Southern Hampshire
PRIMARY CARE ALLIANCE

Statement of Confidentiality

1.1

Version Control

Version	Date	Author	Change Summery
1.1	21/07/2022	L Busher	Formatting changes and review

STATEMENT OF CONFIDENTIALITY

INSTRUCTIONS: This statement is to be read and signed in DUPLICATE by all personnel including agency staff, interims, contractors and volunteers immediately they first start with Southern Hampshire Primary Care Alliance (SHPCA). There is a separate version for researchers. One copy to be retained by the signatory and one copy to be held by SHPCA.

INTRODUCTION

1. All employees/engagements including agency staff, interims, contractors and volunteers are responsible for maintaining confidentiality. This duty of confidentiality forms part of your employment/engagement contract. Breach of information gained in the course of duty may lead to disciplinary action that could result in dismissal. You should also be aware that regardless of any disciplinary action taken, a breach of confidence could also result in civil action for damages.

2. In the course of your duties you may have access to confidential information. This will include information about patients, clients, staff records, details of contract prices and terms and other business sensitive data.

3. Gaining access or attempting to gain access to information that you do not need to see to carry out your work is a breach of confidentiality, as is passing information on to someone who is not authorised to receive it.

4. You must not, whether during or after your employment/engagement with SHPCA, unless expressly authorised by the Accountable Officer, make any disclosure to any unauthorised person or use any confidential information relating to the business affairs of the Organisation. This includes any detail about SHPCA clients and employees, actual, potential or past and all details relating to information on any of SHPCA's databases.

BASIC PRINCIPLES

5. Generally personal information given for one purpose must not be used for another purpose without the consent of the person concerned because that use may breach confidentiality.

6. Everyone has a legal right to know what information is being collected about them and why, and the purposes for sharing that information.

7. For patients, consent cannot be implied for purposes other than healthcare. Non-healthcare purposes could include disclosure to the police, to government departments other than the Department of Health, to the courts, etc. In most cases, patients should be asked for their explicit consent before information is shared for non- healthcare purposes. Seek advice if you are not sure whether specific consent is required.

8. Every individual has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it and to follow the rules and guidance available to them.

9. The rules are there to protect both patient and staff but they should not be applied so rigidly that they are impractical to follow or detrimental to the care of the individual concerned. If in doubt seek advice.

10. You are responsible for your decision to pass on information. If you are unsure whether or not to disclose information, consult your line manager and/or if necessary obtain advice from the Head of Corporate Governance, the Caldicott Guardian, Information Governance Officer or information security team.

RELEVENT LEGISLATION

11. Individuals are required to ensure that confidential information is safeguarded and is kept securely in accordance with all relevant legislation. This includes:
    a. Data Protection Legislation. This includes the General Data Protection Regulation (EU) 2016/679 (GDPR),
    b. Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED)
    c. Human Rights Act 1998,
    d. Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
    e. Privacy and Electronic Communications (EC Directive) Regulations.
    f. The Caldicott Principles revised 2013

YOUR DUTY OF CARE

12. You are responsible for protecting the physical security of confidential information from accidental loss, damage, destruction, unauthorised access or accidental disclosure. For example:

Physical Security

    a. You must return to SHPCA upon request (and in any event upon the termination of your employment/engagement), all documents and tangible items which belong to the Organisation or which contain or refer to any confidential information and which are in your possession or under your control.

    b. You must not remove or copy any documents or tangible items including software which belong to SHPCA or which contain any confidential information from the Organisation's premises at any time without proper advanced authorisation

    c. Do not leave confidential information lying around unattended or place paper containing confidential information in the bin. It must be shredded or put in a 'confidential waste' container

    d. You must always wear your identification badge when on SHPCA or partner premises and ensure that any visitor's wear identification badges accordingly. Challenge unknown persons on Organisation premises

    e. Lock away any confidential information and lock offices when unoccupied

    f. Do not remove confidential data (held manually or electronically) from SHPCA sites without the express permission of your Manager/Head of Service/Director. If this is required as part of your job then you are responsible for following the guidelines for storing and transporting confidential information as set out in the Information Security Policy

    g. Be especially careful with the security of portable computers, i.e. hand held devices and laptops and follow the principles set out in the Information Security Policy

    h. Take care when giving personal information over the phone – have you identified the person? Do they have a right to know? Can anybody else hear the conversation?

    i. Be careful when putting a telephone call on hold – what information might they hear?

    j. Don't leave personal information on answer phones

    k. Envelopes containing confidential information must be securely sealed, labelled 'confidential' and clearly addressed to a known contact. Medical records or other sensitive

information should be sent externally by Special Delivery or by approved courier. Please refer to the Information Security Policy for more information

Computer & Electronic Security

l. Keep your PC screen out of sight of others if personal information is showing and log out or lock your computer keyboard if you move away from your desk

m. Never tell anyone your password or share passwords. Change your password regularly

n. Do not email or fax patient identifiable information unless approved safeguards are used or there are exceptional circumstances. Consult your line manager if personal or confidential information has to be sent in this way and refer to the Information Security Policy for instructions.

o. Ensure you store all information on a backed-up shared drive and not on the hard drive/desktop of your computer. Do not keep or process SHPCA confidential/identifiable data on your home PC

p. Under no circumstances should you put software on a SHPCA PC without permission of the head of the IT department

q. Under no circumstances should you connect non-SHPCA supplied equipment to the SHPCA network or computers – for example personal laptops, iPhones/mobile phones, iPods, iPads/tablet devices.

r. The only memory sticks which are permitted for use are those provided by the IT procurement department, which are fully encrypted and meet SHPCA security requirements.

s. Due to confidentiality interims are required to use a secure NHS email account. This does not infer any employment rights'

GENERAL

13. You are also required to:
    a. Report any security risks/incidents
    b. Always protect your data
    c. Ensure that you have accurate and correct information
    d. Don't keep information longer than necessary – refer to your line manager
    e. Do not discuss confidential information with friends or family outside of SHPCA or with colleagues in public places
    f. Read all related policies and guidance on confidentiality and information security
    g. Do not set up any databases or new information flows for personal data without discussing it with the Head of Corporate Governance
    h. If in any doubt – do not share information and seek advice before proceeding further.

DECLARATION

14. I confirm that I am fully aware that I have a legal duty of confidentiality to SHPCA. I further confirm that I will not disclose any unauthorised information belonging to patients, SHPCA's staff or SHPCA's affairs and those of other associated organisations to any other party.

15. I am aware that any breach of this undertaking is a serious matter that may lead to disciplinary action. SHPCA may also instigate legal proceedings against an individual who does not comply with its confidentiality requirements.

16. There may be occasions when staff have a duty to raise concerns over health service issues and the legal duty of confidence may be overridden, i.e. a statutory requirement or in the public interest. In all cases references must be made to your line manager or senior manager who will, if necessary take further advice, before any disclosure is made.

17. Further information can be found in the relevant policies which I will read as soon as possible after commencing my employment/engagement

ACCEPTANCE

18. Signed on behalf of Southern Hampshire Primary Care Alliance.

Signature	
Printed Name	
Date	

Signed by the employee

Signature	
Printed Name	
Date	