imprivata

CASE STUDY

# Building a culture of trust and privacy at Liverpool Women's NHS Trust

NHS
Liverpool Women's
NHS Foundation Trust

## Challenge

- Encouraging adoption of consistent information security processes
- Protecting patient privacy and safeguarding personal information
- Training of staff to ensure data security in working practices

## Benefits

- Protecting patient information and privacy
- Faster, easier analysis of working processes and practices
- Immediate alerts of irregular activity/contraventions of records management

**LOCATION**
Liverpool, UK

**EMPLOYEES**
1,400

**INDUSTRY**
Healthcare

**COMMUNITY SERVED**
50,000 patients

Liverpool Women's NHS Trust specialises in the health of women and their babies – both within the hospital and out in the community. It is the only such specialist Trust in the UK and represents some of the most outstanding expertise and experience in this field.

Its main hospital is a modern landmark building located in Toxteth, Liverpool, where each year around 8,500 babies are delivered, and 10,000 gynaecological procedures performed. It is a pioneering centre for fertility help and gynaecology oncology. The genetics team at the Liverpool Centre for Genomic Medicine (LCGM) supports families with the diagnosis and counselling of genetic conditions.

The Trust also works closely with the University of Liverpool to deliver the highest standards of undergraduate and post-graduate medical education and training.

As a leading institution in hospital care, research, and delivering effective healthcare within the community, patient confidentiality and privacy are a top priority for the Trust. Safeguarding personal patient data is a priority for the Information Governance team.

## The solution

Liverpool Women's NHS Trust is an established long-time user of Imprivata Enterprise Access Management with single sign-on to manage secure access to patient data. The Trust implemented FairWarning, now Imprivata Patient Privacy Intelligence, a threat detection platform that provides alerts and reports on activity when records are accessed out of routine or required clinical practice, as part of a wider focus on safeguarding patient data across the organisation.

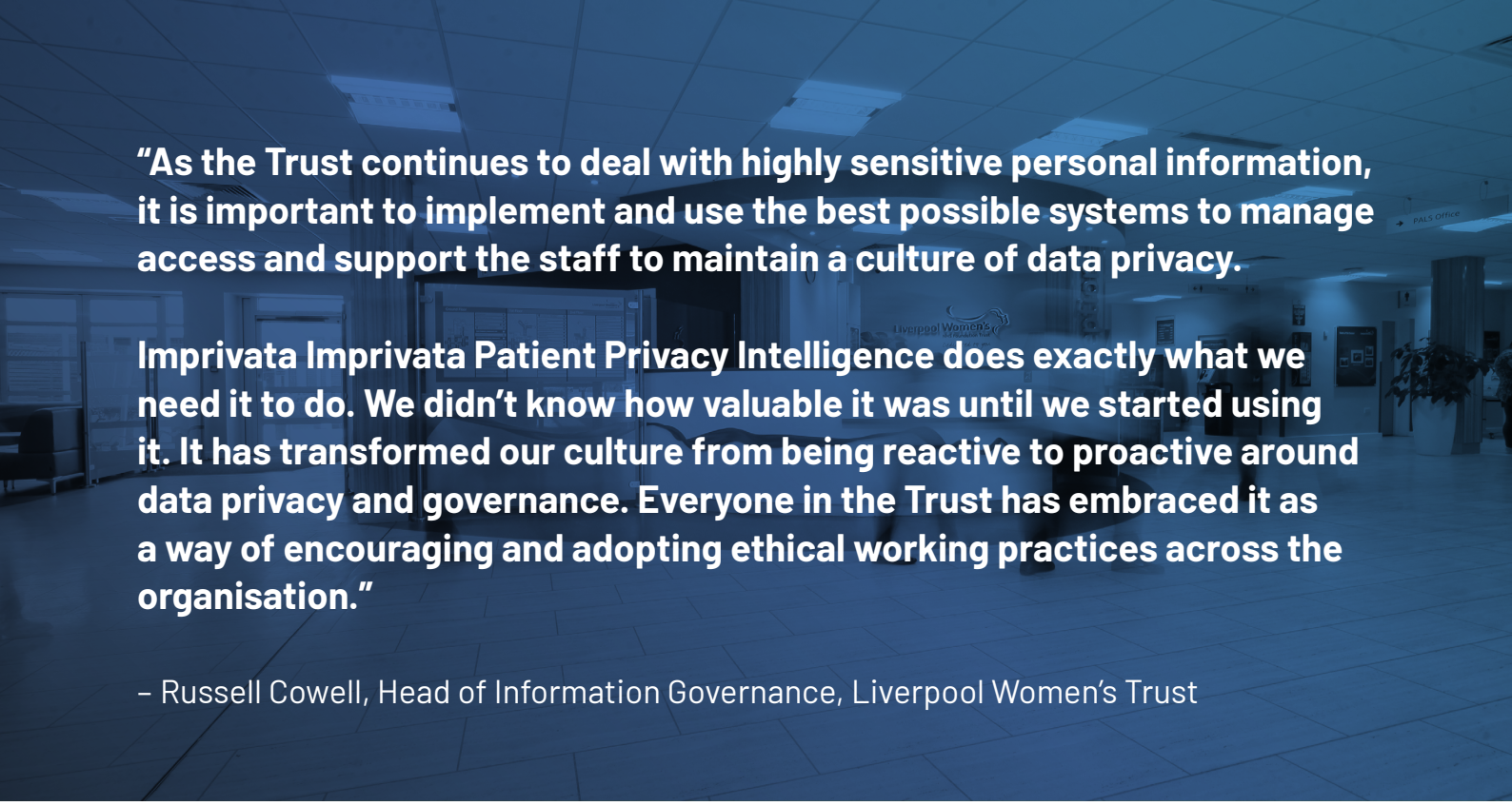
**"The Trust is becoming more dependent on digital working, aligned with the government's drive for digital transformation, and is relying more on accessing data than before. As such, we need assurance that the data is being managed safely and that we have the right systems in place to do so. Together Imprivata Enterprise Access Management with single sign-on and Imprivata Patient Privacy Intelligence give us effective access controls, robust identity governance, and critical data privacy compliance."**

– Matt Connor, CIO, Liverpool Women's Trust

The initiative was introduced to support common working methods amongst staff, with a consistent and transparent approach as to how patient data was managed and accessed. It also contributed to developing an organisation-wide culture of understanding the importance of both patient privacy and adoption of uniform ethical working practices.

The Information Governance (IG) team at the hospital configured the Imprivata Patient Privacy Intelligence software to work alongside its Meditech EMR, HR, and Laboratory investigations systems. Working with the Senior Leadership team and HR, the IG project staff designed reports from the software to monitor staff access for records, aligned to job requirements and working procedures.

The Imprivata Patient Privacy Intelligence report highlights when access is outside of a clinical or administration requirement and requires further investigation. Guidelines are provided for line managers and HR to assess and validate access when a potential data breach is flagged.



**"As the Trust continues to deal with highly sensitive personal information, it is important to implement and use the best possible systems to manage access and support the staff to maintain a culture of data privacy.**

**Imprivata Imprivata Patient Privacy Intelligence does exactly what we need it to do. We didn't know how valuable it was until we started using it. It has transformed our culture from being reactive to proactive around data privacy and governance. Everyone in the Trust has embraced it as a way of encouraging and adopting ethical working practices across the organisation."**

– Russell Cowell, Head of Information Governance, Liverpool Women's Trust

The reports may identify when a member of staff might be accessing their own record, or that of a colleague, family member, or associate. The HR team refers to family details, personal connections, and internal authorisations, as well as other background information, to validate the action and ensure that personal confidentiality has not been infringed.

The solution includes the following elements from Imprivata:

- Imprivata Enterprise Access Management with single sign-on and Authentication Management
- Imprivata Patient Privacy Intelligence analytics and insider threat detection platform

## Implementation

Since implementing the Imprivata Patient Privacy Intelligence system and reports, the Trust has introduced a 'zero tolerance policy' to data privacy breaches. Irregular activity is flagged to the Head of Information and subsequently to the CIO, Matt Connor, as well as to the HR team, when deemed appropriate. As a result, the hospital has seen a positive change in how data privacy and governance is considered and respected throughout the organisation.

This is now evident in its culture of trust and adoption of ethical working practices across clinical and administration teams. The credibility of the Imprivata Patient Privacy Intelligence system and reports have also helped with external requests and investigations on confidentiality breaches. Clear audits and records of irregular data access help to protect staff from being wrongfully accused of malpractice.

## The future

As the Trust evaluates and adopts new systems to support its work, data security continues to be high on the agenda. While all the clinical and administration applications and systems used by the Trust provide audit data, often they provide the bare minimum of information, with the forensic investigation required after a security breach time-consuming to carry out.

For the Information Governance team, the reports from the Imprivata Patient Privacy Intelligence solution enable more complex analysis of security breaches, facilitating a much higher standard of internal audit to continue to support data privacy. It enables a preemptive approach to security, rather than reactive.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organisations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:


**Global headquarters USA**
Waltham, MA
**Phone:** +1 877 663 7446
www.imprivata.com

**European headquarters**
Uxbridge, England
**Phone:** +44 (0) 208 744 6500
www.imprivata.com/uk

**Germany**
Langenfeld
**Phone:** +49 (0) 2173 99 385 0
www.imprivata.com/de

**Australia**
Melbourne
**Phone:** +61 3 8844 5533





3764-2026_PPI-CS-liverpool-womens