NHS
Surrey and Borders Partnership
NHS Foundation Trust

Information Governance
18 Mole Business Park
Leatherhead
Surrey KT22 7AD

Tel: 01372 216059
Fax: 01372 217114
Email: IGTeam@sabp.nhs.uk

08 January 2019

ID Number – FOI 6714

Title: Social Engineering

Trust Response:

Question:	Trust Response:
1. Does the organisation have training that covers: 1. Recognising and reporting Phishing emails 2. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc) 3. Disposal of confidential information 4. Dangers of using USB sticks being given away or finding one that looks like it has been dropped	Yes.
2. Does the organisation allow the use of USB sticks?	Yes: Trust encrypted USB sticks
3. Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, ie finance, execs etc)?	Yes
4. Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit? Can you also answer relating to the audits: 1. Where the audits are undertaken would these be organised with the local team manager or the head of department ie the director etc? 2. Would an audit ever be carried out unannounced? 3. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy. 4. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.	Yes: 1. Yes 2. No 3. Refer to file: 'IG_response - 6714_Redacted.pdf' 4. Refer to file: 'template - 6714.pdf'
5. Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?	Yes
6. Does the organisations Exec board receive board level training relating to Cyber Awareness?	Yes
7. How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable): a. Third party application package b. third party Trainer / class room c. eLearning for Health Data Security Awareness d. In house developed package e. Combination of any of the above	• Currently use NHS Health Education England e-learning Data Security and Awareness training package. • An internal in-house package is being developed.

Surrey and Borders Partnership
NHS Foundation Trust

Information Governance

Process and Procedure

Version 1.1

Privacy Reports - SystmOne

Author: [redacted]
Last updated: November 2018

Change History

Title	Draft_Procedure_Document
Author	[redacted]
Reference	
Document Location	
Date of Peer Review Signoff	
Date of Final Authorisation Review Signoff	

Version	Date	Author/Editor	Details of Change
0.1	Jan 2018	[redacted]	All: First Draft
0.2	Nov 2018	[redacted]	Addition of Task List activities

1. Introduction

About this Document

1.1 Purpose

This document describes the process for supporting and ensuring Privacy Reports from SystmOne are downloaded in accordance to established guidelines.

1.2 Background

Privacy reports are produced on a monthly basis for IG team, with details extracted for the IGSG monthly meeting.

Privacy data monitoring is based on data extraction within the TPP/SystmOne reporting parameters. SystmOne access is at a Privacy Officer level.

Data is managed in accordance with IG data management guidelines and processes to ensure confidentiality and data security.

The main types of reports and actions are:

- **Report 1**: External SABP partners with access to SystmOne:
  Monitoring access in accordance to established guidelines: e.g.; Beacon CYPS records for people who use SABP services are aged 25 or less **(2018-1993)**
- **Report 2**: Duplicate record access:
  Staff does not accesses own records/family members (with same family name).
- **Report 3**: As well as the above reports, an additional report is downloaded each month, which details deducted patient access (Privacy messenger records).
- **Action 4:** Tasks on SystmOne: Notification of users accessing records outside the team area

2. Actions:

Report 1: Patient Retrieval Reason audit

Data is downloaded each month (calendar month period), during week 1 following the completion of the month.

Report is accessed by downloading data on Systole:

- Audit> Patient> Patient Retrieval Reason audit
- Period: Full calendar month
- Format: Downloaded from SystmOne as a CVS table;
  Saved: O:\IG Audits\SystmOne general audits as an XLS file
  File Name: Patient retrieval reason – *Month Year*

Report is used to:

- Verify access by SABP partners to SystmOne is in accordance to service guidelines.

- Identify numbers of records access by each service (based on service guidelines);
- Identify numbers of records incorrectly accessed by service records (based on service guidelines);
- Produce a summary monthly report to IG manager to review and report to IGSGS.

Report 2: Failed Patient Retrieval Attempts
Data is downloaded each month (calendar month period), during week 1 following the completion of the month.

Report is accessed by downloading data on SystmOne:

- Audit> Patient> Failed Patient Retrieval Attempts
- Period: Full calendar month
- Format: Downloaded from SystmOne as a CVS table;
  Saved: O:\IG Audits\SystmOne general audits as an XLS file
  File Name: Failed Patient Retrieval Attempts – *Month Year*

Report is used to:

- Verify SABP Staff as listed in the monthly report, are not accessing own records/accessing family records:
- Note:
  Based on assumption of matching staff family name against the family name of the patient;
- Where a family name match is highlighted; run additional match to see if first name of SABP staff matches first name of matched patient.
- Produce a summary monthly report to IG manager to review and report to IGSG.

Report 3: Deducted Patient Access
Data is downloaded each month (calendar month period), during week 1 following the completion of the month.

Report is accessed by downloading data on SystmOne:

- Privacy> Privacy Messenger
- Period: Full calendar month
- Format: Downloaded from SystmOne as a CVS table;
  Saved: O:\IG Audits\SystmOne general audits as an XLS file
  File Name: Deducted Patient Access - *Month Year*
- Notify IG manager report is available.
- Delete from the Privacy Messenger screen the downloaded records (click the Privacy Officer Messages tab)

Issues:

- SABP partner staffing profile changes: Need to ensure records being checked match current staffing.
- Limited audit flexibility: Report 2 assumes family members have same family name.

Action 4: Tasks on SystmOne

Issues:

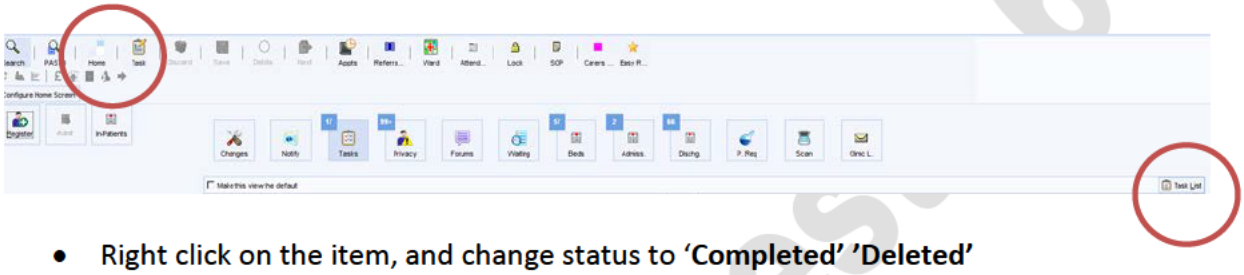
Task List identifies when SystmOne user accesses records outside of team parameters:

Digital Technology may highlight when there are a large number, so need to check occasionally to clear:

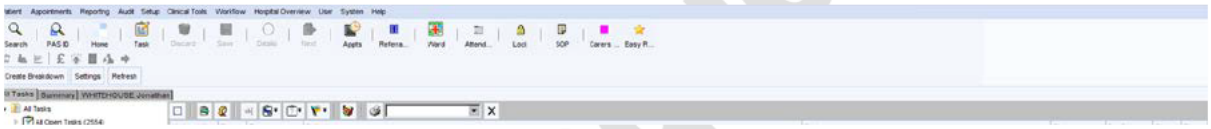
- On Home screen, click the Task List button (right of screen)
- Right click on the item, and change status to '**Completed**'

In addition:

- On Home screen, click Task List



- Right click on the item, and change status to '**Completed**' '**Deleted**'



Checklists:

- **Sussex Perinatal, Eikon and Richmond Fellowship:** Check for updated list of SystmOne access: [redacted] (DT team)
- **Beacon:** Refer to file: **O:\IG Audits\CAMHS\Audit of Failed Pt Retrieval**

SystmOne: Audit Summary: **December 2018**

NHS
Surrey and Borders Partnership
NHS Foundation Trust

Number of records:

	Confirmed	Not confirmed	%
Records confirmed			
Records indicate 25+			
No patient listed			
Multiple records			

Number of records:

	Confirmed	Not confirmed	%
Records confirmed			

Number of records:

	Confirmed	Not confirmed	%
Records confirmed			

Number of staff: Month:

Staff Records: Staff/Patient

Shared surname		
Same name & surname		