# Client Alert: Lessons for healthcare providers after ICO enforcement action against HCA

**Date :** February 28, 2017

The Information Commissioner's Office (ICO) has fined a private health company, HCA International Ltd, for failing to keep fertility patients' personal information secure. This is just the latest in a long line of cases highlighting the regulator's campaign to make healthcare providers take their data protection responsibilities seriously.

**What was the penalty?**

A £200,000 monetary penalty has been issued as a result of an ICO investigation into the way the Lister Hospital was transferring, transcribing and storing records of IVF appointments. HCA owned the Lister Hospital and received the monetary penalty as a result.

**Who are HCA?**

HCA are a US-based corporation listed on the New York Stock Exchange and providing healthcare services in the US and UK. They currently employ more than 200,000 people across more than 160 hospitals.

**What went wrong?**

The Lister Hospital offered a range of services including private (non-NHS) fertility treatment. The issue was uncovered in April 2015 when a patient found that transcripts including details from interviews with Lister Hospital IVF patients could be freely accessed by searching online. The records were available online for 3 weeks.

The investigation revealed that the hospital had been routinely sending unencrypted audio records of the interviews by email to a company in India since 2009. Details of private conversations between a doctor and various hospital patients wishing to undertake fertility treatment were transcribed in India and then sent back to the hospital.

The ICO found the Indian company could not restrict access to the personal information because it stored audio files and transcripts using an unsecure server.

HCA also breached the Data Protection Act 1998 by failing to ensure that their sub-contractor acted responsibly. The ICO found this to be a breach of Principle 8 of the Data Protection Act 1998 (and likely also a breach of Principle 7). The ICO was especially critical of the fact that proper agreements were not in place to secure personal data. The case also emphasizes the need to have proper data transfer or data processing agreements in place (or Binding Corporate Rules) when transferring data outside the European Economic Area (EEA).

**Is healthcare data treated differently?**

Yes and no. Health data is sensitive personal data and that means that it needs special treatment in data protection law. In addition the ICO has special powers under Section 41A of the Data Protection Act 1998 to enforce data protection compliance within state owned health care. There are more details on this here - http://www.corderycompliance.com/ico-now-able-to-apply-compulsory-audit-powers-in-the-healthcare-sector/.

**What did HCA do right?**

The ICO did give HCA credit for taking steps to deal with the breach. It got credit for:

1. Voluntarily reporting the breach to the ICO
2. Fully cooperating with the ICO
3. Taking 'substantial' remedial action (the Monetary Penalty Notice gives no further details)

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2021 Cordery. All rights reserved.

In addition the ICO took into account the damage to HCA's reputation which it assessed as *'a significant impact'*.

**What about the future and GDPR?**

We've written extensively on new legislation, the General Data Protection Regulation (GDPR), which comes into force across the EU in May 2018. GDPR will strengthen regulators powers and increase the potential level of fine to 4% of global annual turnover or €20m whichever is the higher. There are extensive resources to understand more about GDPR, including detailed guidance on the fining mechanism and likely factors influencing the level of fine in Cordery GDPR Navigator here www.bit.ly/gdprnav.

As an illustration in this case HCA's worldwide annual turnover in 2016 was $39.678 billion making the potential fine under GDPR $1.59 billion (around £1.3 billion at today's exchange rate). In this case HCA were fined 2/5ths of the maximum fine which would translate to a fine of more than $0.6 billion under GDPR.

For healthcare providers however this is not their only worry. Also next year the EU Network Information Security Directive (2016/1148 - "the NIS Directive") will come into full force as EU Member States must apply this fully in national law from 10 May 2018. The NIS Directive has detailed security incident requirements including an obligation to report security incidents without undue delay and many healthcare providers (including some in the private sector) will be subject to its provisions too. You can find out more about the NIS Directive here - http://www.corderycompliance.com/uk-to-implement-eu-cybersecurity-directive/.

Many healthcare providers are working on their data plans as a result. There are more details of some of the projects we have worked on in this area here - http://www.corderycompliance.com/healthcare/.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com

Cordery is a trading name of Cordery Compliance Limited. Authorised and regulated by the Solicitors Regulation Authority. SRA number 608187. Company number 07931532 registered in England and Wales. VAT number: 730859520 Registered office: Lexis House, 30 Farringdon Street, London, EC4A 4HH, United Kingdom Copyright © 2021 Cordery. All rights reserved.