

Safety Case Report – Clinical System Failure

SCiMP

September 2020

Document filename:

Directorate / Programme		Project	
Document Reference			
Director	I Thompson	Status	
Owner		Version	1.2
Authors	S Mclean A Vickerstaff, C Weatherburn,	Version issue date	10/09/20

Document Management

Revision History

Version	Date	Summary of Changes
1.0	03/04/19	First draft
1.1	16/04/19	Brief Comments and reordering by CW
1.2	10/09/20	Revisit plus reflect pandemic impact by AV

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Title	Date	Version

Related Documents

These documents provide additional information and are specifically referenced within this document.

Ref	Doc Reference Number	Title	Version
1		Clinical system failure risk register	10/09/20

Contents

Introduction	4
System Definition / Overview.....	4
Clinical Risk Management System	4
Clinical Risk Analysis.....	4
Clinical Risk Evaluation	4
Clinical Risk Control	5
Summary Safety Statement	5

Introduction

An initial clinical safety based approach to consider the implications for GP practices of the failure of their main clinical IT system.

System Definition / Overview

GP practices in Scotland all use the following GP IT systems:

- An Electronic Paper Record (EPR) system from one of 2 independent private sector providers (EMIS www.emishealth.com or Vision www.visionhealth.co.uk)
- The Docman document management system (www.docman.com) for the capturing, filing and workflowing of letters, results and other content that form part of the patient's medical record

Clinical Risk Management System

The suppliers of GP IT systems have their own clinical risk management systems to ensure the risk of harm to patients is minimised while their systems are in use. GP practices are joint Data Controllers with their local health board for the information held in GP IT. Practices also need to provide for the risk that they may be left without access to GP IT system(s) due to local or remote failure. In this case the practice must consider how to respond to this scenario either as part of a local clinical risk management approach or as part of business continuity planning.

Clinical Risk Analysis

The following hazards were identified which could lead to the loss of GP IT system(s) and the potential for patient harm:

- The practice power supply fails
- The practice LAN server fails
- External communications fail
- Water ingress due to plumbing failure, flooding, impact from neighbours, etc.
- Software failure
- Fire, natural disaster or other catastrophic premises disruption
- Cyber attack

Clinical Risk Evaluation

The initial level of risk against each of these hazards was evaluated and an initial risk register established. The results are summarised below:

		LIKELIHOOD				
		Remote	Unusual	Possible	Probable	Almost Certain
IMPACT	Catastrophic					
	Major	Fire	Cyber attack		System fails	
	Moderate			Server fails	Water ingress	
	Minor		Power fails	Network fails	Comms fail	Software fails
	Negligible					

Clinical Risk Control

See associated Risk Register (Ref. 1) for details of proposed action plans and controls.

The individual practice’s response to each risk will be dependent upon their own local re-evaluation based on particular circumstances. For example, if a practice has an uninterruptible power supply and generator backup then the probability of suffering power failure is reduced, although the potential impact is unchanged.

Another consideration is the expected timescale of any loss of clinical GP IT system(s), this will depend upon local circumstances and how widespread the failure is. If only one practice is affected and the practice is located within the same town/city as their IT support providers they might reasonably expect same day on-site support after reporting a system failure. However remote and rural practices should consider alternative risk controls and more widespread failures may require different approaches.

Changes to working practices implemented in the light of the Covid-19 pandemic mean that consideration should also be given to the impact of system failure on home workers as well of those based on surgery premises.

Summary Safety Statement

The risk evaluation indicates that loss of clinical GP IT systems can have a major impact on the practice and it is probable that this will happen at some time due to a particular hazard occurring. The individual hazards identified do not by themselves give rise to any High level of risk but it is the combination that is of concern.

Further risk evaluation could be carried out to explore further the granularity of proposed response discussed above and to develop alternative proposals to suit practice circumstances.