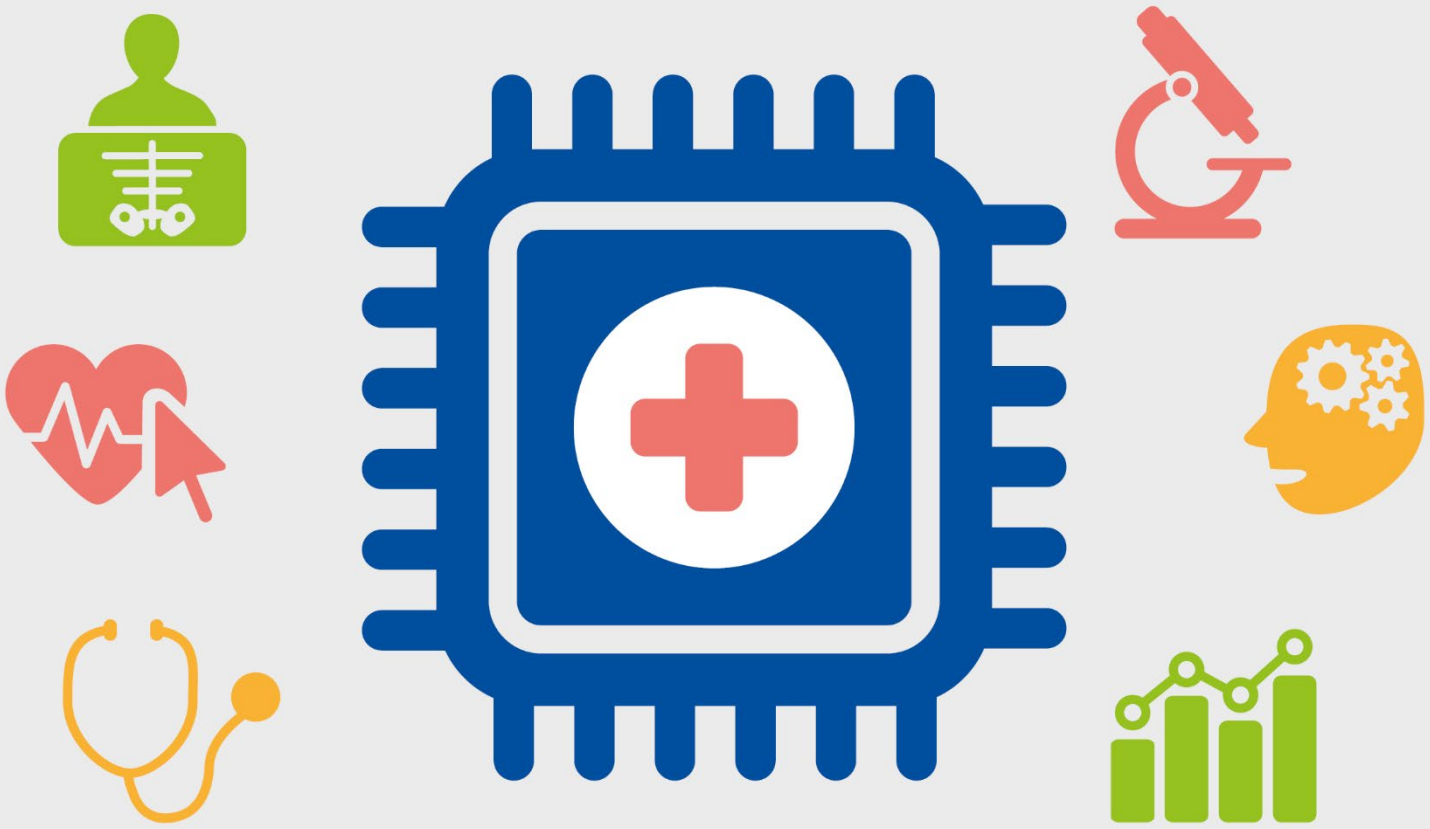
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



## CONTACT

## EDITORS

## LEGAL NOTICE

## COPYRIGHT NOTICE

This new report analyses cybersecurity and privacy requirements and measures in use of AI in medical imaging diagnosis of osteoporosis. The report describes the scenario fundamental principles (assets, actors processes etc.), identifies the security and privacy risks it poses, and finally cybersecurity and privacy controls, which counteract the identified risks.

## 1.1 STUDY OBJECTIVES

- medical imaging diagnosis
-
-

## 1.2 METHODOLOGY

-

- 
- 

### 1.2.1 Description of the scenario

- 
- 
- 
- 
- 
- 
- 
- 

### 1.2.2 Identification of cybersecurity and privacy threats and vulnerabilities

### 1.2.3 Identification of cybersecurity and privacy controls

- 
- 

## 1.3 TARGET AUDIENCE

- **All actors (private or public):**

- **AI technical community, AI cybersecurity and privacy experts and AI experts**

- **Cybersecurity and privacy community**

## 1.4 USING THIS DOCUMENT

-

-

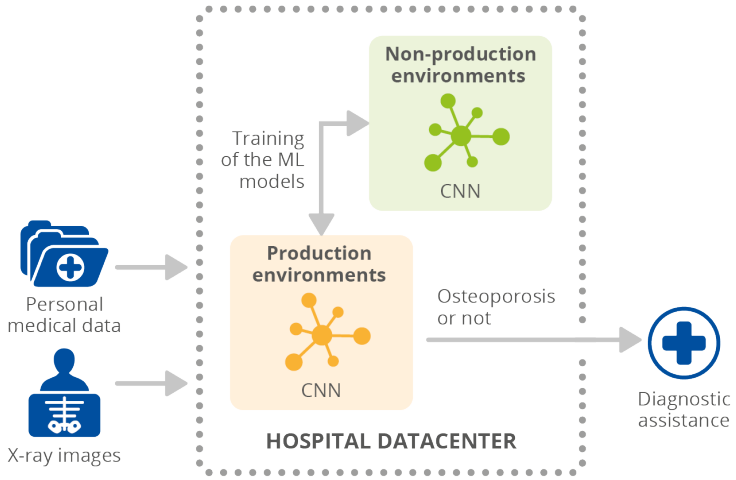
-

**Figure 1:**

# MEDICAL IMAGING

## DESCRIPTION

Osteoporosis is a major bone disease characterized by a reduction in bone mineral density (BMD) and deterioration of bone architecture, leading to an increased risk of fracture that causes significant morbidity and mortality worldwide. Considering this, a private medical practice aims **to detect the presence or absence of osteoporosis in its patients** much more easily. To achieve this goal, the practice uses medical imaging and machine learning to detect the disease.




## DATA

**Data used to build the model**

- Historical X-rays of patients with or without osteoporosis
- Data related to age, gender, and body mass index of historical patients of the medical cabinet

**Data used once the model is in production**

- X-rays of patients who come for consultation
- Data related to age, gender, and body mass/ Faimess index of who come for consultation

## CYBERSECURITY AND PRIVACY REQUIREMENTS

**Cyber requirements**

Availability · Integrity · Confidentiality · Traceability

**Privacy Requirements**

Availability · Integrity · Confidentiality · Traceability

- Lawfulness
- Transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Security of personal data
- Database creation
- Compliance of the training model

Critical · High · Low

## ACTORS

- Radiologists/medical practice
- Large tech companies
- Historical Patients
- New Patients
- Cloud provider
- Data scientists
- Developers and Data Engineers
- System and communication network's administrator

## ASSETS

- CNN-algorithm used
- Data lake - in the cloud
- Model server - in the cloud
- Scanner
- X-ray computer-aided diagnostic system. on-premises
- Integrated Development Environment
- Libraries
- Communication protocols and network

## 2.1 PURPOSE AND CONTEXT

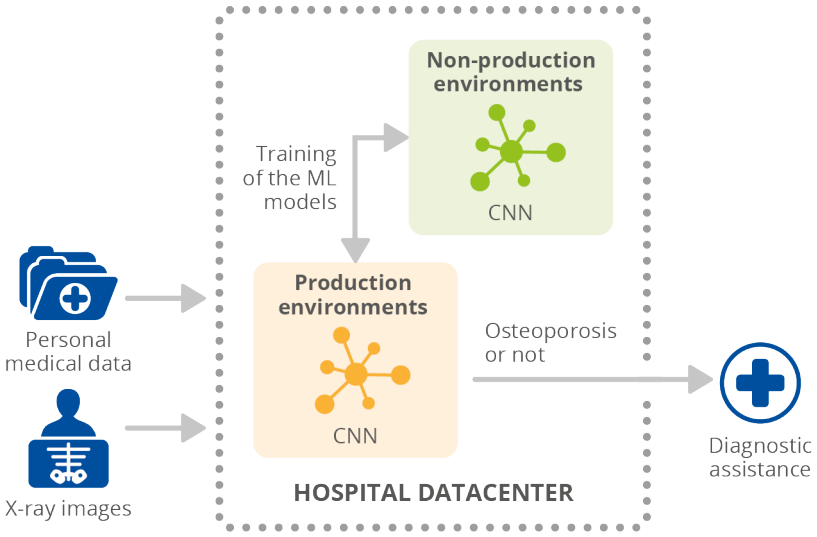
- 
- 

## 2.2 HIGH-LEVEL DESCRIPTION

**to detect the potential presence of osteoporosis by giving the radiologist a probability that the bone contains the disease**

- 
- 
- 
- 
- 

Figure 2:




## 2.3 ACTORS AND ROLES

Figure 3:

| Actor | Role | Description |
|---|---|---|
| **Radiologists/medical practice** | *End Users and Data Owner (**Data Controller**)* | |
| **Large tech companies** | *Model Provider* | |
| **Historical Patients (before the occurrence of the diagnosis)** | *Data Provider* | |
| **New Patients (during the occurrence of the diagnosis)** | *Data Provider* | |
| **Cloud Provider** | *Cloud Provider* | |
| **Data Scientists** | *Data Scientists* | |
| **Developers and Data Engineers** | *Developers and Data Engineers* | |

| | | |
|---|---|---|
| **System and communication Network Administrator** | *Network Administrators* | |

## 2.4 PROCESSED DATA

**Figure 4:**

| Data | Data type | Source / data provider | Data Procurement |
|---|---|---|---|
| | | | |
| onymised | | historical patients' radiographies<br>former patients. | |
| pseudonymised | | former patients. | |
| | | | |
| | | patients. | |
| | | patient . | |

## 2.5 MACHINE LEARNING ALGORITHMS

Convolutional Neural Network (CNN)

*Augmenting Osteoporosis Imaging with Machine Learning.*

**Figure 5:**

| Learning paradigm | Subtype | Algorithm | Type of data ingested | Description |
|---|---|---|---|---|
| | | | | |

## 2.6 ASSETS

**Figure 6:**

| Type of asset | Asset | Description |
|---|---|---|
| **Models** | | |
| **Environment tools** | *in the cloud* | |
| | *in the cloud* | |
| | | |
| | *– on-premises* | |
| | | |
| | | |
| | | |

## 2.7 OVERALL PROCESS

**Data collection**

**which must be annotated**

**Data cleaning and data pre-processing**

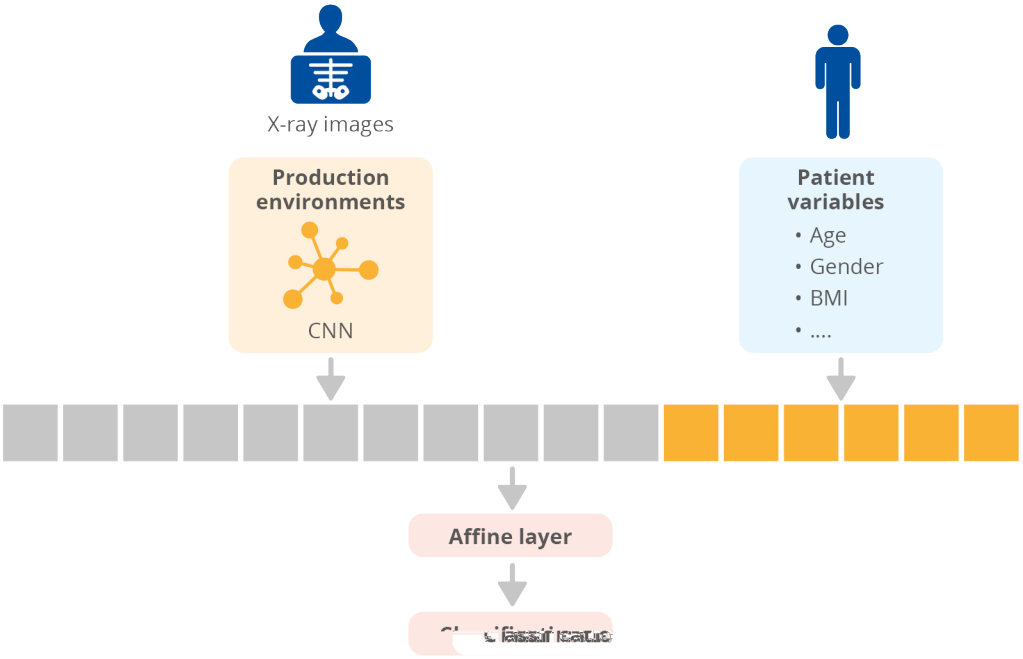
**cleaned**

**pre-processing.**

**Model design and implementation**

*CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning.*

**Figure 7:**




**The input of the network**

**the output of the network**

**Model training, model testing and optimisation**

**the training method**

**Model Evaluation**

**evaluate the model**

**Model Deployment**

*Metrics for evaluating 3D medical image segmentation: analysis, selection, and tool.* **Taha, Allan and Aziz, Abdel.**

Monitoring and inference

**Figure 8:**

| Steps | Description | Actors | Assets |
|---|---|---|---|
| Data Collection | | | |
| Data Cleaning | | | |
| Data pre-processing | | | |
| Model design and implementation | | | |
| Model training | | | |

| | | | |
|---|---|---|---|
| **Model testing** | | | |
| **Optimization** | | | |
| **Model evaluation** | | | |
| **Model deployment** | | | |
| **Monitoring and inference** | | | |

## 2.8 PRIVACY AND CYBERSECURITY REQUIREMENTS

**Cybersecurity requirements**

**Figure 9:**

| | Level | Explanation |
|---|---|---|
| **Availability** | **Low** | |
| **Integrity** | **Critical** | |
| **Confidentiality** | **Critical** | |

| | | |
|---|---|---|
| Traceability | High | |

**Privacy requirements**

**personal data are processed when patients come to the practice and are diagnosed for osteoporosis, adding information like last name, name, and consultation date in the patient's file**

**the following privacy requirements and recommendations should be satisfied**

**Figure 10:**

| Requirements | Explanation |
|---|---|
| **Lawfulness, fairness, and transparency** | **Lawfulness:**<br><br>**Fairness:**<br><br>**Transparency:** |
| **Purpose limitation** | |

| | |
|---|---|
| **Data minimisation** | |
| **Accuracy** | |
| **Storage limitation** | |
| **Security of personal data (Integrity and Confidentiality)** | |

**Figure 11:**

| Recommendations | Explanation |
|---|---|
| **Database creation** | |
| **Compliance of the training model (i.e. before production)** | |

**Figure 12:**

| Criteria | Does it match the criteria? | Justification |
|---|---|---|
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Figure 13:**

| | Level | Explanation |
|---|---|---|
| **Availability** | **Low** | |
| **Integrity** | **Critical** | |
| **Confidentiality** | **Critical** | |
| **Traceability** | **High** | |

## 3.1 THREAT CONTEXTUALISATION

reputation degradation lawsuit
company and physical and permanent injury for the patient

- 
- 

reputation
degradation and a lawsuit,

Phishing attempts,
targeted advertising. Uniqure a07.7 (alnt)-5 0.7 (n)5.7 1 Tf-5 (and )TJh onl(al)-1 ((e)-7 (d gc)-3 (asv-5 (o per)-n 5 (y)-3 ( ofi

Figure 14:


## 3.1.1 Compromise of diagnostic system components

**reputation degradation lawsuit significant feeling of invasion of privacy phishing attempts, or targeted advertising unique targeted opportunities.**

### 3.1.2 Evasion

reputation degradation, lawsuit, and physical and permanent injury

### 3.1.3 Human error

reputation degradation and lawsuit
significant feeling of invasion of privacy phishing attempts, or targeted advertising loss of unique targeted opportunities

reputation degradation
significant feeling of invasion of privacy phishing attempts, or targeted advertising unique targeted opportunities

### 3.1.4 Data disclosure

- 
- 
- 

reputation degradation and lawsuit
serious feeling of invasion of privacy phishing attempts, targeted advertising loss of unique targeted opportunities .

### 3.1.5 Poisoning (by label modification)

reputation degradation lawsuit
physical and permanent injury

### 3.1.6 Unlawful Processing

a significant feeling of invasion of privacy

### 3.1.7 Unfair processing

with discriminations created by the treatment such as
better diagnosis of osteoporosis for men than for women, for example.

a feeling of infringement of fundamental rights.

### 3.1.8 Lack of transparency

significant feeling of invasion of privacy.

### 3.1.9 Diversion of purpose

targeted advertisements
significant feeling of invasion of privacy unique
targeted opportunities.

### 3.1.10 No respect of data minimisation

significant feeling of invasion of privacy

### 3.1.11 No respect of accuracy

temporary or permanent physical injury of the patient.

### 3.1.12 No respect of storage limitation

targeted advertising unique targeted opportunities.

### 3.1.13 No respect of compliance of the training model

reputation degradation lawsuit significant feeling of invasion of privacy phishing attempts, or targeted advertising unique targeted opportunities.

### 3.1.14 Synthesis of possible impacts and associated threats

**Figure 1:**

| Impact | Severity | Type | Associated Threats |
|---|---|---|---|
| Physical and permanent injury and harm | High | | |
| Lawsuit | High | | |
| Reputation degradation | High | | |
| Phishing attempts, targeted advertising | High | | |
| Loss of unique targeted opportunities | High | | |

| | | | |
|---|---|---|---|
| | | | |
| Significant feeling of invasion of privacy | Moderate | | |
| Feeling of infringement of fundamental rights | Moderate | | |

## 3.2 VULNERABILITIES ASSOCIATED TO THREATS AND AFFECTED ASSETS

**Figure 2:**

| Vulnerabilities | Threats | Actors | Assets Involved |
|---|---|---|---|
| Absence of an identified data controller | | | |
| Contract with a low security third party | | | |
| Disclosure of sensitive data for ML algorithm training | | | |
| Existing biases in the ML model or in the data | | | |
| Lack of auditability of processing | | | |
| Lack of accuracy criteria | | | |
| Lack of documentation | | | |

| | | | |
|---|---|---|---|
| | | | |
| **Lack of pseudonymisation** | | | |
| **Lack of consideration of attacks to which diagnostic systems could be exposed** | | | |
| **Lack of consideration of real-life conditions in training the model** | | | |
| **Lack of control for poisoning** | | | |
| **Lack of control of Data processor (including external stakeholder)** | | | |
| **Lack of control over model performance** | | | |
| **Lack of controls to ensure that data is used only for the purposes defined** | | | |
| **Lack of controls to ensure that the data collected are minimal for the purposes intended** | | | |
| **Lack of controls to ensure the adequacy of the purpose and its current use** | | | |

| | | | |
|---|---|---|---|
| **Lack of data deletion mechanisms** | | | |
| **Lack of data for increasing robustness to poisoning** | | | |
| **Lack of data retention policy** | | | |
| **Lack of detail on the purposes and justification for their legitimacy** | | | |
| **Lack of detection of abnormal inputs** | | | |
| **Lack of justification and traceability of decisions taken** | | | |
| **Lack of justification for the collection of individual personal data collected** | | | |
| **Lack of measures to prevent further data collection** | | | |
| **Lack of necessary data selection** | | | |
| **Lack of practical means and justification for the legal basis (legitimate interest)** | | | |
| **Lack of security by design** | | | |
| **Lack of privacy by design** | | | |
| **Lack of review of treatment by a dedicated committee to check fairness** | | | |

| | | | |
|---|---|---|---|
| **Lack of security process to maintain a good security level of the components of the diagnostic system** | | | |
| **Lack of traceability of actions and/or modifications made to the assets on which rely personal data** | | | |
| **Lack of training based on adversarial attacks** | | | |
| **Lack of transparency on the purpose, the exact data that are collected, and how they are processed.** | | | |
| **Lack of verification that the data is adequate, relevant and not excessive for the purpose of making a diagnostic** | | | |
| **Model easy to poison** | | | |
| **No detection of poisoned samples in the training dataset** | | | |
| **Poor consideration of evasion attacks in the model design implementation** | | | |
| **Poor access rights management process** | | | |

| | | | |
|---|---|---|---|
| **Poor data management** | | | |
| **Too much information available on the model** | | | |
| **Unprotected sensitive data on test environments** | | | |
| **Use of uncontrolled data** | | | |
| **Use of unreliable sources to label data** | | | |
| **Use of unsafe data or models (e.g., with transfer learning)** | | | |

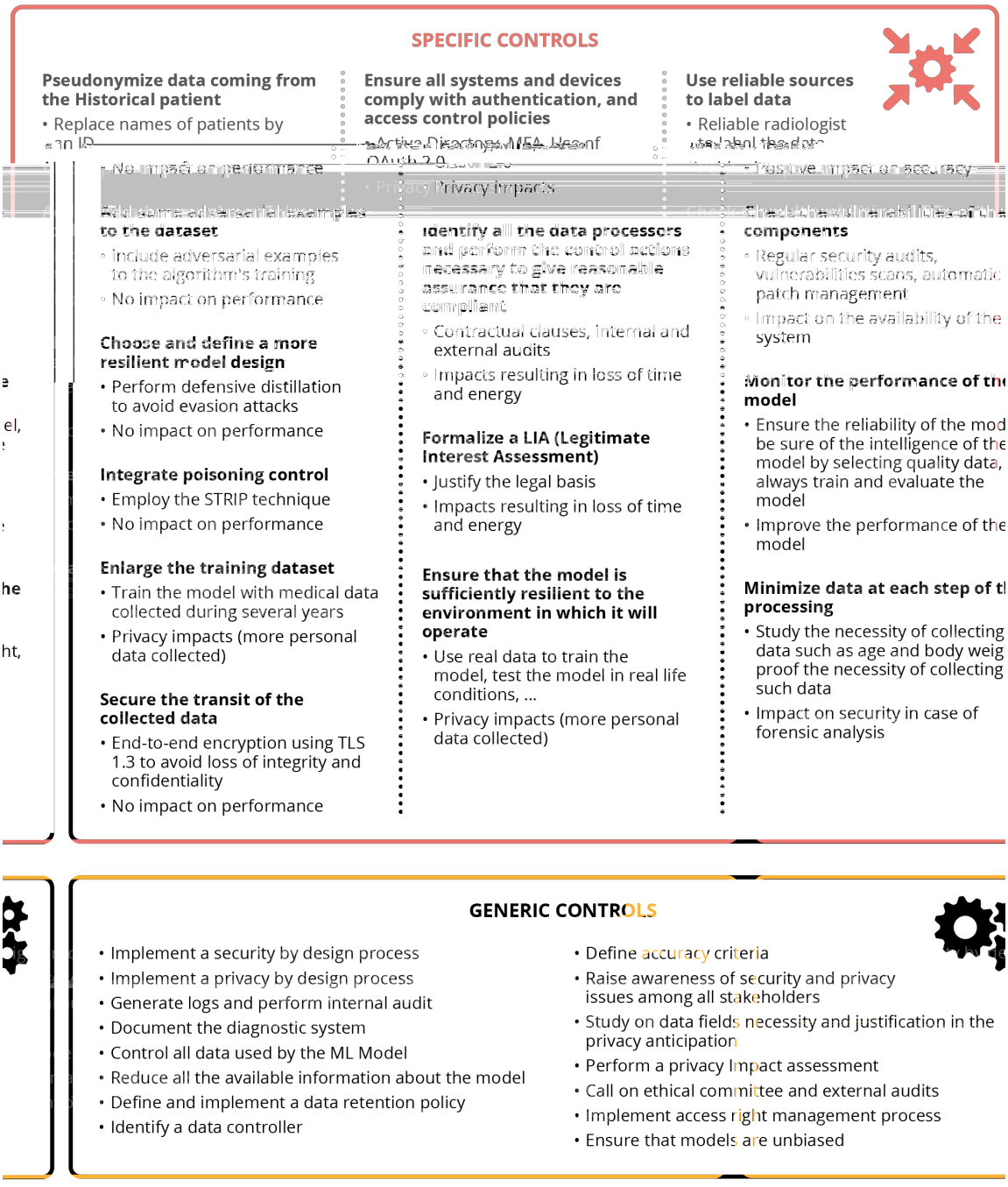
[redacted]

[redacted]

[redacted]

[redacted]

**Figure 17:**


SPECIFIC CONTROLS
Pseudonymize data coming from the Historical patient
• Replace names of patients by
Ensure all systems and devices comply with authentication, and access control policies
Use reliable sources to label data
• Reliable radiologist
• No impact on performance
• Privacy Impacts
• Positive impact on accuracy
Add some adversarial examples to the dataset
• Include adversarial examples to the algorithm's training
◦ No impact on performance
Choose and define a more resilient model design
• Perform defensive distillation to avoid evasion attacks
• No impact on performance
Integrate poisoning control
• Employ the STRIP technique
• No impact on performance
Enlarge the training dataset
• Train the model with medical data collected during several years
• Privacy impacts (more personal data collected)
Secure the transit of the collected data
• End-to-end encryption using TLS 1.3 to avoid loss of integrity and confidentiality
• No impact on performance
Identify all the data processors and perform the control actions necessary to give reasonable assurance that they are compliant
◦ Contractual clauses, internal and external audits
◦ Impacts resulting in loss of time and energy
Formalize a LIA (Legitimate Interest Assessment)
• Justify the legal basis
• Impacts resulting in loss of time and energy
Ensure that the model is sufficiently resilient to the environment in which it will operate
• Use real data to train the model, test the model in real life conditions, ...
• Privacy impacts (more personal data collected)
components
◦ Regular security audits, vulnerabilities scans, automatic patch management
◦ Impact on the availability of the system
model
• Ensure the reliability of the mod be sure of the intelligence of the model by selecting quality data, always train and evaluate the model
• Improve the performance of the model
processing
• Study the necessity of collecting data such as age and body weig proof the necessity of collecting such data
• Impact on security in case of forensic analysis
GENERIC CONTROLS
• Implement a security by design process
• Implement a privacy by design process
• Generate logs and perform internal audit
• Document the diagnostic system
• Control all data used by the ML Model
• Reduce all the available information about the model
• Define and implement a data retention policy
• Identify a data controller
• Define accuracy criteria
• Raise awareness of security and privacy issues among all stakeholders
• Study on data fields necessity and justification in the privacy anticipation
• Perform a privacy Impact assessment
• Call on ethical committee and external audits
• Implement access right management process
• Ensure that models are unbiased

## 4.1 IMPLEMENT A SECURITY BY DESIGN PROCESS

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • |

## 4.2 DOCUMENT THE DIAGNOSTIC SYSTEM

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • |

**This control does not impact system performance, cybersecurity, or privacy.**

## 4.3 CHECK THE VULNERABILITIES OF THE COMPONENTS USED AND IMPLEMENT PROCESSES TO MAINTAIN SECURITY LEVELS OF ML COMPONENTS OVER TIME

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br> • <br> • | • <br> • |

**This control would impact the availability of the system, thus its performance, as it may be audited or even updated.**

## 4.4 ADD SOME ADVERSARIAL EXAMPLES TO THE DATASET

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

**This control does not impact performance or privacy.**

## 4.5 CHOOSE AND DEFINE A MORE RESILIENT MODEL DESIGN

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

This control does not impact performance or privacy.

## 4.6 INTEGRATE POISONING CONTROL IN THE TRAINING DATASET

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br> • | |

This control does not impact system performance, cybersecurity, or privacy.

## 4.7 ENLARGE THE TRAINING DATASET

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

In this case, privacy is negatively impacted because enlarging the data set means taking even more personal data which could be stolen by an attacker.

## 4.8 SECURE THE TRANSIT OF THE COLLECTED DATA

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|

| | | |
|---|---|---|
| | | |

**This control won't have any impact on privacy or performance of the system.**

## 4.9 CONTROL ALL DATA USED BY THE ML MODEL

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• | |

## 4.10 IMPLEMENT ACCESS RIGHT MANAGEMENT PROCESS

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • <br>• <br>• <br>• |

## 4.11 ENSURE ALL SYSTEMS AND DEVICES COMPLY WITH AUTHENTICATION, AND ACCESS CONTROL POLICIES

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • | • <br> • <br> • <br> • |

## 4.12 MONITOR THE PERFORMANCE OF THE MODEL

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| **Cybersecurity** | | • <br> • |

This will have an impact on the performance of the model in the sense that by applying this control, the model is always efficient and reliable.

## 4.13 REDUCE THE AVAILABLE INFORMATION ABOUT THE MODEL

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br> • | |

This control could have an impact on privacy

## 4.14 IDENTIFY A DATA CONTROLLER FOR THE MEDICAL DATA PROCESSING

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • <br> • <br> • |

the control improves the privacy of users without impacting the performance of the model.

## 4.15 PSEUDONYMISE DATA COMING FROM THE HISTORICAL PATIENT

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• | |

**This control does not impact on security or performance.**

## 4.16 GENERATE LOGS AND PERFORM INTERNAL AUDIT

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• <br>• | • <br>• <br>• <br>• <br>• <br>• |

## 4.17 IDENTIFY ALL THE DATA PROCESSORS FOR THE MEDICAL DATA PROCESSING AND PERFORM THE CONTROL ACTIONS NECESSARY TO GIVE REASONABLE ASSURANCE THAT THEY ARE COMPLIANT

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br> • | • <br> • |

**The impact this control could have for the medical practice would be a loss of time and energy spent to formalise documents, and complete the assessments and audits.**

## 4.18 PERFORM A PRIVACY IMPACT ASSESSMENT

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br> • <br> • | |

**Such analysis may possibly impact the performance of the scenario**

## 4.19 DEFINE AND IMPLEMENT A DATA RETENTION POLICY

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• | |

**this control can have an impact on the performance of this scenario.**

## 4.20 STUDY ON DATA FIELDS NECESSITY AND JUSTIFICATION IN THE PRIVACY POLICY

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• | • <br>• <br>• |

## 4.21 FORMALIZE A LIA (LEGITIMATE INTEREST ASSESSMENT)

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| **Privacy** | • <br>• | |

| | | |
|---|---|---|
| | • | |

## 4.22 MINIMISE DATA AT EACH STEP OF THE PROCESSING; COLLECT ONLY WHAT IS NEEDED WHEN NEEDED

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | • <br>• <br>• | |

## 4.23 IMPLEMENT A PRIVACY BY DESIGN PROCESS

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • <br>• <br>• <br>• <br>• |

## 4.24 CALL ON ETHICAL COMMITTEE AND EXTERNAL AUDITS

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

## 4.25 DEFINE ACCURACY CRITERIA

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

**Such a measure does not affect this scenario.**

## 4.26 ENSURE THAT THE MODEL IS SUFFICIENTLY RESILIENT TO THE ENVIRONMENT IN WHICH IT WILL OPERATE

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

- 
- 
- 

- 

## 4.27 RAISE AWARENESS OF SECURITY AND PRIVACY ISSUES AMONG ALL STAKEHOLDERS

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | • |

This control does not directly impact performance of the system.

## 4.28 USE RELIABLE SOURCES TO LABEL DATA

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

This control will have a positive impact on accuracy since the dataset will be correctly labelled.

## 4.29 ENSURE THAT MODELS ARE UNBIASED

| Type | Associated Vulnerabilities | Threats it mitigate |
|---|---|---|
| | | |

| | | |
|---|---|---|
| | | |

**This privacy control could improve performance of the system over longer periods**

## 4.30 SUMMARY

**Figure 18:**

| Control name and type | Associated Vulnerabilities | Threat mitigated | Privacy and security requirements addressed |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |

**medical imaging in osteoporosis diagnosis supported by Artificial Intelligence (AI) is presented**

**AI can be very beneficial for the industries areas it applies to, it can also have quite a significant impact for security and privacy**

**depending on the context of the scenario, the same threats apply differently and have different levels of impact.**

**the entire cybersecurity and privacy context (requirements, threats, vulnerabilities, and controls) must be adapted to the context and reality of the individual organization**

## A.1 CYBERSECURITY AND PRIVACY SEVERITY SCALES

| Availability | |
|---|---|
| Low | few days or less |
| Moderate | a day or less |
| High | half a day or less |
| Critical | few hours or less |

| Integrity | |
|---|---|
| Low | does not need to be identified or corrected |
| Moderate | must be identified but not necessarily corrected |
| High | must be identified and corrected |
| Critical | No degradation |

| Confidentiality | |
|---|---|
| Low | accessed by everyone |
| Moderate | restricted to internal staff and trusted partners |
| High | restricted to employees having an organisation or functional link with the process |
| Critical | restricted to a very limited number of individuals |

| Traceability | |
|---|---|
| Low | absence of traces is acceptable |
| Moderate | Actions identified |
| High | actions actors identified and dated imputable |
| Critical | actions legally enforceable time stamped probative value |

## A.2 CYBERSECURITY SCALE OF IMPACT

| Severity[29] | |
|---|---|
| 1 - Low | |
| 2 - Moderate | |
| 3 - High | |
| 4 - Critical | |

## A.3 PRIVACY SCALE OF IMPACT

| Severity[30] | |
|---|---|
| 1 - Low | |
| 2 - Moderate | |
| 3 - High | |
| 4 - Critical | |

## A.4 PRIVACY REQUIREMENTS CRITERIA

| Requirements | Article |
|---|---|
| Lawfulness, fairness and transparency | |
| Purpose limitation | |
| Data minimisation | |
| Accuracy | |
| Storage limitation | |
| Security of personal data (integrity and confidentiality) | |

| Recommendations | Details |
|---|---|
| Database creation | |
| Compliance of the training model (i.e. before production) | |

## ABOUT ENISA

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
Agamemnonos 14, Chalandri 15231, Attiki, Greece

**Heraklion Office**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu