BU

Bournemouth
University

Bournemouth University

26th IEEE International
Requirements Engineering Conference
The 5th International Workshop on Evolving
Security & Privacy Requirements Engineering
20 August 2018
Banff, Alberta, Canada

[dstl]

Tool-supporting Data Protection Impact Assessments with CAIRIS

Joshua Coles, Shamal Faily, Duncan Ki-Aries

Approach

- We present an approach for conducting a tool supported Data Protection Impact Assessment (DPIA) relating to a system.

- This applies 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.

- **CAIRIS – cairis.org**
  Computer-Aided Integration of Requirements and Information Security

GDPR

The General Data Protection Regulations

GDPR Six Principles

- Lawfulness, Fairness & Transparency;
- Purpose Limitation;
- Data Minimisation;
- Accuracy;
- Storage Limitation;
- Integrity & Confidentiality.

Roles when processing personal data:

- 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.

DPIA’s

DPIA’s - Data Protection Impact Assessments

- A method of ensuring and understanding what data is collected for within your organisation;
- Evidence of proper data management practice/ data management process development;
- Recommended to be performed on a new process being implemented within the organisation which involves the following:
  - Across Border Contact
  - Systematic Monitoring
  - Sensitive Data
  - Vulnerable Data Subjects
  - Large Scale Processing
  - New Technologies
  - Withholding Access

DPIA Requirements

- Ensuring the need for a DPIA
- Description of the data processing
- Consider consultation
- Assess necessity and proportionality
- Identify and assess risks
- Identify measures for risk mitigation
- Sign off and record outcomes
- Integrate outputs into a project plan
- Keep under review

Existing Guidance on DPIAs

The ICO provides guidance on when to perform a DPIA and what one consists of, and showcases a step-by-step guide on the stages required to perform a DPIA.

The drawback of this guidance however, is that it can be perceived as quite ambiguous, and in need of context, as was discovered during the production of the process showcased in the paper.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Case Study

- The process was applied to a small local medical company’s concept level application, referred to as “The PLA” or Patient-Led Application

- The PLA was in very early concept stages, thus the clients only had an initial idea on how the PLA would function.

- The PLA required a DPIA in order to show compliance to GDPR, and to incorporate Privacy by Design in the PLA design.

The Process

- The process was devised by analysing ICO guidelines and understanding what CAIRIS can do to support it.

- The process is discussed in further detail within the paper, but can be broken down into the following stages:
    - Data Collection
    - Define Contexts of Use
    - Define Roles & Personas
    - Asset Modelling
    - Define Processes & Goals
    - Define Data Flows and GDPR non-compliance checks
    - Privacy Risk Analysis

CAIRIS

Computer-Aided Integration of Requirements and Information Security

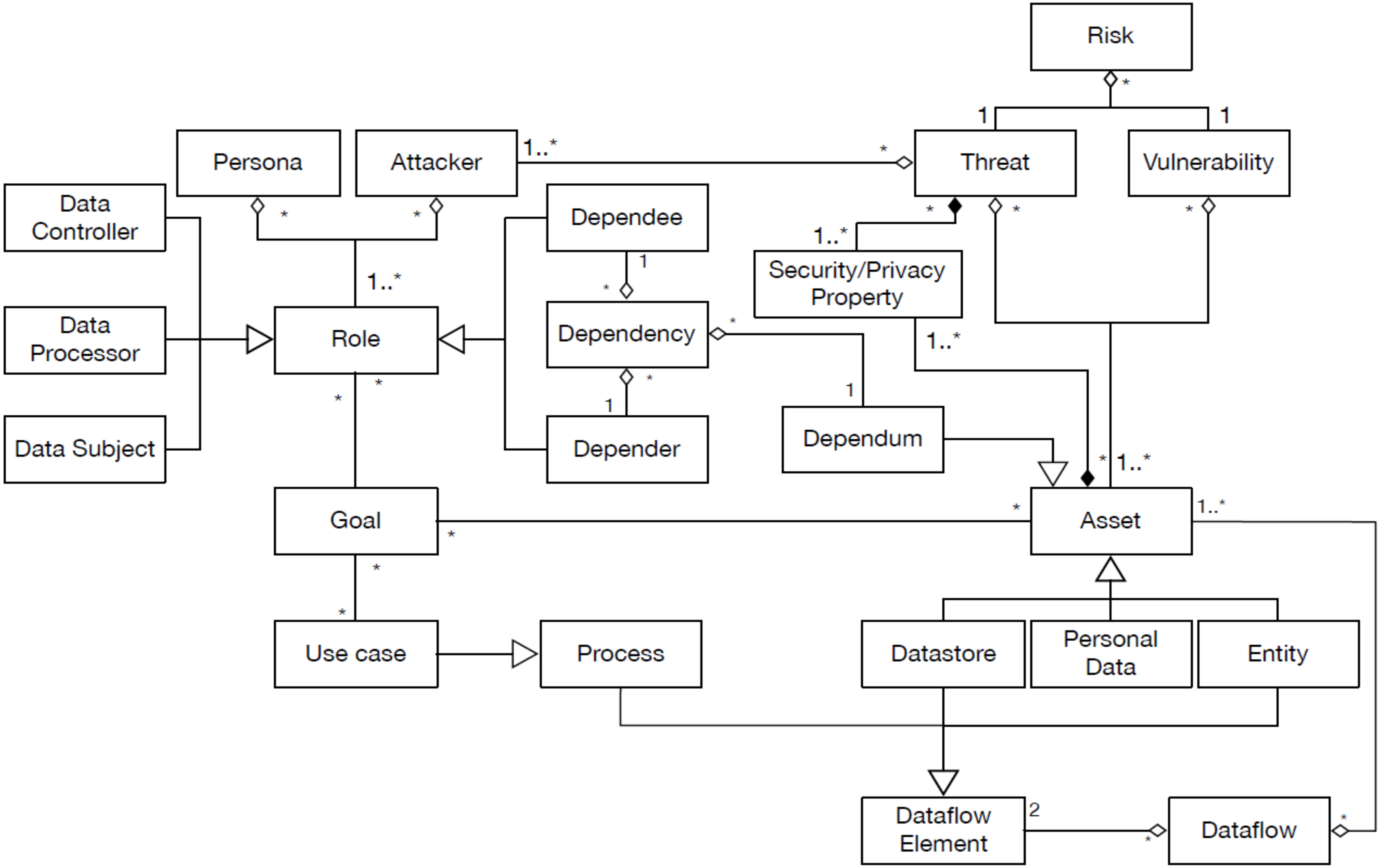
- Currently Open Sourced software with continual improvements and enhancements;
- Provides a centralised platform that either individuals or whole teams can contribute towards;
- Enter or import a wide range of security, usability, and requirements data, and automatically generate security, usability, and requirements visual models based on connections between concepts that analysts make, and which summarise quantitative and qualitative data analysis;
- Help find new insights ranging from interconnections between requirements and risks;
- Provide functionally to integrate persona characteristics;
- Generate Volere compliant requirement specifications in different formats.

https://cairis.org/

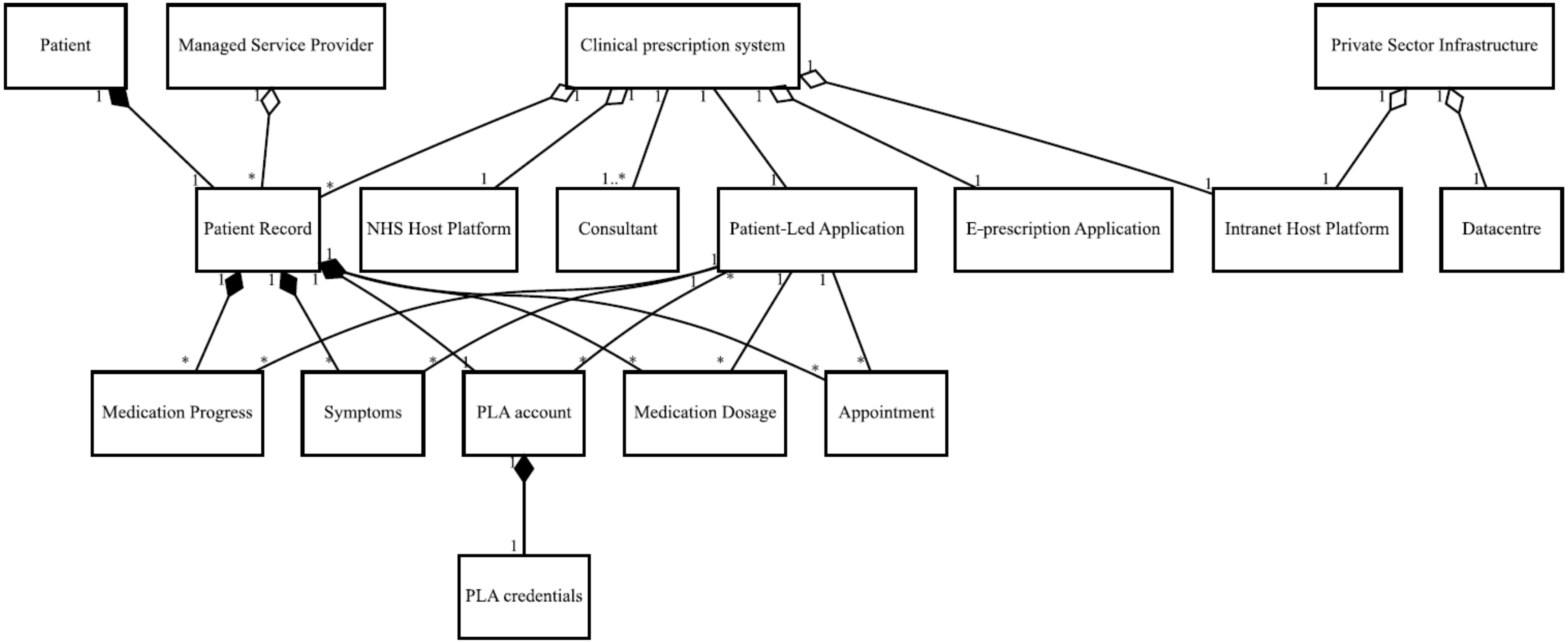
CAIRIS's Importance

- Each stage followed within the process is done so within CAIRIS.
- The stages within the process are incrementally performed; each stage builds off of the previous. The way CAIRIS is designed promotes this.
- GDPR principle validation is solely reliant on CAIRIS functionality.

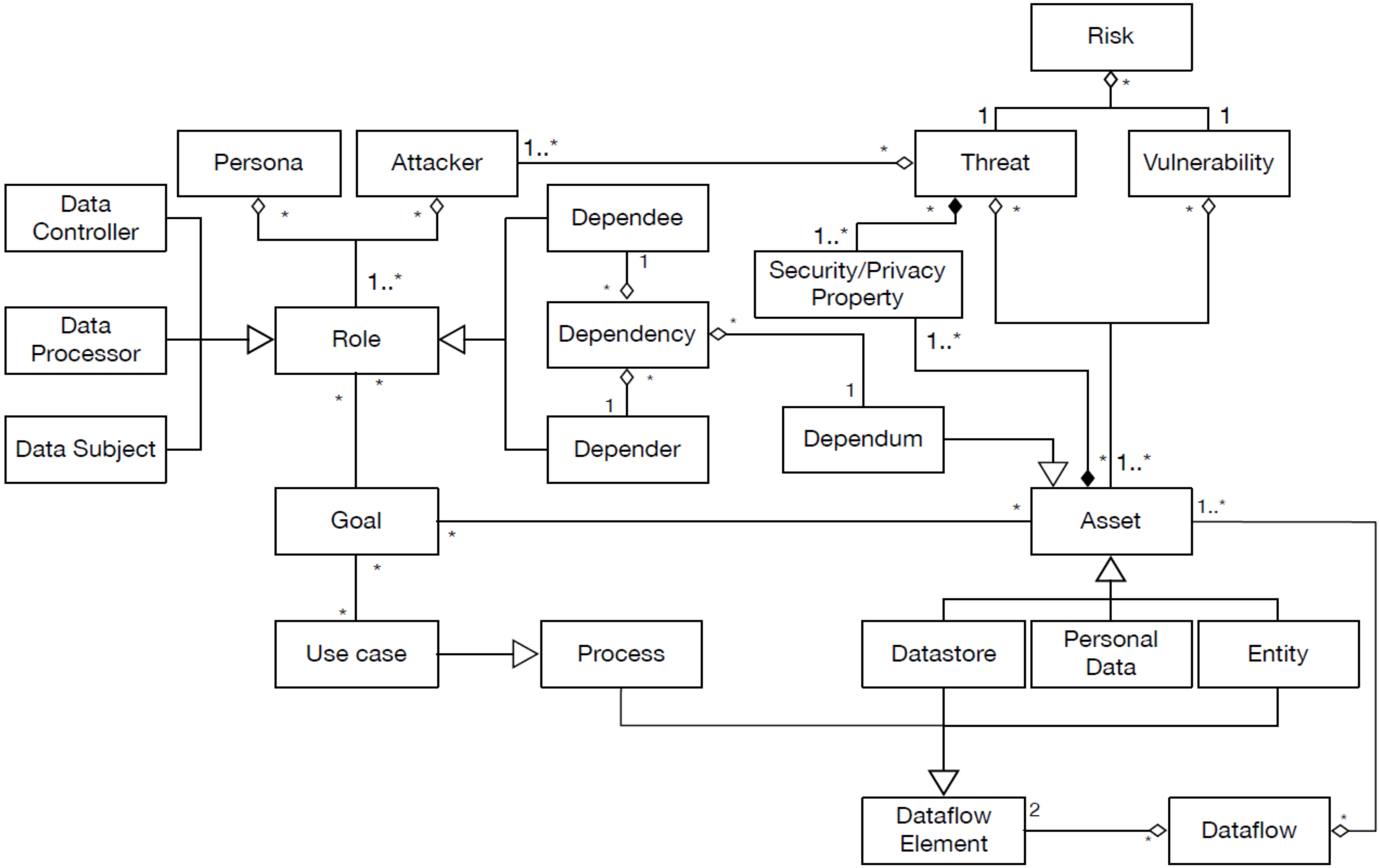
IRIS Meta Model for DPIA



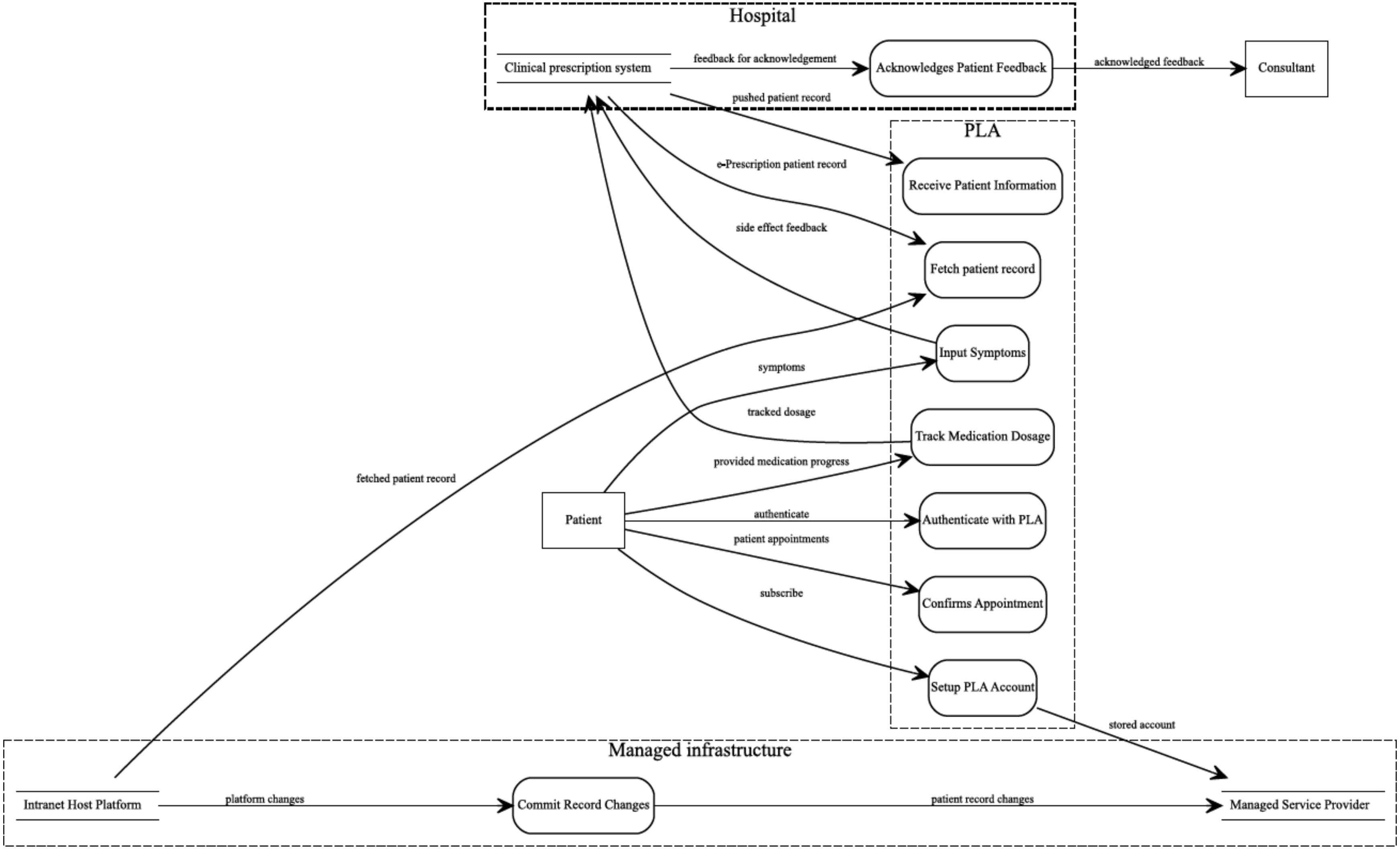
CAIRIS Asset Model



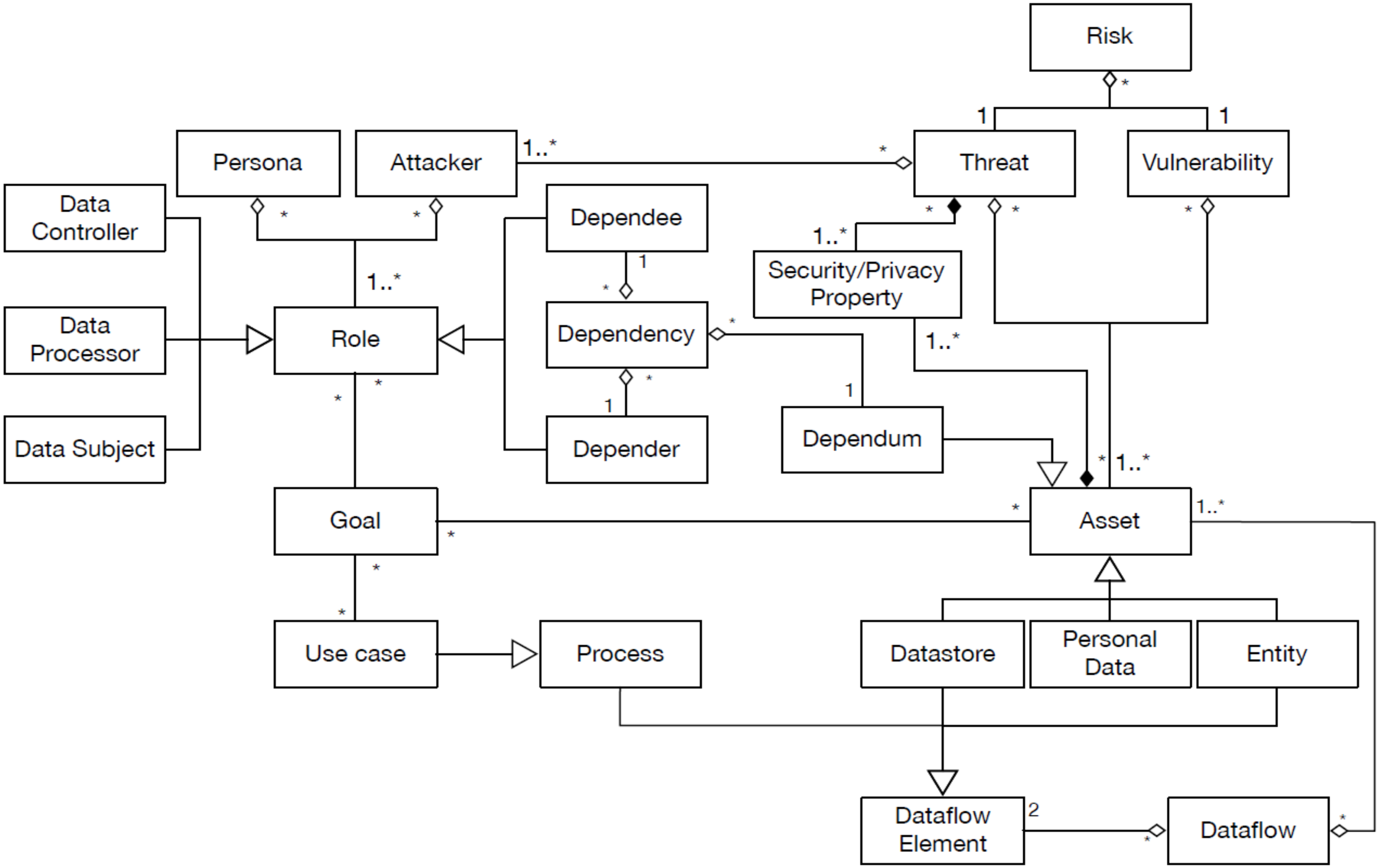
IRIS Meta Model for DPIA



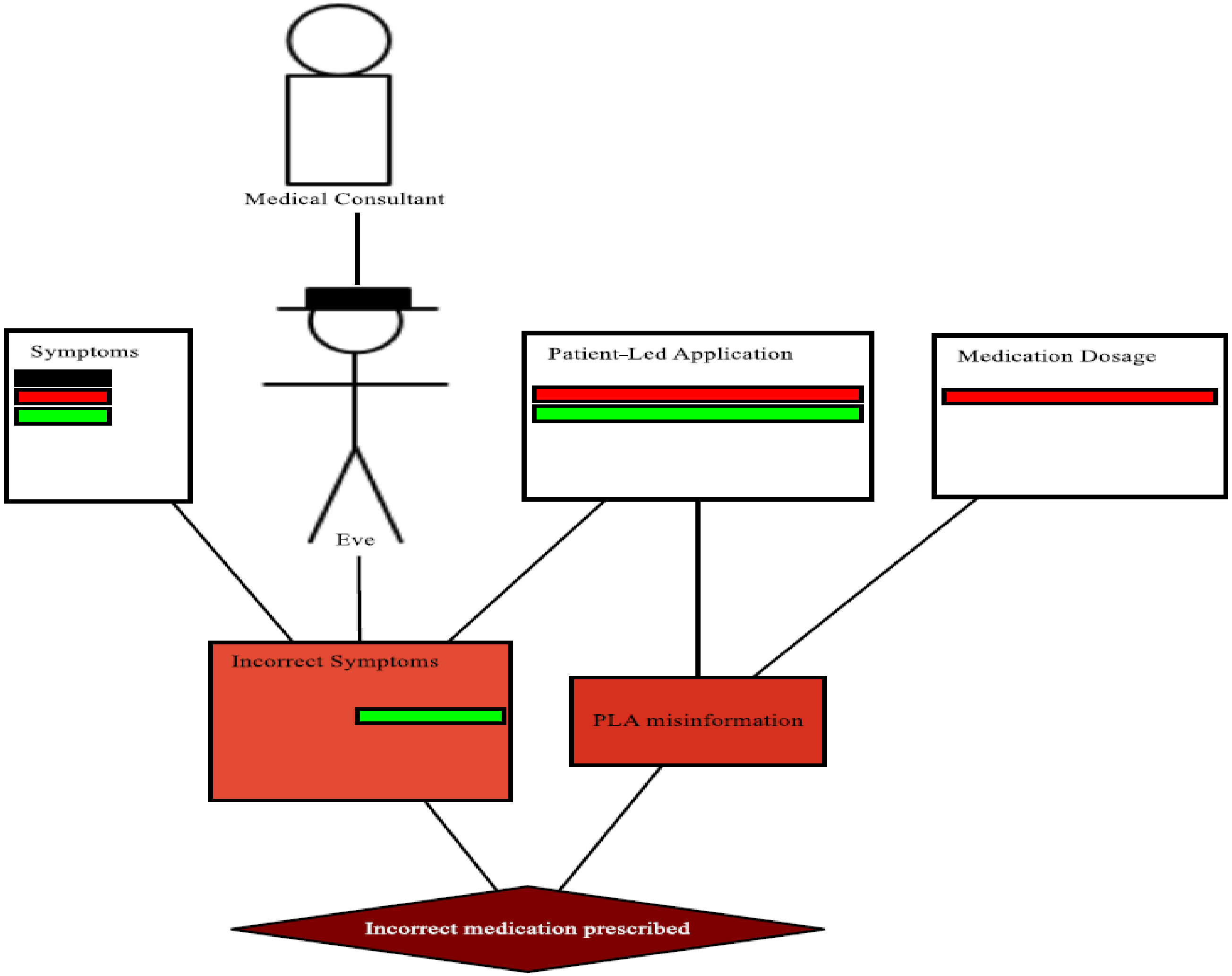
CAIRIS Data Flow Model



IRIS Meta Model for DPIA



CAIRIS Risk Model



Summary

- The paper demonstrated how existing Requirements Engineering techniques associated with IRIS can be effective when supporting the different steps needed when carrying out a DPIA.
- 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. Our approach also removed some of the ambiguity associated with how GDPR principles are interpreted.
- Using a real example where our approach assessed the conceptual design of a medical application, we 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.
- The techniques used were effective in discovering additional functionality, and envisaging different forms of intended and unintended device use.

Questions?

Duncan Ki-Aries
PhD Researcher - Cyber Security

dkiaries@bournemouth.ac.uk

Department of Computing & Informatics
Bournemouth University
Fern Barrow,
Talbot Campus,
Poole
BH12 5BB

Bournemouth University Cyber Security Research group (BUCSR)
https://cybersecurity.bournemouth.ac.uk/

Bournemouth University Human Computer Interaction group (BUCHI)
hci.bournemouth.ac.uk/

CAIRIS – https://cairis.org/

BU
Bournemouth
University