ICO Ref: **COM0573510**

# DATA PROTECTION ACT 1998

# UNDERTAKING

Data Controller: Sirona Care & Health

St Martins Hospital
Clara Cross Lane
Bath
BA2 5RP

I, Janet Rowse, Chief Executive, of Sirona Care & Health, for and on behalf of Sirona Care & Health hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Sirona Care & Health is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by Sirona Care & Health and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed in March 2015 that an email containing sensitive personal data had been sent to a previous service user in error. The email contained sensitive details about three service users including names, dates of birth, NHS numbers, addresses and medical details. The employee had intended to send the email to her colleagues however the personal email address of a former service user was selected in error.

3. The data controller only became aware of this incident when it was contacted by the unintended recipient who then deleted the email. The incorrect email address had been selected after the employee looked up a colleague's email address using their first name and incorrectly selected a former service user, who shared the same first name. The email address of the former service user had previously been saved and not deleted. The data controller did have some data protection policies and procedures in place, however our investigation revealed that these were not fully effective because they did not provide any detailed guidance in relation to checking

email addresses or any requirement for staff to delete email addresses which were no longer in use.

4. Whilst the data controller does provide induction and annual mandatory information governance training, our investigation determined that the employee who sent the email had not received information governance training for over two years prior to the incident. In addition to this, it was established that only 66% of the data controller's staff were up to date with their information governance training. In response to a previous incident reported by the data controller, the Commissioner had expressed concerns that the organisation was unable to demonstrate that all new and existing employees had completed information governance training on an annual basis. In addition to this it was noted that staff may not have been sufficiently aware of the data controller's data protection policies and procedures. Consequently the Commissioner determined that the data controller may not have taken sufficient steps to act on his previous advice.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. The Principle is set out in Schedule 1 Part I to the Act.

6. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

**The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:**

1) **The data controller ensures that mandatory annual data protection refresher training is in place for all staff who routinely process personal data.**

2) **The data controller shall ensure that the completion rate of data protection training sessions is monitored. Appropriate follow up procedures should also be in place in the event of staff non-compliance.**

3) **The data controller shall review its policies to ensure that appropriate advice is provided to staff on email checking**

**procedures and that these are readily accessible to its employees;**

4) **The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Signed: ……..

Janet Rowse
Chief Executive
Sirona Care & Health

Dated: ……..

Signed: ……..

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: ……..