threats to the personal data, the attackers behind these threats, and risks that combined threats and vulnerabilities. These risks can be visualised using automatically generated risk analysis models in CAIRIS. Based on the privacy risks elicited, responses are devised to attend these risks. The use of CAIRIS for risk analysis is described in more detail in [6].

IV. Evaluating a Patient-Led Application

There are many challenges associated with the safe treatment of chemotherapy to cancer patients; one is ensuring that patients are made as comfortable as possible during treatment, and attend hospital only when absolutely necessary. To reduce both the stress and the cost associated with patients making unnecessary hospital trips, a UK-based e-prescription company plans to create a handheld *Patient-Led Application* (PLA) patients can use to report symptoms and the progress made with medication they are receiving, and co-ordinate appointment dates for hospital visits.

We evaluated our approach by eliciting privacy risks for the initial design of PLA. The PLA currently existed only as a conceptual design, but – before any further design & development work – we worked with the company to examine how it would interact with patient data and the existing e-prescription infrastructure the company delivers. All aspects of the PLA that involve personal data handling and processing would need to be assessed during the DPIA. Consequently, the scope of investigation would need to include associated systems that handle data collected and processed by the PLA.

A. Data Collection

To begin the process of data collection, an initial hour long semi-structured interview was undertaken on-site with a company analyst. Interview questions began by establishing the main areas of functionality for the PLA, before eliciting information about who the intended users would be, what devices they would use, and how information (personal or otherwise) would flow between the PLA and other connected systems. The latter stages of the interview were devoted to understanding the threat model associated with the PLA. Information from the interview transcript was then used as the main source of data for the subsequent steps of this process. This was complemented with ad-hoc communication with the company analyst.

B. Define Contexts of Use

Because the PLA is currently only in the conceptual design stages, and the contexts of use were not fully understood by the company, only a single environment (Development) was defined for this DPIA.

C. Define Roles and Personas

Based on the data collected, six different roles were identified. One of these was a Data Protection Officer (DPO) role; a role acting on behalf of the company as Data Controller. Three roles represented human interaction with the PLA or associated systems: patients, medical consultants, and company employees. The final roles represented machine agents: the host platform API and prescription system API. These two roles were not initially identified from the data collected, but were later added as an output from defining processes and goals.

Three personas were created to put these roles in context, and add a human dimension to the personal data processing. Ben represented the company's DPO, Catherine represented a patient receiving chemotherapy that would use the PLA, and Henry represented a medical consultant responsible for prescribing the medication based on the information inputted into the PLA. These were *assumption* personas rather than

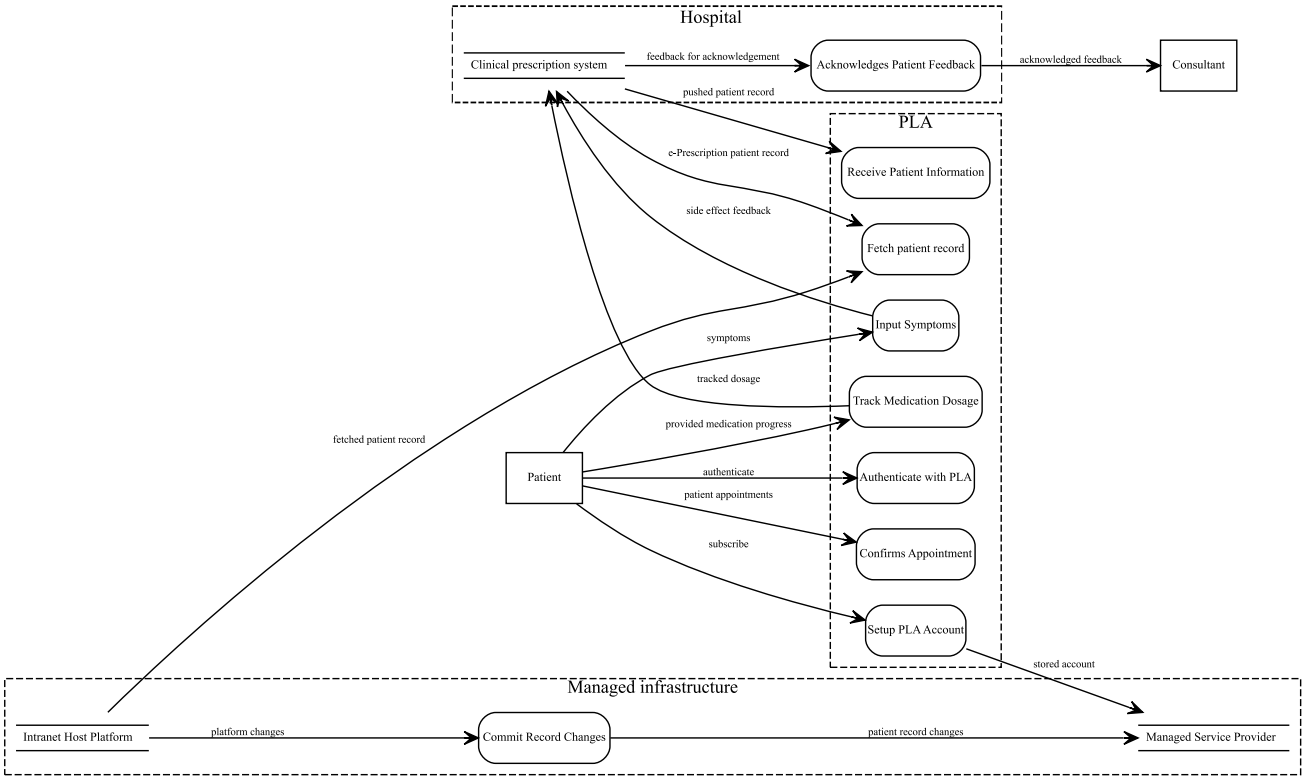

Fig. 3. Data Flow Diagram showing the data flows associated with the Development context of use

personas grounded in data collected about these human roles. The personas did, however, make it possible to put assumptions about the humans interacting directly and indirectly with PLA in one place.

D. Asset Modelling

Ten assets were initially identified based on discussions with the company. However, a further seven assets were identified in later stages together with additional asset relationships. The final asset model generated by CAIRIS can be seen in Figure 2. Although the focus of the approach is the PLA, the asset model shows that this is just part of the larger environment where the PLA is used. This environment also includes the clinical prescription system used in the hospital responsible for treating chemotherapy patients, and the private sector infrastructure providing hosting services to both the hospital and the PLA.

An initial dependency relationship was added to indicate that a DPO is dependent on patients for providing the consent necessary for the PLA to process a subset of patient records. However, as additional assets were elicited in later stages, dependency relationships between these roles were also added for medication progress data, appointments, and symptoms.

E. Define Processes and Goals

Goals related to the PLA were then elicited and modelled. From the interview transcript, 22 goals were obtained from where it was explicitly stated what mechanics and functionality they required PLA to have. These goals were then broken down into high level goals elicited from the interview, and further refined as sub-goals.

Nine data processing activities were elicited from the source data, and inferred from the analysis carried out in previous steps. Seven of these processes were use cases associated with the PLA, e.g. registering and authenticating with the PLA, inputting symptoms and tracking medical dosage and confirming appointments with the hospital. However, two processes were associated with external systems that process or manage personal data collected by the PLA.

F. Define Data Flows and GDPR non-compliance checks

The DFD generated by CAIRIS shown in Figure 3 illustrates the information flows associated with the PLA, the data processing it needs to support, and the associated data processing in related systems such as the hospital, and managed infrastructure used by both the hospital and the PLA. The DFD also shows dotted boxes that represent *trust boundaries*; these are anywhere where data flows cross privilege levels [17]. These trust boundaries delimit the processing that takes place within the PLA, the hospital, and the managed infrastructure. Examining these data flows, particularly where the trust boundaries were, was useful for identifying potential vulnerabilities and threats.

A GDPR non-compliance check of the emerging CAIRIS model flagged 17 warnings. The majority of these were necessary processing warnings due to use cases processing personal data without any indication why the data processing

was necessary. The data purpose validation warnings were generated because no goals were currently associated with the personal data being processed, therefore additional goals were identified to protect the personal data processed by the PLA and associated systems.

G. Privacy Risk Analysis

Based on the privacy risk analysis undertaken, two privacy risks were identified. The first related to the creation of multiple PLA accounts. The second, as illustrated by the CAIRIS risk analysis model in Figure 4, relates to the incorrect prescription of medication. This risk puts into context what happens when Catherine enters inaccurate information, which is acknowledged by Eve – another consultant handling Catherine's treatment – in time for the next prescription cycle. The inaccuracy leads to the diagnosis of incorrect symptoms, and the subsequent prescription of incorrect medication. Figure 4 shows both the vulnerability (PLA misinformation) and the threat (Incorrect symptoms) leading to the risk, together with the assets associated with both. This is considered a privacy risk because the assets *Symptoms* and *Medication Dosage* were previously identified as personal data.

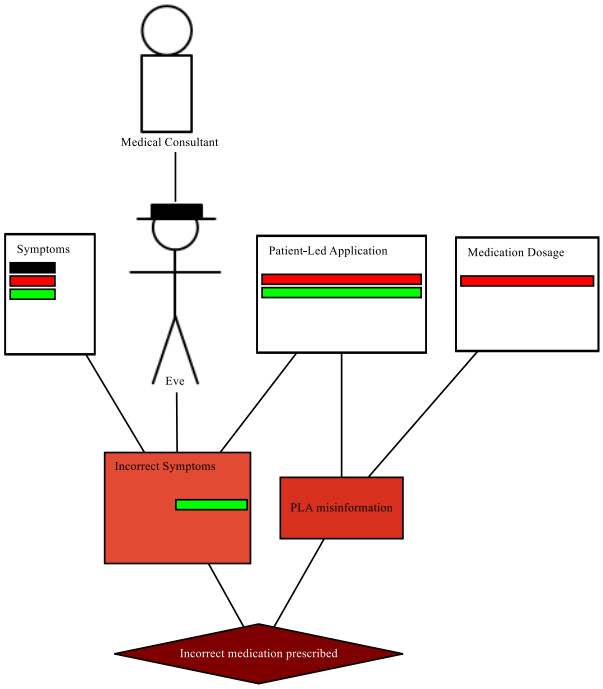

Fig. 4. Risk Analysis model showing the elements contributing to the prescription of incorrect medication

The DFD in Figure 3 also provided some help in responding to this risk. In addition to revising the design of the PLA interfaces reporting the symptoms, the quality of the information flowing between the PLA and the consultant needs to be accounted for. It is also necessary to identify any additional processing that might take place within the hospital trust boundary, and look for any ambiguity in the handling of personal data in the Acknowledges Patient Feedback process.

V. Conclusion

In this paper, we presented a tool-supported DPIA process based on CAIRIS to help assess the impact that GDPR might have on some product, service, or practice. In doing so, we have made three contributions. First, we have shown how existing Requirements Engineering techniques associated with IRIS can be effective when supporting the different steps needed when carrying out a DPIA. As our approach identified, there is no one-to-one mapping between requirements and techniques, and several techniques might be needed to support a single step. Second, we have demonstrated how CAIRIS – as an exemplar for Security Requirements Engineering tool-support – can not only support such a process, but help reason about potential GDPR compliance issues as a design evolves. Those interested in further details about the PLA example or reproducing the approach may be interested in reviewing the final CAIRIS model created by the authors [18]. Finally, we presented a real example where our approach assessed the conceptual design of a medical application without an initial specification, and only the most preliminary of known functionality. As such, we have shown that the use of our approach, and the Requirements Engineering techniques in general, were effective in discovering additional functionality, and envisaging different forms of intended and unintended device use.

We found the ability of CAIRIS to automatically generate models particularly useful for promoting discussion, and exploring the implications of making changes in earlier steps of the process. As a result, we found this approach stimulated the company's interest in not only the tool-support, but in the Requirements Engineering techniques used as well. Consequently, the company is considering how this approach can be used to evaluate the impact of GDPR on other systems.

Our approach also removed some of the ambiguity associated with how GDPR principles are interpreted. For example, the principle of maintaining Integrity and Confidentiality across the organisation is open to interpretation depending on how different stakeholders interpret *appropriate* measures for protecting personal data. Our approach removes this ambiguity because CAIRIS provides set definitions for these terms, and – by visualising the impact of risk – stakeholders can use the same model as a boundary object when evaluating the appropriateness of mitigating controls.

An improvement to our approach would be support for referral stages throughout the process. Referral stages would be performed after critical stages to ensure information produced is being processed correctly. This improvement would ensure that the stakeholders are content with what is being produced and assessed. It would also address a threat to validity with this approach - the lack of explicit input from a DPO or some other stakeholder with legal expertise in GDPR.

REFERENCES

[1] Information Commissioner's Office, "Data protection by design and default," http://bit.ly/2umnTYI, 2018.

[2] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A process for data protection impact assessment under the european general data protection regulation," in *Privacy Technologies and Policy*, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Springer, 2016, pp. 21–37.

[3] K. Beckers, "Comparing privacy requirements engineering approaches," in *Proceedings of the 7th International Conference on Availability, Reliability and Security*, 2012, pp. 574–581.

[4] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the PriS method," *Requirements Engineering*, vol. 13, pp. 241–255, 2008.

[5] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3–32, Mar 2011.

[6] S. Faily, *Designing Usable and Secure Software with IRIS and CAIRIS*, 1st ed. Springer, 2018.

[7] ——, "CAIRIS web site," https://cairis.org, June 2018.

[8] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," http://bit.ly/2zCQTjN, April 2018.

[9] Anonymous, "International Workshop Series on Requirements Engineering and Law: History," http://gaius.isri.cmu.edu/relaw/, June 2017.

[10] M. Hosseini, A. Shahri, K. Phalp, and R. Ali, "Four reference models for transparency requirements in information systems," *Requirements Engineering*, vol. 23, no. 2, pp. 251–275, Jun 2018.

[11] A. Cooper, R. Reimann, D. Cronin, and C. Noessel, *About Face: The Essentials of Interaction Design*. John Wiley & Sons, 2014.

[12] I. Fléchais, M. A. Sasse, and S. M. V. Hailes, "Bringing security home: a process for developing secure and usable systems," in *Proceedings of the 2003 New Security Paradigms Workshop*. ACM, 2003, pp. 49–57.

[13] F. Dalpiaz, E. Paja, and P. Giorgini, *Security Requirements Engineering: Designing Secure Socio-Technical Systems*. MIT Press, 2016.

[14] E. Yu, P. Giorgini, N. Maiden, and J. Mylopoulos, *Social Modeling for Requirements Engineering*. MIT Press, 2011.

[15] A. van Lamsweerde, *Requirements Engineering: from system goals to UML models to software specifications*. John Wiley & Sons, 2009.

[16] S. Faily, "CAIRIS manual: Model Validation," https://cairis.readthedocs.io/en/latest/validation.html, June 2018.

[17] A. Shostack, *Threat Modeling: Designing for Security*. John Wiley & Sons, 2014.

[18] J. Coles, S. Faily, and D. Ki-Aries, "Tool-supporting Data Protection Impact Assessments with CAIRIS: PLA model," Aug. 2018. [Online]. Available: https://doi.org/10.5281/zenodo.1311935