Data Security Protection Toolkit – Top Tips?

Information and technology
for better health and care

Presented by: John Hodson
NHS Digital

Data Security and Protection Toolkit in numbers

33 development sprints completed

9,000+
Registered organisations

Active Users

Integrated GDPR + NIS Incident notification for streamlined automated reporting

Care Homes **300+%**
Uptake so far*

Feedback items

Takes in account other recognised Certifications and systems

380 **GDPR Incidents Reported to ICO**

8 **Bugs**
Reported and fixed[2]

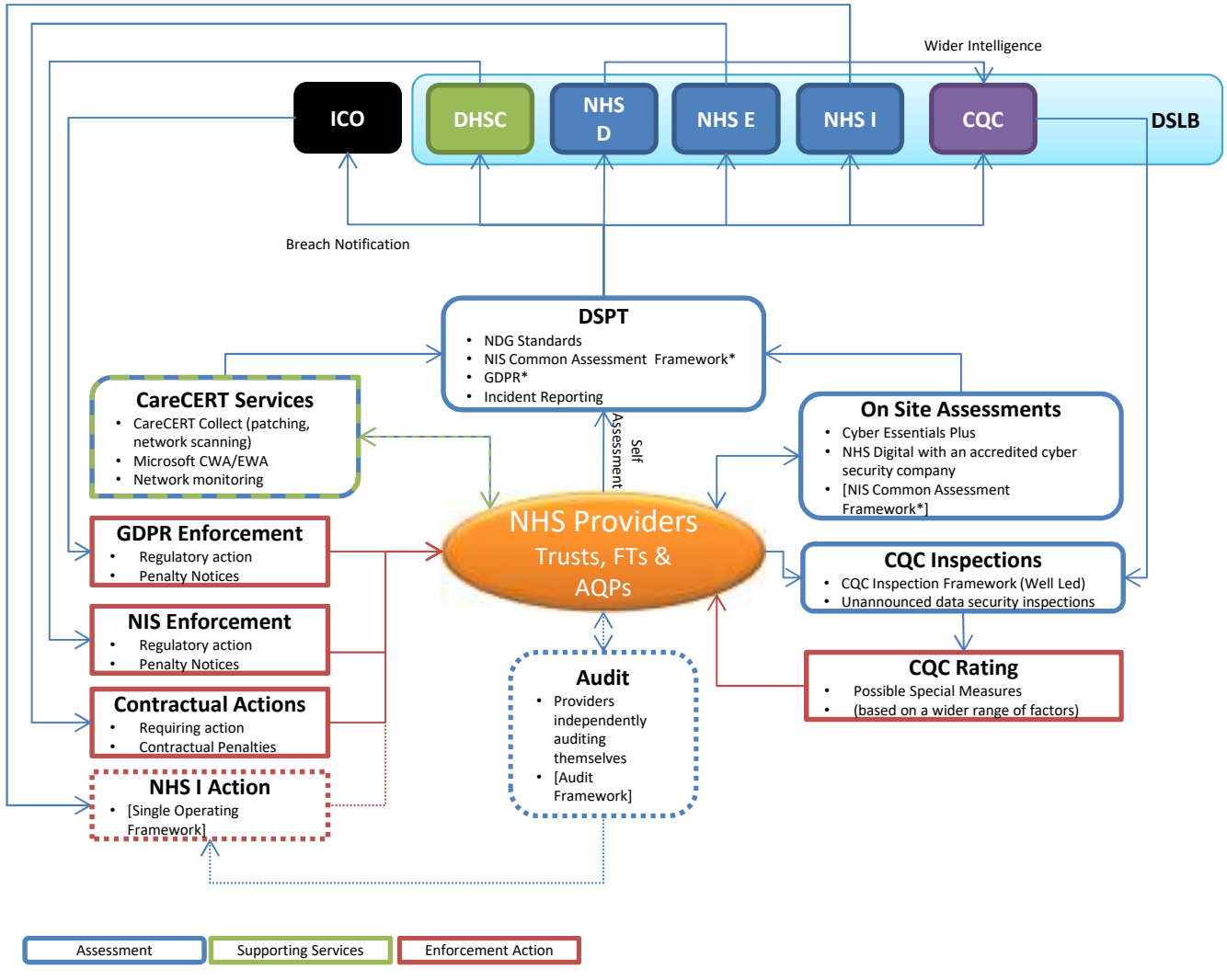
What is coming Functionality

- Accessibility and User Interface Improvements
- Provide evidence for multiple organisations but not submitting (any volunteers to test?)
- Public View
- Enhanced reporting
- Generate an action plan

* Not exhaustive

Overview of levels in the DSP Toolkit

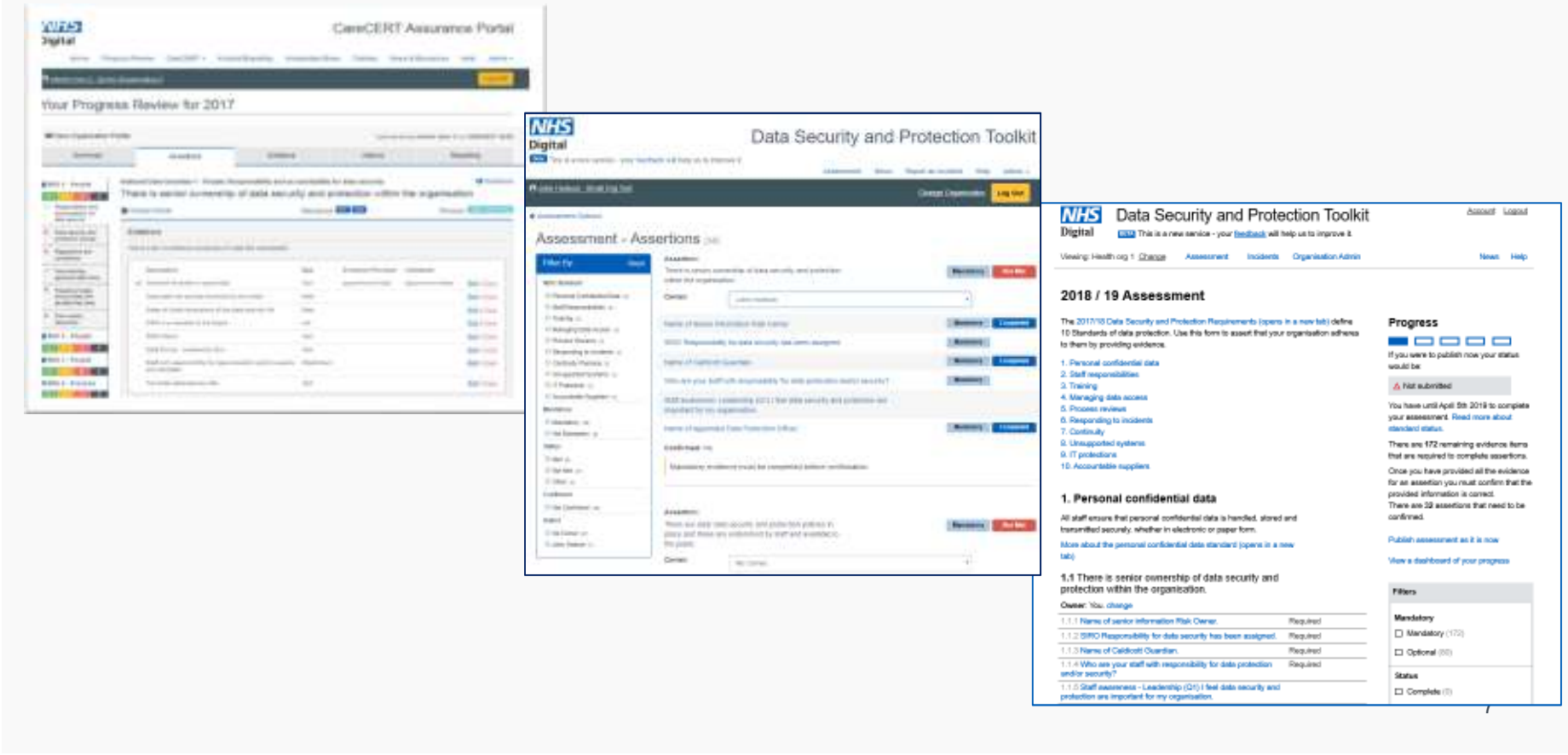
Name	Description
Entry Level	Time-limited level (subject to review) for smaller organisations. Evidence items for critical legal requirements are being met; but some expected mandatory requirements have not been met. (https://www.dsptoolkit.nhs.uk/Help/32) Allows access to NHSmail.
Standards Met	Evidence items for all mandatory expected requirements have been met. Access to NHSmail, other secure national digital solutions, e.g. Summary Care Records, and potentially local digital information sharing solutions.
Standards Exceeded	Evidence items for all mandatory expected requirements have been met. The organisation has external cyber security accreditation. Evidence of best practice.
Critical Standards Not Met	Evidence items for critical legal requirements have not been met by the organisation. No access to information sharing tools e.g. NHSmail.


Wider Intelligence
ICO
DHSC
NHS D
NHS E
NHS I
CQC
DSLB
Breach Notification
DSPT
NDG Standards
NIS Common Assessment Framework*
GDPR*
Incident Reporting
CareCERT Services
CareCERT Collect (patching, network scanning)
Microsoft CWA/EWA
Network monitoring
Self Assessment
On Site Assessments
Cyber Essentials Plus
NHS Digital with an accredited cyber security company
[NIS Common Assessment Framework*]
GDPR Enforcement
Regulatory action
Penalty Notices
NHS Providers
Trusts, FTs & AQPs
CQC Inspections
CQC Inspection Framework (Well Led)
Unannounced data security inspections
NIS Enforcement
Regulatory action
Penalty Notices
Audit
Providers independently auditing themselves
[Audit Framework]
CQC Rating
Possible Special Measures
(based on a wider range of factors)
Contractual Actions
Requiring action
Contractual Penalties
NHS I Action
[Single Operating Framework]
Key
Assessment
Supporting Services
Enforcement Action

What is coming….continued

- October deadline for trust(s) to publish baseline
- Develop CQC Inspections and Audit
- Webinars https://www.dsptoolkit.nhs.uk/News/10
- Drive on take up especially in social care
- Prepare for next year

Iterative development



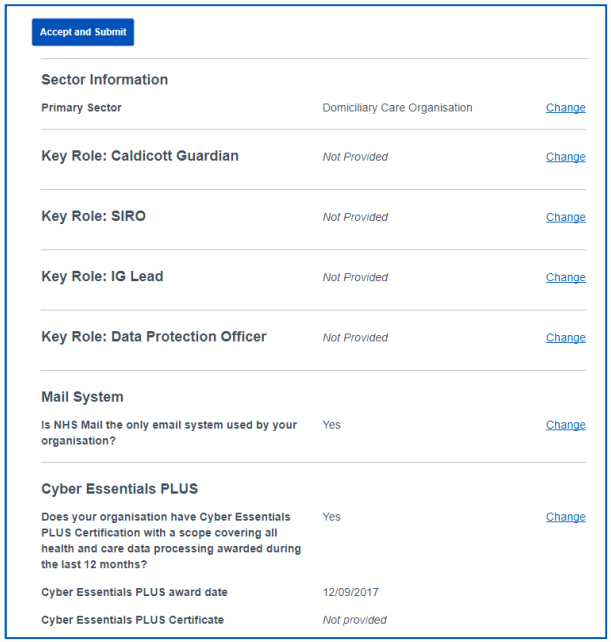
Baseline

- Large NHS organisations (Acute, Ambulance Trust, Mental Health Trust, Community Trust) must publish a baseline by the end of October https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0086-data-security-and-protection-toolkit-version-1-0

- You won't be able to publish a baseline if:
  - You are not one of the above organisation types
  - You have not completed your profile
  - You have already published a full (standards met) assessment
- You can publish more than one baseline (but you don't have to)*
- Deadline 31st October midnight

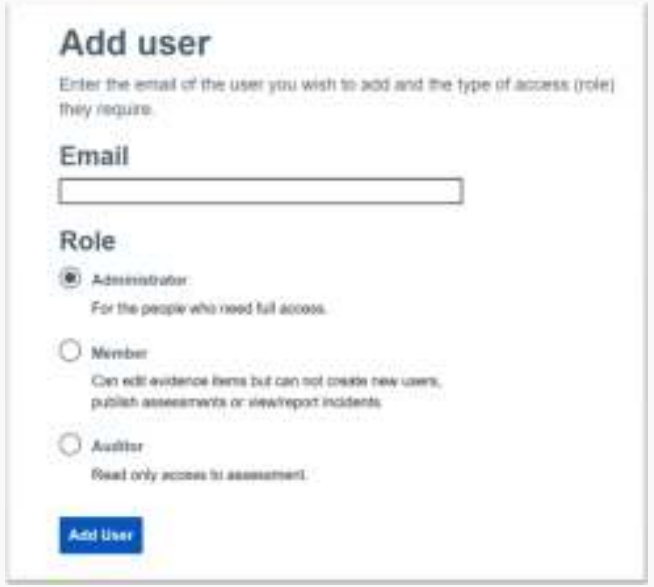
Top Tips /1

- You can go back in and change any of the Org Profile Questions right up to publication.
- PSN and Cyber Essentials Certificate dates may need to be updated before publication
- Need to accept and submit any changes
- Work on Mandatory First
- Survey Questions are not Mandatory



Top Tips /2

- Administrators can create new users and set permissions
- Only Administrators can publish an assessment (or report incidents)
- Member users can add evidence (and confirm assertions where an administrator has made them an owner)
- Audit users are read only
- You can set up external users here
- If you manage more than one org you must select it to set up users.



Top Tips /3

- You can add links to evidence rather than upload it
- For LAs the scope is Adult Social Services and Public Health
- CQC Inspections so far have focussed on governance of information risk
- To meet the standard you must confirm all the mandatory assertions before you publish

Top Tips /4

- If inviting sites onto the DSPT send them
- https://www.dsptoolkit.nhs.uk/Account/Register
- Guidance for Coding, Service User Data, Smartcards
- Sites which have registered and/or published are available https://www.dsptoolkit.nhs.uk/News/34)
- Document explaining DSPT levels https://www.dsptoolkit.nhs.uk/News/33
-

E-Learning Top tips

- **Self-registration on e-learning for healthcare (e-LfH)** https://nhsdigital.e-lfh.org.uk/
- **Organisation registration** https://healtheducationyh.onlinesurveys.ac.uk/nhs-digital-data-security-awareness
- **Access through Athens** (http://portal.e-lfh.org.uk)
- **More details** (https://www.dsptoolkit.nhs.uk/Help/30)

Help and Support

- Register
- https://www.dsptoolkit.nhs.uk/Account/Register

- Presentation developed to be used by IG Leads.
- https://www.dsptoolkit.nhs.uk/News/25

- FAQs including Training Tool.
- https://www.dsptoolkit.nhs.uk/News/9

- DSP Toolkit Support available through.
- Exeter.helpdesk@nhs.net

- Toolkit training and update events including presentations
- https://www.dsptoolkit.nhs.uk/News/10

Incident Reporting

- Tool Launched
- https://www.dsptoolkit.nhs.uk/Incidents
- Guidance Published https://www.dsptoolkit.nhs.uk/Help/29
- Worked with ICO DHSC, NHS England and NHS
- Guidance updated including guidance on Annual reports.
- May need to update local policy to reflect changes

What is Changing

- The scoring system of SIRI has been changed
- Level 2 is no longer the trigger for reporting
- Number of people effected not a Sensitivity factors anymore
- Trigger for reporting is harm and impact
- Notification System not an Incident Management System

What is reportable ?

- ICO -The incident is assessed that it is (at least) likely that there is a risk to individual rights and freedoms (harm) and that the impact is (at least) minor
- DHSC - -The incident is assessed that it is (at least) likely that there is a risk to individual rights and freedoms (harm) and that the impact is (at least) serious.
- Where the 72 hours (real hours) deadline is not met an organisation must provide an explanation

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

DHSC & ICO

ICO

Factors to consider

- Type of breach
- Nature, sensitivity and volume of personal data
- How easy it would be identify the individuals
- Potential consequences

- Look at the examples at the back of the guidance

What to report - Not ideal

- A patient letter was sent to the wrong address.

What to report - A bit better

- A letter was sent to a single patient of the physiotherapy service on 10th August. It has come to light that this was sent to the wrong address. The letter was opened, and all of the information included in the letter was read by another person who had no reason to view this data.
- The letter has been sent back to the Trust and returned to the department.

What to report - A bit better

- A physiotherapy appointment letter was sent from the Hospital dated 10th of August. This letter contained demographic details of the patient, a summary of the medical condition of the patient, a brief patient history and a list of other appointment's that the patient has in the next few months as a reminder. This will contain sensitive personal information.
- The person who opened the letter has the same surname as the patient and may be a family member.
- An initial investigation has identified that this was an individually typed letter so the issue is unlikely to be replicated widely across the service. It was individual letter as the appointment was being rearranged. As the patient didn't receive information about the appointment they missed their appointment, so it will have to be rearranged delaying the start of their treatment.
- The DPO , Caldicott Guardian have been informed and the incident has been recorded on the internal incident reporting system.
- We are speaking to the Physio service manager and the patient to provide the earliest possible appointment to minimise the impact.
- We have spoken to the patient to explain what has happened and apologies. A written apology is also being drafted to be signed by the Head of Service.
- Key Contacts for the incident is john.smaith@nhs.com 01111 111111.

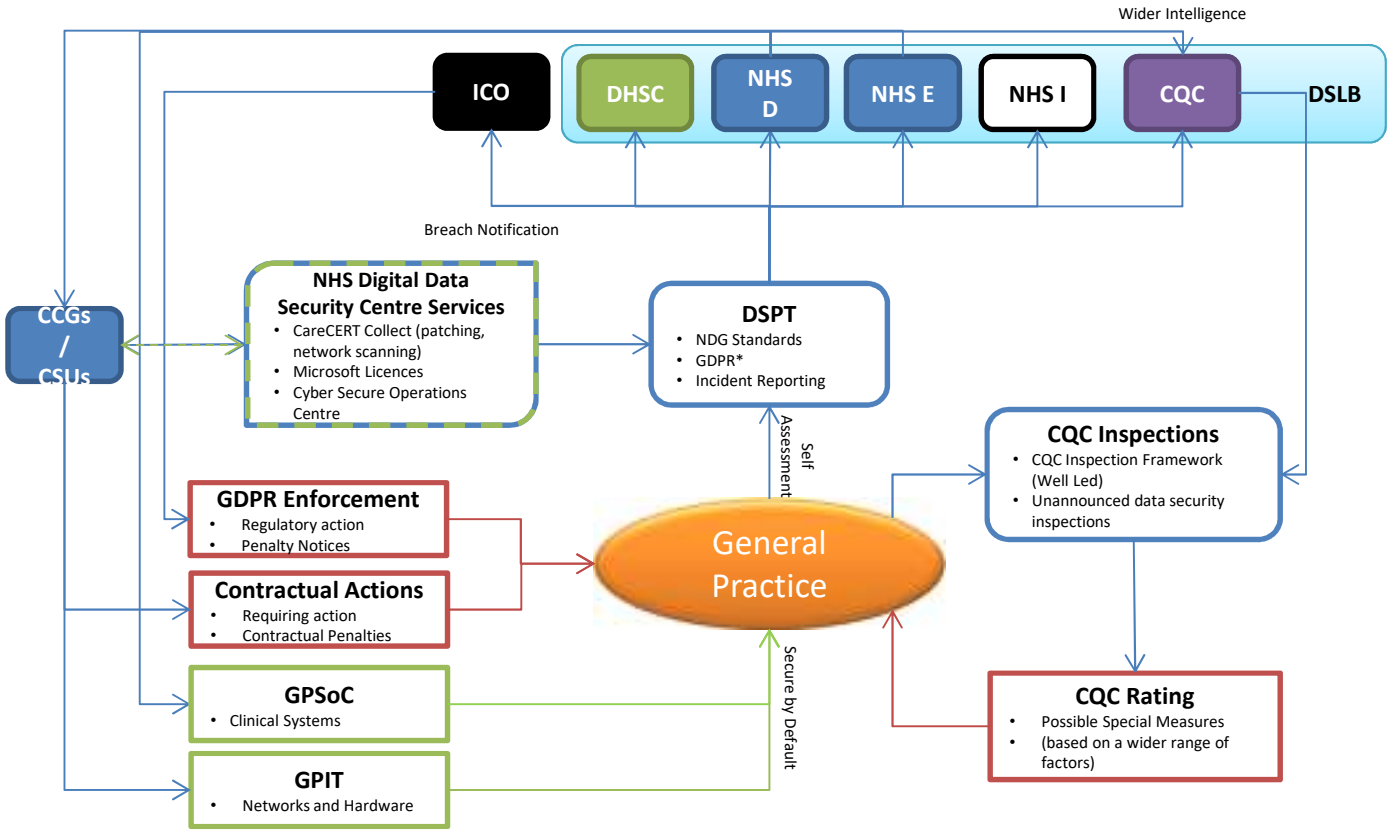
www.digital.nhs.uk

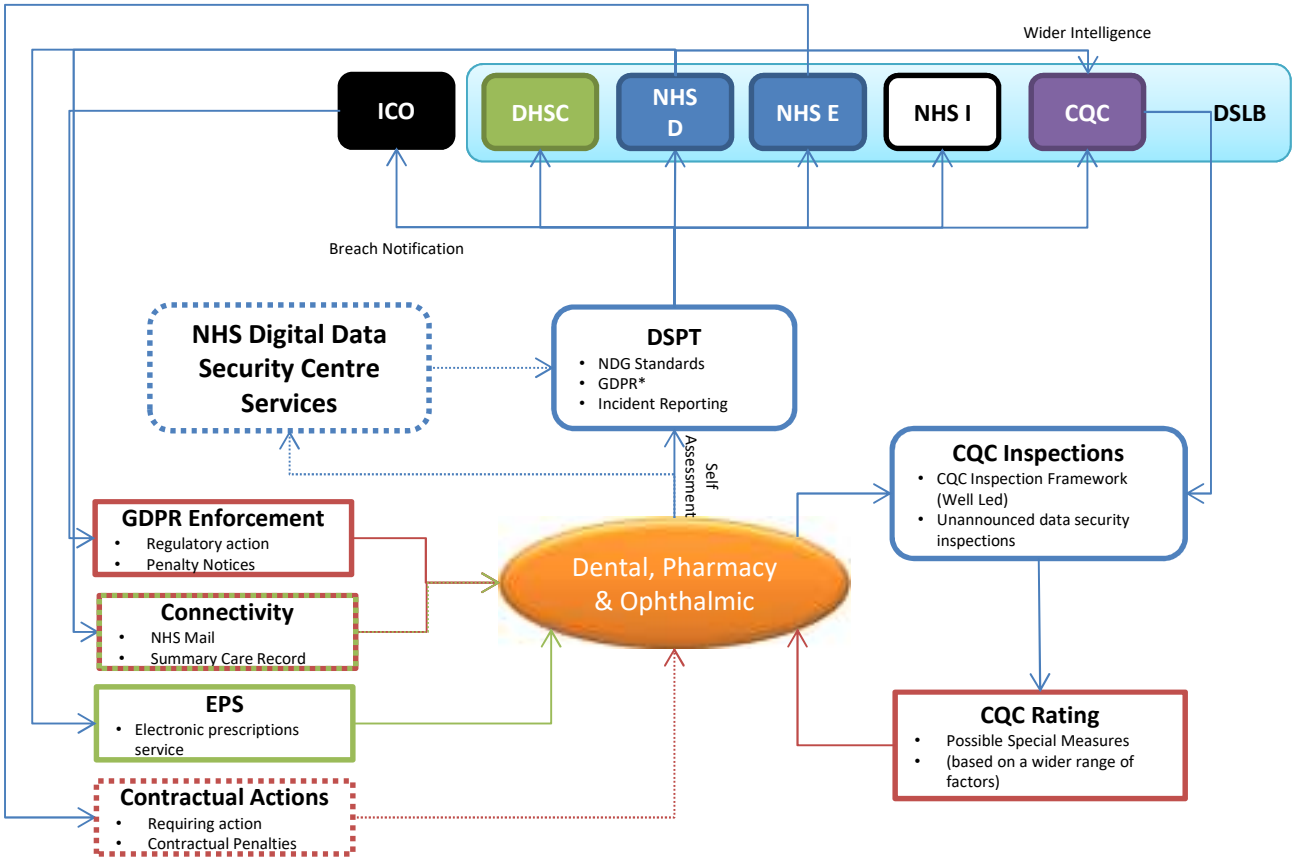
@nhsdigital

enquiries@nhsdigital.nhs.uk

0300 303 5678

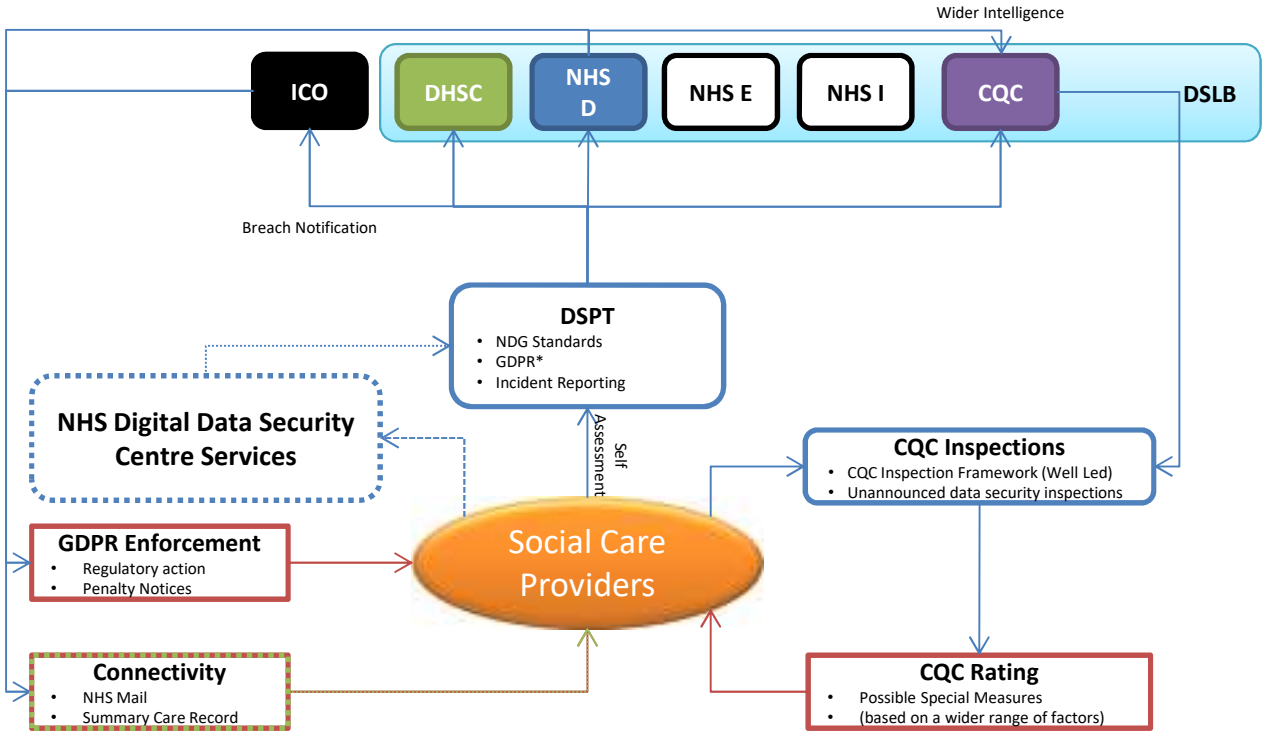
Information and technology
for better health and care


Wider Intelligence
ICO
DHSC
NHS D
NHS E
NHS I
CQC
DSLB
Breach Notification
CCGs / CSUs
NHS Digital Data Security Centre Services
• CareCERT Collect (patching, network scanning)
• Microsoft Licences
• Cyber Secure Operations Centre
DSPT
• NDG Standards
• GDPR*
• Incident Reporting
Self Assessment
CQC Inspections
• CQC Inspection Framework (Well Led)
• Unannounced data security inspections
GDPR Enforcement
• Regulatory action
• Penalty Notices
Contractual Actions
• Requiring action
• Contractual Penalties
General Practice
GPSoC
• Clinical Systems
GPIT
• Networks and Hardware
Secure by Default
CQC Rating
• Possible Special Measures
• (based on a wider range of factors)
Key
Assessment
Supporting Services
Enforcement Action



Key

Assessment | Supporting Services | Enforcement Action



Key

Assessment | Supporting Services | Enforcement Action