Connectbatch Limited Privacy Notice

(AI-enabled NHS Data Processing)

AI Transparency Statement:

Connectbatch Limited uses Artificial Intelligence (AI) solely to automate the extraction and digitisation of patient information from letters for integration into Electronic Patient Records (EPRs). AI is applied under strict governance and human oversight. Patient data processed by our solution is not used to train AI models, and we do not repurpose patient data for research or algorithm development. All outputs are verified by NHS professionals before integration.

Compliance References:

- UK GDPR & Data Protection Act 2018
- NHS Data Security and Protection Toolkit (DSPT)
- Common Law Duty of Confidentiality

Contact:

Data Protection Officer (DPO)
Email: dpo@connectbatch.co.uk

Introduction

This is Connectbatch Limited's Privacy Notice.
As part of the services we provide to NHS organisations and related stakeholders, we process personal data about our staff, service users (including NHS clients), and, in some cases, their representatives. "Processing" means collecting, recording, organising, storing, sharing, or destroying data.

We are committed to being transparent about why we need your personal data and what we do with it. This notice also explains your rights under UK GDPR and the Data Protection Act 2018.

Service Users

What Data Do We Have?

To deliver secure and compliant technology solutions for NHS workflows, we may process:

- Basic details: Name, address, contact information.
- Financial details: Payment or funding arrangements.
- Technical data: IP addresses, system usage logs, and authentication credentials.

We do not routinely process health or social care data unless explicitly required for NHS projects and under strict contractual and legal controls.

Why Do We Have This Data?

We process your data because:

- We have a legal obligation under NHS data governance frameworks and UK GDPR.
- It is necessary for the performance of a contract with NHS organisations.
- We have a legitimate interest in ensuring system security and service delivery.
- Where applicable, we process data with your consent (e.g., optional services).

Common Law Duty of Confidentiality

When handling NHS-related data, we comply with the common law duty of confidentiality by:

- Obtaining consent where required.
- Acting under legal obligations or public interest grounds (e.g., safeguarding, serious crime prevention).

Where Do We Process Your Data?

Data may be collected from:

- You or your authorised representative.
- NHS organisations and approved third-party providers.

Methods include secure portals, encrypted email, and approved NHS systems.

National Data Opt-Out

Connectbatch Limited does not use confidential patient information for research or planning purposes. If this changes, we will comply with the National Data Opt-Out policy.

Staff

We process staff data for employment purposes, including:

- Contact details, payroll information, training records.
- DBS checks where required for NHS project compliance.

Lawful bases: legal obligation, contract, and legitimate interest.

Friends/Relatives

We may hold emergency contact details for staff and next of kin information for service continuity.

How Do We Store Your Personal Information?

Data is stored securely using NHS-approved standards and encryption. Retention periods follow the NHS Records Management Code of Practice. After expiry, data is securely destroyed or anonymised.

NHS Data Security and Protection Toolkit Compliance

Connectbatch Limited is committed to meeting the requirements of the NHS Data Security and Protection Toolkit (DSPT). This means:

- Annual DSPT assessments to demonstrate compliance with NHS data security standards.
- Technical and organisational measures aligned with NHS guidance, including encryption, access controls, and secure data transfer protocols.
- Mandatory data protection and cyber security training for staff.
- Incident response procedures for reporting and managing data breaches in accordance with NHS and ICO requirements.

Data Breach Notification Procedure

Connectbatch Limited has a formal procedure for managing data breaches:

- **Immediate Assessment:** Any suspected breach is assessed within 24 hours to determine scope and impact.
- **Containment and Recovery:** Steps are taken to contain the breach and prevent further unauthorised access.
- **Notification:**
    - If the breach poses a risk to individuals' rights and freedoms, we will notify the Information Commissioner's Office (ICO) within 72 hours, as required by UK GDPR.
    - Where there is a high risk to individuals, we will also inform affected individuals promptly, providing details of the breach and advice on protective measures.
- **Documentation:** All breaches are recorded in our internal incident log, including actions taken and outcomes.
- **Reporting to NHS:** For NHS-related data, we will follow the NHS DSPT breach reporting requirements and notify relevant NHS bodies.

Your Rights

You have rights under UK GDPR, including:

- Access, correction, erasure, restriction, objection, and portability.
- Withdrawal of consent where applicable.

Contact dpo@connectbatch.co.uk to exercise your rights. Complaints can be made to the ICO at https://ico.org.uk.

Website

Our website may collect IP addresses and usage data for security and analytics. See our **Cookie Policy** for details.