IMPLEMENTATION OF A DEGRADED PROCEDURE FOR THE IMPLANTABLE MEDICAL DEVICES CIRCUIT AT AMIENS-PICARDIE UNIVERSITY HOSPITAL IN THE EVENT OF AN INFORMATION SYSTEM OUTAGE OR CYBERATTACK

L. Gaudefroy [1], M. Babin [2], A. Petit [1]

[1] Service Pharmacie CHU Amiens Picardie
[2] Service Pharmacie CH Compiègne

gaudefroy.lauriane@chu-amiens.fr

2SPD-023

BACKGROUND AND IMPORTANCE

The increasing digitalization of hospital processes has significantly improved traceability and efficiency but has also increased vulnerability to cyberattacks, particularly ransomware. Implantable Medical Devices (IMDs) require strict traceability for patient safety, regulatory compliance, and medical device vigilance. In case of information system (IS) outage, the IMD circuit is highly exposed, potentially compromising continuity of care and traceability.

AIM AND OBJECTIVES

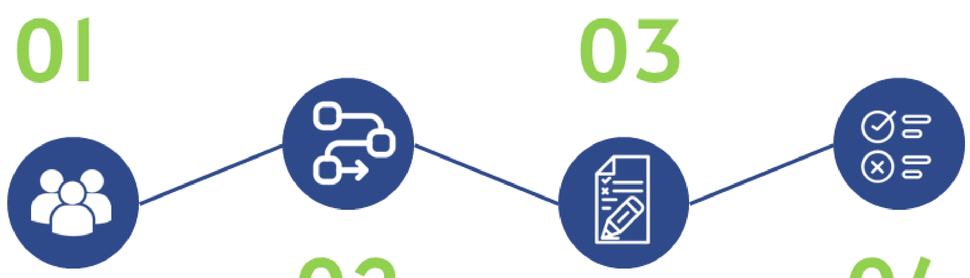
This work, part of the COPIL DMI action plan, aims to **design, implement and test a structured degraded procedure ensuring continuity of IMD supply, traceability, and ordering** in case of major IS outage or cyberattack.

MATERIAL AND METHODS

Multidisciplinary working group

- Hospital pharmacy : pharmacists, pharmacy technicians, quality risk manager
- Operating room managers
- Digital Services Department (DSN)
- Hospital quality department

Design of the degraded process and procedure



Critical steps identified using Failure Mode, Effects, and Criticality Analysis (FMECA)

Procedure tested in a simulated information system outage scenario

RESULTS

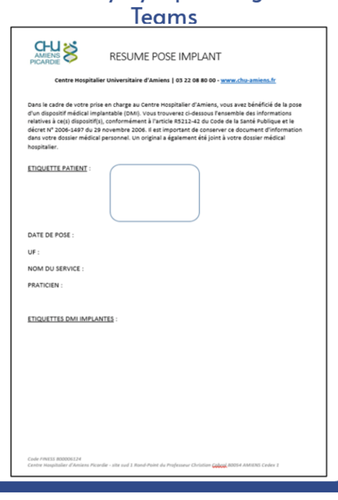
Tools Used

Computer

USB drive:

- Excel® extraction of DMI from Sédistock®
- Excel® extraction of suppliers from Magh-2®
- Excel® extraction of products from Magh-2®
- Word® purchase order
- Downtime procedure for the DMI supply pathway

Traceability by Operating Room Teams


RESUME POSE IMPLANT

Centre Hospitalier Universitaire d'Amiens | 03 22 08 80 00 - www.chu-amiens.fr

Dans le cadre de votre prise en charge au Centre Hospitalier d'Amiens, vous avez bénéficié de la pose d'un dispositif médical implantable (DMI). Vous trouverez ci-dessous l'ensemble des informations relatives à ce(s) dispositif(s), conformément à l'article R5212-42 du Code de la Santé Publique et le décret N° 2006-1497 du 29 novembre 2006. Il est important de conserver ce document d'information dans votre dossier médical personnel. Un original a également été joint à votre dossier médical hospitalier.

ETIQUETTE PATIENT :

DATE DE POSE :

UF :

NOM DU SERVICE :

PRATICIEN :

ETIQUETTES DMI IMPLANTES :

Implant Traceability Check by the Pharmacy Technician

Traceability in the Excel® Order Register

DMI Stock Extraction from Sédistock® for Stock Tracking

Order

Fallback Hospitalis® Solution via Hospisecu if Internet is Available

Word® Purchase Order Generated by Mail Merge


BON DE COMMANDE

FOURNISSEUR : MEDTRONIC FRANCE
ADRESSE : 9 BOULEVARD ROMAIN ROLLAND
75014 PARIS
MAIL : commande@medtronic.com
TEL : 01 55 38 60 60
FAX : 01 55 38 18 89

CHU AMIENS PICARDIE
SIRET : 26800014800125
CHU HOSPITALIER UNIVERSITAIRE
AMIENS PICARDIE
80054 AMIENS CEDEX 1

Reception

Traceability in the Excel® Order Register by Reception Staff and Traceability Agents

The FMECA performed on 10 key steps of the IMD circuit identified **6 high-risk steps** with a criticality score of 32. Most of these critical failures were related to loss of access to digital reference databases, breakdowns in inter-system communication (DXCare®, Magh2®, Gildas®, EDI), and disruption of computerized order transmission and validation.

The degraded procedure, based on **paper documentation and offline Excel® databases**, ensured minimal operational continuity during the simulated outage. However, the simulation revealed a **threefold increase in processing time** (30 minutes per order vs. 10 minutes under standard conditions), associated with increased manual workload and a higher risk of transcription errors.

CONCLUSION AND RELEVANCE

The IMD circuit is highly dependent on hospital information systems and therefore particularly vulnerable during cyberattacks or major outages. Implementing and testing a degraded procedure is essential to ensure continuity of care and minimal traceability compliance. Such preparedness must be integrated into institutional risk management strategies, with strong collaboration between pharmacy, clinical departments and digital services. Future steps include integration into the hospital Business Continuity Plan and regular simulation exercises.