The new NHS Data Security and Protection Toolkit

Are you ready for 30 June?

Keepabl™
PRIVACY
SECURITY
COMPLIANCE

What is the DSP Toolkit?

All organisations with access to NHS patient data and systems must use the DSP Toolkit to demonstrate, by self-assessing against the Toolkit's assertions:

- ***that they are practising good data security and***
- ***that personal information is handled correctly***

Covered organisations need to self-assess against the assertions and evidence set out in the Toolkit.

Deadline: 30 June 2021

"The Data Security and Protection (DSP) Toolkit is an online tool that enables relevant organisations to measure their performance against the data security and information governance requirements mandated by the Department of Health and Social Care (DHSC)"

https://digital.nhs.uk/

What's new – at a glance

The DSP Toolkit's been refreshed for 2021, with escalating changes through the levels

Level 4
GPs

- **Evidence items updated** to aid understanding & support completion

Level 3
Primary Care etc

- **Evidence items updated** to aid understanding & support completion
- **Evidence items rationalised** where there's overlap
- **Extra evidence items:** mobile devices & paper records

Level 2
CCG, CSUs & ALBs

- **Evidence items rationalised** where considered 'business as usual' or there's overlap
- **Extra evidence items:** backups & technical requirements
- **CE+ on-site assessment:** non-mandatory requirement

Level 1
NHS Trusts

- **Evidence items rationalised** where considered 'business as usual' or there's overlap
- **Extra evidence items:** backups & technical requirements
- **Mandatory technical evidence items**, particularly on Cyber Essentials
- **CE+ on-site assessment:** non-mandatory requirement

https://digital.nhs.uk/

Toolkit & Data Protection

The Key Data Protection Assertions

Data protection by design & default

Senior ownership of data protection

Lawful use & sharing of personal data

Individuals' rights respected & supported

Clear data protection policies in place, understood & available

Effective data quality controls in place & records maintained

Documented Records of Processing Activities (GDPR & UK DPA 18)

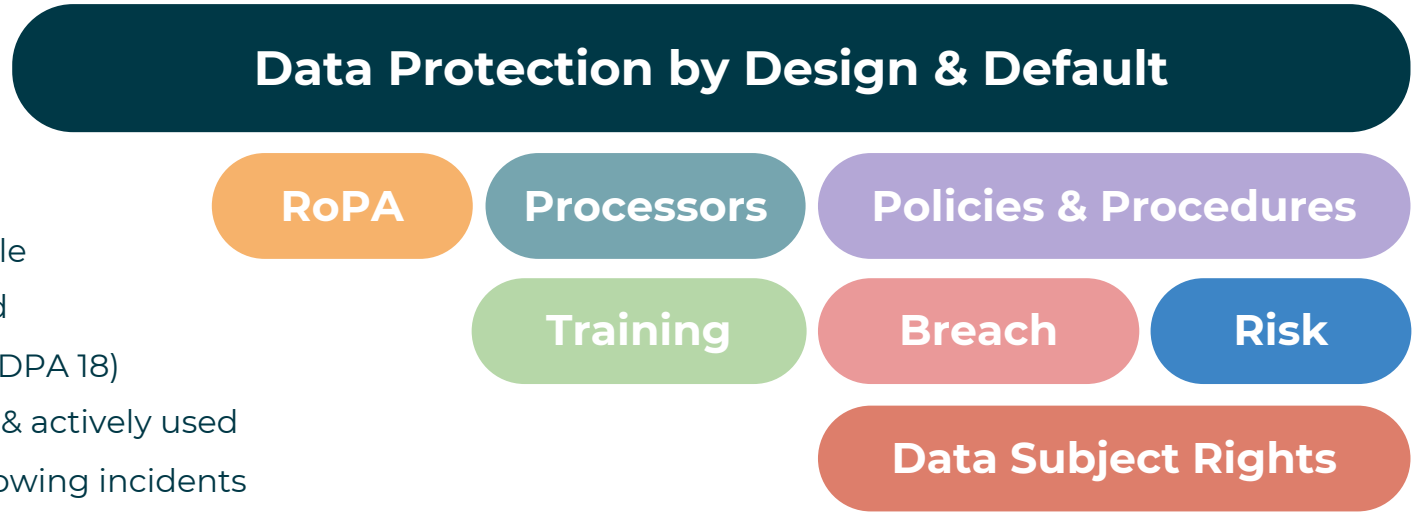
Confidential Breach System for reporting breaches, in place & actively used

Process Reviews at least annually, where data is at risk & following incidents

Basic supplier due diligence on processors in accordance with ICO & NHS Digital guidance

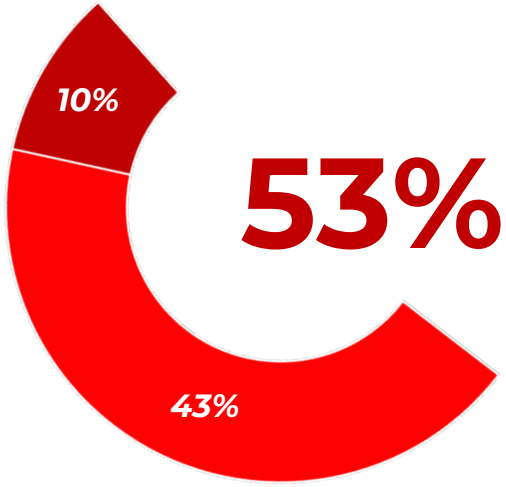
Clear risk understanding & management of identified, significant risks to information & services

Training needs assessed, staff pass tests, specialists trained appropriate to role, including leaders & board members



How ready is the NHS?

In December 2020, the UK ICO published its report on 12 consensual GDPR audits of NHS organisations, carried out from May 2018 to May 2019. The UK ICO reported a number of significant concerns and made 312 recommendations.



53% were classified as**:**

Urgent (10%) – *'clear and immediate risks to the data controllers' compliance with data protection legislation'*

High Risk (43%) – *'tackle at the earliest opportunity to mitigate a breach of data protection legislation'*

UK ICO's 'Headline Areas of Concern' coincide with Toolkit requirements:

Data Map: Most NHS Trusts did not have a RoPA in place, and some hadn't started

DSRs: Most Trusts had not made specific provisions for how to handle verbal requests

Training: Not always mandatory or completed, despite DSP Toolkit requirement

DPOs: Better collaboration needed, sharing of knowledge and promotion of best practice

Privacy Notices: Generally only in one form, no layered approach, accessibility a concern

Processors: Serious concern about lack of processor compliance checks

How Keepabl Can Help

Keepabl's SaaS solution and Privacy Policy Pack is a **complete Privacy Framework for GDPR**, with everything you need for **Data Protection by Design and by Default**.

It gives you a great answer for the DSP Toolkit, addressing all the areas called out by the UK ICO's report onto the NHS. Don't just take our word for it, take a look at our success story from Health-tech company, Syndi.

We know that GDPR can be stressful and time-consuming, so why not see how our award-winning, easy-to-use Privacy Management SaaS can help you get up to scratch with your DSP Toolkit obligations, your BAU compliance requirements and save you a lot of headaches in the long term?

Book your Keepabl demo

REGTECH100 2021
www.RegTech100.com

THE FINTECH POWER 50

CYBER ESSENTIALS CERTIFIED PLUS

"Keepabl's data activity management platform provided us with a go-to place to manage what personal data was flowing through the company, and ensure that it was being managed correctly"

Jorge Alexander
Co-Founder and CTO
Syndi Health

Keepabl™

PRIVACY
SECURITY
COMPLIANCE

Visit our website **Keepabl.com**
Contact us at **hello@keepabl.com**