Ultramed® Ltd

Data Protection Impact Assessment

Migration to Microsoft Office 365 for all email communications from Ultramed.co, enforcing encryption when sending emails to NHS email accounts.

Table of Contents

Table of Figures

No table of figures entries found.

Purpose & Scope

This is a Data Protection Impact Assessment for securing email sent to NHS email services from Ultramed.co to meet DCB1596 standards.

Step One - Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. If necessary, refer or link to other documents such as the project proposal. Summarise why a DPIA is required.

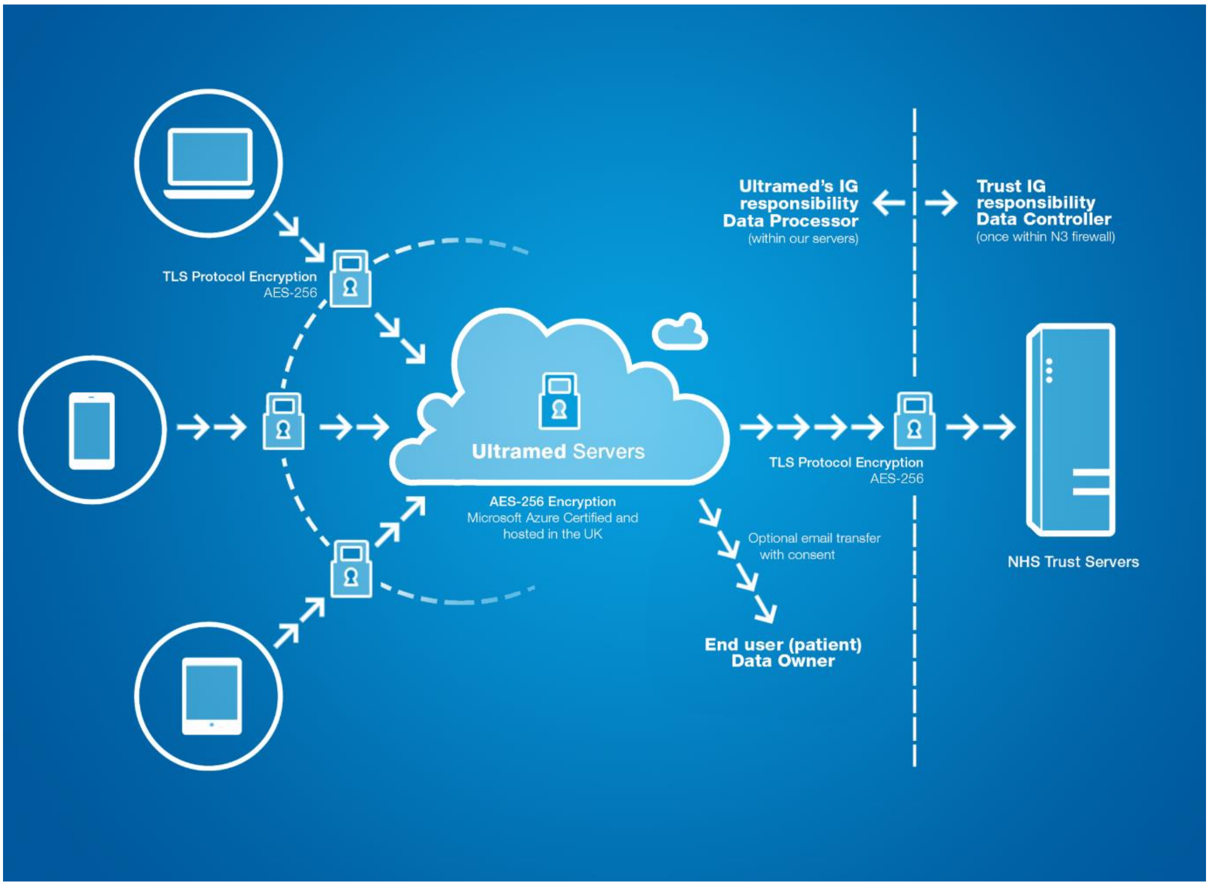
To secure the connection and transfer of emails in Microsoft Office 365 from Ultramed.co to meet the secure email standard (DCB1596) when sending the output clinical summary reports. The current email transfer from Ultramed.co is carried out by SendGrid, this service is not a recognised system for sending secure person identifiable data (PID), to mitigate this non-compliance risk we will be sending mail securely through Office 365, enforcing TLS encryption when sending to an NHS email account.

Step Two – Describe the processing

Describe the nature of the processing: how will the data be collected, used, stored and deleted? What is the source of the data? Will the data be shared with anyone? A flow diagram or other way of describing the data flows might be helpful. What types of processing identified as likely high risk are involved?

The data is collected from the End User (patient) in their own Ultramed account. The data is processed into a readable PDF which is sent to the Customer (health care provider), the report data is then used by the Customer to facilitate the care of the End User, the End User owns their own account and therefore their data. Once the report is sent to the Customer, the Customer becomes the data controller of that information, not the data in the End User's account. The data in the End User's account is stored on localised Microsoft Azure Servers, located in the UK. Once the report has arrived with the Customer the data is stored on the Customer's internal server.

The processing by Ultramed is conducted through sending a secure email to the Customer which contains the report, once the End User has agreed to send their information to the Customer. If the email is not sent in line with the DCB1596 standard there is risk of PID breach.



Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will be collected and used? How often? How long will it be kept? How many individuals are affected? What geographical area does it cover?

The data is person identifiable information (PID) and contains the special category of health information. The End User enters a full (or as full as possible) depiction of their health history to assist the Customer in making decisions about the treatment they may need. The data in the End User account is 'live' for 60days before the content will need reconfirming before a re-submission of the data can be made. The End User can log back into their account at any time to update the information held. The record will be kept for 10years after the last account activity, after which point the account will be permanently deleted.

All accounts currently held, and any new accounts made will be affected by the change. The change will affect UK patients (End Users) and Customers, specifically the transfer securely to NHS email.

Describe the context of the processing: what is the nature of the relationship with the individuals? How much control will they have? Would they expect to have their data used in this way? Are children or vulnerable groups involved? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that should be factored in? Are you signed up to any approved code of conduct or certification scheme?

The End User creates their account, using their NHS number/patient identifier number, DOB and creating a secure password. The End User has full control of the information held in their account as it is inputted by them. The End User will expect this information to be used to facilitate their care, and agree to send information onto the Customer, in this case their healthcare provider. The groups affected could include vulnerable adults and children, if the Customer gives these groups access to create an account.

We will be submitting to NHS Digital with a conformance statement using Microsoft Office 365. This is an accredited service.

Ultramed chooses to not need any integration of IT within the NHS firewall, this keeps costs down for the health care provider, as no internal storage is needed, and also means the data held in End User accounts remains in the End User's control. This approach is novel as it is truly a patient owned health record.

Ultramed are Crown Commercial Service providers and are complaint with the IG Toolkit to level 2. Ultramed are currently working towards submitting to the DSP Toolkit by the March 31st 2019 Deadline.

Describe the purposes of the processing: What is the aim? What is the intended impact on individuals? What are the benefits of the processing for you and more broadly?

The aim is to be compliant with the secure email standard (DCB1596). No impact is expected to affect the End Users or the Customer. The benefit is conforming with the standards for better IG security overall for Ultramed, Customers and End Users.

Step Three – Consultation Process

Consider how to consult with relevant stakeholders: describe when and how individuals' views will be sought – or justify why it's not appropriate to do so. Who else from the organisation needs to be involved? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Each current Customer will be notified of the changes, there will be no migration period as the steps to secure the email will not affect service. The Customers will be provided with a breakdown of actions taken and an updated IG/IT document for records.

Step Four – Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is the lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Compliant with DCB1596 standards. The lawful basis for processing is consent, End User gives consent for Ultramed to process data and deliver it securely to the Customer. Data is owned by the patient and therefore expected to be kept up to date in their account. End users have the option to receive the same report as the trust but Ultramed make it clear that the connection is not as secure going across to a personal email and they have to opt-in.

Using Microsoft Office 365 mitigates risk as the service provider keeps all functionality up-to-date and has an auto reporting functionality built in, in case of breach. O365 conforms with the standard: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/a/h/microsoft_office_365_08122016.pdf

Step Five – Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Email being sent and them being compromised/breached	Remote	Severe	Medium

Step Six – Identify measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
O365 is approved by NHS DCB1596 standard as a secure method for email transfer. Migrating all emails will bring us in line with the standards and reduce the risk of emails being compromised/breached.	O365 already conforms with DCB1596, migrating reduces risk significantly.	Reduced	Low	Yes

Step Seven – Sign off and record outcomes

Item	Name/date	Notes

Measures approved by:	NHS Digital 08/12/2016	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Paul Upton 13/02/2019	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Migrate all emails over to approved O365 standards	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: To ensure email service is in line with DCB1596 standards using Office 365 mail ensuring TLS encryption.		
DPO advice accepted or overruled by:	Accepted by company Directors 13/02/2019	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	Jonty Brook 13/02/2019	If your decision departs from individuals' views, you must explain your reasons
Comments: This is an approved and secure way to transfer email from Ultramed.co to NHS email. It mitigates the remote risk of non-TLS encrypted emails reaching an NHS email inbox, meaning the email will always come securely from Ultramed.co		
This DPIA will be kept under review by:	Elise Worrall	The DPO should also review ongoing compliance with DPIA