# ICOPEV

5TH INTERNATIONAL CONFERENCE ON PRODUCTION ECONOMICS AND PROJECT EVALUATION

2022

# CONFERENCE PROCEEDINGS BOOK

29 – 30 SEPTEMBER 2022

**POLYTECHNIC INSTITUTE OF CASTELO BRANCO,**
CASTELO BRANCO, PORTUGAL

# INNOVATION AND KNOWLEDGE TRANSFER FOR MONITORING, PREDICTING AND PREVENTING PRESSURE ULCERS: THE SENSOMATT APPROACH

## Keywords:

Pressure ulcer, Artificial intelligence, Security and privacy requirements

## Authors:

Arlindo Silva,[1,2*]
Osvaldo Santos,[1,2]
Fernando Reinaldo,[1,2]
Filipe Fidalgo,[1,2]
José Metrôlho,[1,2]
Mohammad Amini,[3]
Luís Fonseca [1]
Rogério Dionísio[1,2]

[1] Polytechnic Institute of Castelo Branco, Castelo Branco, Portugal

[2] DiSAC – Digital Services, Applications and Contents, Castelo Branco, Portugal

[3] SensoMatt Lda, Castelo Branco, Portugal

***Corresponding author:**
rdionisio@ipcb.pt,
Polytechnic Institute of Castelo Branco, Castelo Branco, Portugal

## Abstract:

Pressure ulcers are skin injuries that develop mainly over bony areas as the result of prolonged pressure caused by the immobility of bedridden patients. They constitute not only a source of additional suffering for these patients but also contribute to the burnout of healthcare professionals who must maintain continuous monitoring of these patients. Data from countries such as the UK or the USA allows the cost of this problem to be estimated to be, respectively, near £2 billion and $80 billion. In this article, we describe the SensoMatt approach to pressure ulcer prevention and management, which is being developed as a research project that includes partners from industry, healthcare, and academia. The SensoMatt solution is centered on a pressure sheet that is placed under the patient's mattress, complemented by an online management portal and a mobile app. These provide patients and healthcare providers with an unparalleled set of services that include personalized analysis, prevention warnings and recommendations.

# INTRODUCTION

Pressure ulcers (PUs) are injuries to the skin and underlying tissues resulting from prolonged pressure on the skin, which often develop over bony areas, such as hips, ankles, or tailbone (Bluestein and Javaheri, 2008). They are also called bedsores or decubitus ulcers. Healthcare professionals are required to closely monitor people who are at risk of developing pressure ulcers, since timely and accurate prediction of pressure injury risk can significantly facilitate early prevention and treatment and avoid adverse outcomes (Garcia and Thomas, 2006). Even with careful prevention, PUs will still frequently develop, after which close monitoring remains essential to avoid worse consequences.

Data from healthcare systems that keep accurate statistics on the problem can help us better understand its dimension. In the UK, every year, roughly 7 million people are treated by the NHS for PU issues at a cost of £1.4 to £2.2 billion. The estimated cost for treating a single patient varies from £1,064 to £10,551, depending on the seriousness of the issue. This makes PU related problems the most expensive chronic wound issue faced by the NHS (Coleman et al., 2016).

Pressure ulcers are a health problem that causes immeasurable physical and emotional suffering for patients, increases the health systems' costs, and contributes to healthcare professionals stress and eventual burnout. As such, many approaches have been proposed to ameliorate the issue, with none being yet totally successful (Ribeiro et al., 2021) (Silva et al., 2022).

The SensoMatt project, proposes a new and different approach to tackle this long-standing problem, by emphasizing prediction and prevention in a technically innovative context over more traditional approaches. On the hardware side, a thin sensor sheet is placed underneath the mattress of a bedridden person to monitor and measure the patient's pressure distribution in real time. Custom software, supported by machine learning techniques, analyses sensor data to identify risk patterns, raise alarms, and produce predictions and recommendations. Personalized data and analysis is stored in the cloud and can be accessed by healthcare providers using a mobile app. A management portal enables administrators to make informed decisions regarding patients, staff, and equipment. The goal of the project is to help predict future PU occurrences, reduce the effects of existing ones, and decrease the costs for healthcare systems and providers.

# CURRENT PU PREVENTION PROCEDURE

Tackling PUs has led to many efforts over decades to create reliable and practicable manual risk assessment methods, and technology-based answers.

On the manual side, hospitals use a number of techniques for dealing with PUs. The cycle usually starts with risk assessment, widely performed today with the Braden (1987), Norton (1962) or Waterlow (1985) methods. However well these are applied, they rely fully on human observation, procedures, data collection, and care; in short, they are costly, prone to error, and burden an already burdened staff. While scientifically sound, they lie technologically at the opposite end of an AI-based, automated, and predictive risk assessment solution.

The cycle proceeds to monitoring PUs, and then either preventing or curing sores, or a combination of both. Perfect monitoring being impossible, some PUs are bound to appear; that no

two patients are alike only compounds the problem. Nursing staff continue monitoring the patient, possibly revising procedures and repositioning frequency, often in almost reactive mode.

These shortcomings have been spurring technology-based answers that make today's competitive landscape, essentially composed of passive devices that extend nursing's reach. Most measure the parameters of one of the methods, using their sensors, calculate margins, and give the nurse a list of risk factors and a measure thereof. However, the parameters are still quite qualitative, and the assessment picture may be undesirably incomplete. They cannot be relied upon to handle assessment by themselves. Table 1 present a sample of the current market offer with a list of features (o: available; x: not available).

## THE SENSOMATT SOLUTION

SensoMatt hardware is a battery-powered, air-bubble sensor matrix to be placed underneath a bed mattress, with each sensor measuring a pressure value, as shown in Figure 1. Taken together, the constantly updated values make up a pressure map, which is converted into digital form to be sent wirelessly over the Internet to the cloud server. SensoMatt software then analyses that data and converts it into a body contour to be fed to the Machine Learning (ML) engine. The last stage consists of the Artificial Intelligence (AI) module analysing the ML output for risk patterns and making decisions and predictions on it.

It is designed to be placed underneath the mattress, which is more than an innovative detail. SensoMatt design and development are meant to give it self-healing properties: if a sensor within a bubble breaks down or a bubble gets punctured and leaks, a no-or abnormal-reading condition is decided, and the error reported. Until the sensor is repaired, readings from the adjacent sensors are used to weigh its pressure profile. At a fixed, standard (80 cm) width, SensoMatt is customizable in length, number of sensors, shape or special requirements (e.g. having sensor-free areas). The mobile app and the management portal are customizable too. The app's user interface is fully brandable: clients can add their own logo and theme. A new patient is automatically sized up and learned in a number of dimensions; their initial data is read, and keeps being updated, after which SensoMatt acts upon it, offering predictions, producing recommendations and informing medical decisions by using state-of-the-art AI and ML algorithms.

Medical and caregiving staff may then follow the resulting recommendations aided by an interactive mobile-app interface.

SensoMatt direct end users use a mobile app to access any patient's data and recommendations after AI has analysed their movements and pressure distribution.

Table 1

Commercial brands with actual offer on PU.

| Brand | Description | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Under mattress | Tracks Sleep | Prevents PUs | Senses pressure | General usage | Measures Weight | Uses AI | Mobile App |
| BodyFitter | x | x | x | o | x | x | x | x |
| | Meant for mattress manufacturers and retailers to measure pressure distribution and magnitude. (bodyfittersystem.com). | | | | | | | |
| Luna | x | o | x | x | o | x | o | o |
| | Mattress-top cover that learns sleep habits and cycles by tracking heart and breathing rates, and bed temperature changes. (lunamattress.com). | | | | | | | |
| Sleepace | x | o | x | x | o | x | o | o |
| | Records heart and breathing rates, movement, and sleep cycles during sleep and suggest habits that will result in better sleep. (sleepace.com). | | | | | | | |
| Aura | o | o | x | x | o | x | o | o |
| | The pad tracks sleep patterns and the light and sound programs help the user transition to sleep at night and wake up in the morning. (amazon.com). | | | | | | | |
| Reveal | x | x | x | o | x | x | x | x |
| | Uses pressure imaging technology to serve the mattress retail industry, (www.nbn.at). | | | | | | | |
| Vive | x | x | x | o | o | x | x | x |
| | Alternating pressure mattress designed to provide PU relief. (amazon.com). | | | | | | | |

Data and recommendations include repositioning time and periods, nutrition, and considerations particular to that patient, along with their possible history. The app can convey management or supervision orders from senior staff. SensoMatt provides its indirect end users with a portal where they can manage the SensoMatt beds, follow-up on patients, obtain instant statistics, and get preventive warnings. Knowing which beds are active and in use, which staff cares for which patient and how either is doing, and which patients are priority, becomes routine. All information and data are stored, and all calculations and analysis performed, in the cloud, for reliability, security, versioning, and compliance.

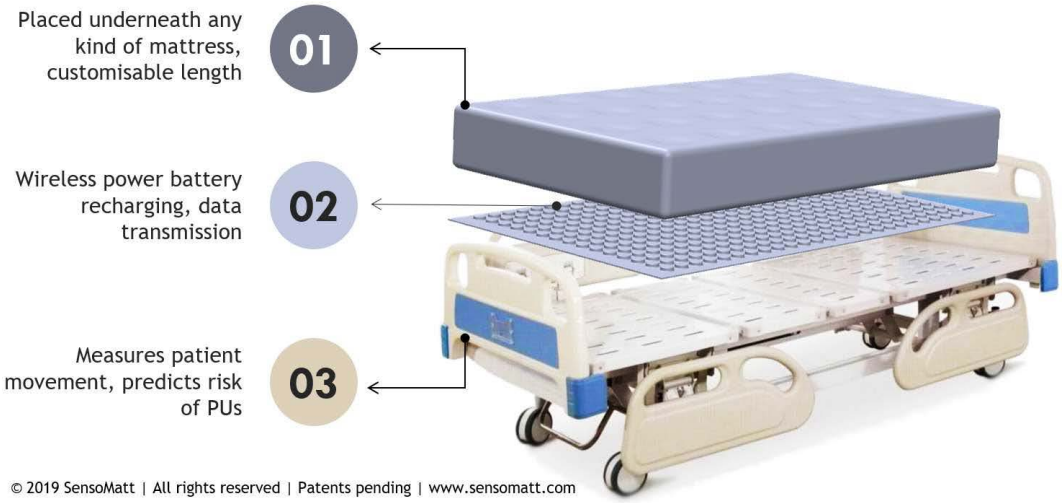


Figure 1

SensoMatt Hardware.

## IoT Requirements

For a clear design and implementation of Sensomatt, we identified a collection of functional and non-functional IoT requirements that describe precisely all aspects and functionalities of the product. They are divided into two main sections: General Requirements and Health Requirements, inwspired by four different themes:

1. Security and privacy;

2. Performance and environmental needs;

3. Architectural components and elements; the standard layers for health systems are usually three:

    a) Device;
    b) Gateway;
    c) Server.

4. User interface, services and functionalities for health roles (patients, caregivers, doctors and administrators).

To describe each IoT requirement, a template was created and it is organized as follows:

- Requirement ID: Unique identifier that reflects the type of requirement (NF-nonfunctional, F – Functional), the kind of requirement (Generic-G or Health-H related) and the number of the requirement;

- Title: Short sentence describing the requirement;

- Description: Short text describing the requirement;

- Priority: Defines the priority of this requirement. It should be classified as high, medium, or low;

- Acceptance criteria: Conditions that requirement must satisfy to be accepted;

- Change History: Shows each change of the requirement within a timeline. It includes information that identifies the version of the requirement, date it was created/changed and who the authors of the change were.

## Data Protection Requirements

Clinical activities, includes gathering participants' data and determining what is a valid significant number of experiments to perform to validate the research in PU prevention and risk assessment.

As this activity involves the collection of clinical data from the participants in the clinical trial (hereby designated as patients), it is necessary to comply with the GDPR and its principles. The data controller will ensure compliance by defining an explicit data privacy policy and verify its enforcement.

This section contains the main guidelines of the data privacy policy.

### Definition of the GDPR Controller / Processor

Both the data controller and processor roles are assigned to the legal person SensoMatt, which will determine the purposes and means of the processing of personal data, and also process the actual personal data.

The controller is not an individual within the project, but the project as such. All the members of the project staff abide by the controller's duties.

### Informed Consent

The lawfulness of processing of personal data within this project will be based on consent, hence the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. Informed consent guarantees the person's voluntary participation and ensures that the person can withdraw at any time. The entire procedure will be explained, and the participants will be given all the pertinent information by the researchers, who will be available to answer any questions about it.

Informed consent must be written, dated, and signed by each person who participates in the clinical trial of Activity A5. Each person will be free to accept it after being duly informed about its nature, meaning, implications and risks. The document must be signed by any person capable of giving consent or, when the person is unable to give consent, by his legal representative. If the person concerned cannot write, oral consent in the presence of at least one witness can be given in exceptional cases, as provided for by national law.

### Anonymization / Pseudonymization of Sensitive Patient's Data

This project gathers sensitive patient's data, hence special care must be taken to ensure its confidentiality. The patient's data is separated into three different domains:

- Patient's identification: this will hold the patient's identification, namely full name, gender, date of birth, address, email, and telephone number;

- Patient's health data: this will hold the patient's health records, especially those concerning pressure ulcers;

- Mattress data: this will store the data coming from the sensors embedded in the mattress.

These three domains will be stored independently and managed with different access and anonymization policies, to protect the patient's identification. As the first domain contains the patient's personal information, it will be decoupled from the other two domains, and a restricted access policy will be applied to it. Each patient will be given a random identifier (pseudonym), which will be used in the other two domains to identify the patient.

All data of the other two domains will be processed in a automated way, using the pseudonym to identify each patient. These domains will not allow the unequivocal identification of the participant. The data of each participant will not be treated individually, but only as aggregated data, in order to identify patterns and trends.

The research team ensures that there is no conflict of interest and complies with the information contained in the Helsinki declaration.

## Confidentiality, Integrity, and Authenticity of the Collected Data

The confidentiality, integrity, and authenticity of the collected data must be ensured during transmission and storage. This can be achieved using the following cryptographic algorithms recommended by NIST (NIST, 2020):

Table 2

Recommended cryptographic algorithms.

| Principle | Algorithms |
|---|---|
| **Confidentiality** | AES128, AES 192, AES256<br>CBC mode to provide only confidentiality.<br>CCM or GCM mode to provide confidentiality and authentication. |
| **Hashing** | SHA256 |
| **Integrity** | HMAC with AES and SHA256 |
| **Integrity and authenticity** | ECDSA<br>HMAC with AES and SHA256 |

These algorithms can be used directly by the developed software or indirectly when they are incorporated into secure technologies such as TLS or DDS.

## Data Access Policy

One way to protect personal data is enforcing a least privilege policy. This principle states that users should be assigned only the minimum necessary rights to perform their duties, and only for the shortest duration necessary to accomplish their tasks. Basically, if a user does not need an access right, he should not have that right.

In the context of this project, the least privilege policy can be used to protect the patients' actual identification, by restricting the access to their personal information. Therefore, the roles and access rights in Table 3 should be used. The GDPR controller will be assigned the administrator role in order to accomplish the responsibilities described in this document.

Table 3
Roles and data access policy.

| Role | PI | PHD | MD |
|---|---|---|---|
| **Administrator** | CDRW | CDRW | CDRW |
| **Manager** | CDRW | CDRW | |
| **Nurse** | | RW | R |
| **Technician** | | | R |
| **Sensor** | | | CW |
| **Medical** | | CRW | R |
| **Researcher** | | R | R |
| **Others** | | | |

PI: Patient's identification; PHD: Patient's health data (pseudonymized); MD: Mattress data (pseudonymized)

C – Create, D – Delete, R – Read, W – Write

### Audit Policy

All data access should be registered and timestamped, and the id of the user who performs the access must be recorded as well. The controller must periodically audit the log system to ensure that there are no violations of the data access policy.

### Population / Participants

Study participants will be individuals over 18 years old from the community who want to participate voluntarily in the study after signing informed consent. They will be selected randomly upon registration, from those who agree to participate in the study and meet the inclusion criteria.

## Security Requirements

This section provides an overview of several procedures that are crucial to ensure the project's security and compliance with key GDPR's requirements. These procedures are aligned with two of the most popular cloud platforms: Amazon Web Services (AWS) and Microsoft Azure.

### Cloud Account Protection

Cloud based applications are developed and maintained through administrative access to the project being deployed over a specific cloud platform, using one or more administrative accounts. Those users usually have privileges to create, change and delete resources such as virtual machines, databases, containers, virtual networks, and other typical cloud resources. Given that these accounts allow highly privileged access to the project's resources, securing it is paramount.

In addition to the typical security measures commonly applied to passwords (choosing a strong password, avoiding login in insecure devices, safeguarding password exposure) there are some additional procedures that can be applied to strengthen the cloud accounts' security, namely:

- Enable MFA for the root account;
- Limit root user access;
- Disable root access keys;
- Implement a least privilege policy;
- Avoid disclosing access keys in code.

The first and most important security measure to apply to the root account is to set up a multi factor authentication (MFA) device to protect the account from remote attacks such as password guessing or phishing. Setting up MFA is a simple yet powerful best practice that adds an extra layer of protection on top of the typical username and password authentication.

Another best practice that should be followed is limiting root user access (password and API access keys), as this grants unlimited access to the account and its resources. For day-to-day access to the cloud framework, the project's staff should use specific accounts created with a least privilege policy, instead of using the root credentials. This is true even if there is only one person accessing the cloud platform. As a matter of fact, ideally the root account should be used only to create other users.

Another aspect that should be considered is the protection of access keys. Access keys are normally used in cloud computing to grant access from specific modules (for example a piece of serverless code) to a cloud resource (for example a database). If the access keys are embedded in the code or in a script, this may represent a security hazard, should the code or script be inadvertently disclosed to unauthorized people. Those who know the access keys can gain access to the corresponding cloud resource, thus it is necessary to protect them.

There are two main best practices to protect access keys: key rotation and key protection. Key rotation is basically changing the access keys for a cloud resource, to block access from unauthorized users that eventually know the current keys. It is advisable to change it periodically (for example every month) or if there is a suspicion they may have been compromised. Both AWS and Azure support manual and automatic key rotation.

Key protection best practices aim to prevent disclosure of access keys to unauthorized people, providing the access keys to the code or scripts in a way that it is not necessary to hard code the access keys. Both AWS and Azure support the following best practices:

- MFA;
- Root account limitation;
- Role based access control;
- Least privilege policy;
- Access keys rotation;
- Access keys protection.

Identity is now considered the primary perimeter for security, thus these best practices related with cloud credentials must be taken seriously.

### Backup and Disaster Recovery Policies

One of the most basic yet vital security procedures is to frequently backup important data. The importance and societal value of digital data is continuously increasing; thus, organizations cannot afford to lose crucial data. To achieve data durability, organizations need to implement business continuity plans (BCP) or disaster recovery plans (DRP), which rely on data backups. Therefore, there must be an automated backup policy that respects the cost constraints while achieving the target recovery requirements in terms of recovery time objective (RTO) and recovery point objective (RPO) (Suguna and Suhasini 2014).

AWS supports backups at every level of data storage. Its Backup service allows customers to centralize and automate data protection across AWS services, including Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, Amazon Relational Database Service (Amazon RDS) databases (including Amazon Aurora clusters), Amazon DynamoDB tables, Amazon Elastic File System (Amazon EFS) file systems, Amazon FSx for Lustre file systems, Amazon FSx for Windows File Server file systems, and AWS Storage Gateway volumes.

AWS Backup enables customers to configure backup policies from a central backup console, where it is possible to define global backup and retention policies that apply to the AWS services, providing automated backup schedules, retention management, and lifecycle management. This removes the need for custom scripts and manual processes. This eases the alignment of the backup strategy with internal or regulatory requirements, such as the GDPR

Microsoft Azure has a similar service, called Azure Backup Service, which can backup data from VMs, managed disks, file shares, databases, blobs and even on-premises data. This service provides centralized monitoring and management, with alerting capabilities

## SENSOMATT APPLICATION SCENARIOS

One of the main goals of the industrial partners of the SensoMatt project is to acquire enough knowledge and experience to take the SensoMatt system to a clinical trial, and later to market. This means that the main use case scenario for this system are healthcare institutions such as hospitals. To facilitate its adoption, the system includes a management portal that provides healthcare professionals with functionalities to manage the SensoMatt beds, follow-up on patients, obtain instant statistics, and get preventive warnings. These functionalities allow easy access to information such as which beds are active and in use, which staff cares for which patient and how either is doing, and which patients are a priority. Managers can access the full history of beds and patients to measure the performance of PU prediction both for specific patients and the healthcare facility as a whole.

Access to information by healthcare providers that are in direct contact with patients is easily done through a mobile app (Android and iOS). If we consider these facts together, it is possible to envision other use case scenarios for the system, such as monitoring elderly or disabled patients that are being taken care of in their own homes. This type of monitoring could be beneficial, not only for the patient, but also for the healthcare provider, which would be under considerably less stress.

Independently of where it is being used, the SensoMatt project will assist healthcare providers in three different but complementary ways, using three different system components. The first component is visualization. Information regarding the status of the patient, as well as historical data, stored in the information system, will be accessible to the healthcare professional using the mobile applications. A major component of the information to be displayed in the visualization component is the pressure map returned by the sensor system. The lying position and possible alarms raised by the sensor system will also be visualized. Besides this extrinsic information, intrinsic data related to pressure ulcer risk will also be accessible. The healthcare professional will also have access to historical data regarding previous alarms, warnings, and occurrences regarding each patient. This will allow the professional to define and follow the execution of a repositioning protocol or any other proceeding that is adequate for a specific patient.

The second component includes alarms generated by the system. Here, the healthcare provider assumes a more passive stance, as these alarms should be actively pushed by the system into the mobile applications. The repositioning alarm is one the most essential aids in PU prevention, since immobilization in the same position for extended periods of time is still the most important risk factor for pressure ulcer occurrence. The caregiver should be able to set personalized time limits for each patient and position, since a unique interval may not be appropriate for a patient with different ulcers with variable degree of gravity. Pressure data can also be used to raise alerts in other possibly dangerous situations. These include detection of the patient leaving the bed (or falling) when no pressure is felt for a given period of time and restlessness (when the patient changes positions more than some limit number of times in a pre-defined period).

The third component is a predictive component that should be able to use Machine Learning techniques on the collected data to provide some prognosis on how the ulceration process will evolve for a given patient for whom intrinsic and extrinsic factors are collected. The healthcare professional can then use this information to choose a protocol that may lead to a better outcome.

## CONCLUSIONS AND FURTHER RESEARCH

In this article, we described a new approach for monitoring, predicting, and preventing pressure ulcers. This research project, called SensoMatt, involves industrial and academic partners in an effort to develop an integrated solution to this problem. SensoMatt includes a new hardware platform centered on a pressure matt, an information system constituted by a management portal and mobile apps and a set of services (personalized analyses, prevention and recommendations) to provide patients and clinical staff with an unparalleled set of tools for tackling PUs.

We presented a brief state of the art of this field, discussing the main challenges in pressure ulcer prevention and management, followed by the description of the SensoMatt solution. The main aspects discussed in the article include the aim and scope of the project, its reference framework and IoT and data protection requirements. Special attention was given to the project's security and compliance with key GDPR's requirements, including an overview of several crucial procedures.

We also described the application scenarios of the proposed solution, both in terms of prospective markets and contributions to the different stakeholders. The industrial partners of the project intend to take the SensoMatt system to a clinical trial, and later to market. This makes the main use case scenarios for SensoMatt to be in healthcare institutions, but the possibly of using the system to monitor patients in their own homes is also discussed.

Current work on the project is mainly targeting the development of the hardware system and the main components of the information system, including the management portal and the mobile apps. As more data is collected and development advances, with the assistance of the healthcare professionals that are also partners in this project, more effort will be applied to the research and integration of the visualization, automated alarms and predictive components.

## ACKNOWLEDGMENT

The research leading to these results has received funding from the Portugal2020 [PO CENTRO 17/SI/2019] under grant agreement No. 70107 [SENSOMATT].

## REFERENCES

Coleman, S., Smith, I. L., Nixon, J., Brown, S., Wilson, L. (2016). Pressure ulcer and wounds reporting in NHS hospitals in England: Part 2 – survey of monitoring systems. *Journal of Tissue Viability 25*(1), 16–25.

Bluestein, D., Javaheri, A. (2008). Pressure ulcers: prevention, evaluation, and management. *American Family Physician*, *78*(10), 1186–1194.

Garcia, A.D., Thomas, D.R. (2006). Assessment and management of chronic pressure ulcers in the elderly. *Medical Clinics of North America*, *90*(5), 925–944.

Silva, A., Metrôlho, J., Ribeiro, F., Fidalgo, F., Santos, O., & Dionisio, R. (2022). A Review of Intelligent Sensor-Based Systems for Pressure Ulcer Prevention. *Computers*, *11*(1),6.

Ribeiro, F., Fidalgo, F., Silva, A., Metrôlho, J., Santos, O., & Dionisio, R. (2021). Literature Review of Machine-Learning Algorithms for Pressure Ulcer Prevention: Challenges and Opportunities. *Informatics 8*(4),76.

NIST, "Advanced Encryption Standard," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

Suguna, S., Suhasini, A. (2014). Overview of data backup and disaster recovery in cloud. *International Conference on Information Communication and Embedded Systems (ICICES2014)*.

# ICOPEV

5TH INTERNATIONAL CONFERENCE
ON PRODUCTION ECONOMICS
AND PROJECT EVALUATION

2022