



Employee Confidentiality Agreement

1. Purpose of This Agreement

The purpose of this Agreement is to ensure the protection of **patient / service user information, clinical data**, and all other confidential materials handled by the Employee in the course of their duties.

2. Definition of Confidential Information

“Confidential Information” includes, but is not limited to:

- **Patient-identifiable information (PII)**, including medical records, treatment notes, test results, NHS numbers, and personal details
- **Sensitive health data** protected under GDPR and the Data Protection Act 2018
- **Clinical protocols, care plans, and treatment methodologies**
- **Internal policies, incident reports, safeguarding information, and risk assessments**
- **Staff information**, including HR files, rotas, and internal communications
- **Operational information**, including financial data, procurement details, and IT systems
- Any information governed by the **Caldicott Principles** or NHS confidentiality standards

3. Employee Obligations

The Employee agrees to:

- Maintain strict confidentiality of all patient / service user and organisational information
- Access patient / service user information **only when necessary** for legitimate clinical or administrative duties
- Comply with **GDPR, the Data Protection Act 2018, NHS Code of Confidentiality, and Caldicott Principles**
- Store and handle information securely (e.g., password protection, locked storage, secure systems)
- Refrain from discussing patient / service user information in public or non-secure environments

- Report any data breaches or confidentiality concerns immediately to the Employer's Data Protection Officer / Management or Caldicott Guardian
- Return or securely delete all confidential materials upon termination of employment

4. Prohibited Actions

The Employee must not:

- Share patient / service user information with unauthorised individuals, including colleagues without a legitimate need
- Remove patient / service user records or confidential documents from the workplace without permission
- Use personal devices, email accounts, or messaging apps to store or transmit confidential information
- Access patient / service user medical records or those of family, friends, or colleagues without formal authorisation
- Post or discuss any work-related information on social media

5. Legal and Regulatory Compliance

The Employee acknowledges that breaches may violate:

- **General Data Protection Regulation (GDPR)**
- **Data Protection Act 2018**
- **NHS Confidentiality Code of Practice**
- **Caldicott Principles**
- **Professional codes of conduct** (e.g., NMC, GMC, HCPC)

Breaches may result in disciplinary action, termination, regulatory referral, civil liability, or criminal prosecution.

6. Duration of Confidentiality

The Employee's duty of confidentiality:

- Begins on the Start Date
- Continues throughout employment
- **Survives indefinitely** after employment ends, including after retirement or career changes

7. Intellectual Property

Any clinical tools, documentation, training materials, or innovations created by the Employee in the course of employment remain the **exclusive property of the Employer**.

8. Acknowledgement

The Employee confirms they have received training on confidentiality, data protection, and information governance, and understands their responsibilities.

9. Governing Law

This Agreement is governed by the laws of **England and Wales**.

Romy Managing Director

OPT HEALTHCARE LIMITED