Data Security & Protection Toolkit and NHSmail

Pip Tomalin – NHS England and NHS Improvement (Midlands)

E: philip.tomalin@nhs.net

May 2019

House Keeping

- Fire drills and evacuation procedures
- Toilets
- Refreshments
- Q&As
- Wi-Fi code
- Signed in?

Our Goal

Enable you to (confidently) complete the

Data Security and Protection toolkit

on behalf of your organisation to

“Standards Met”

so that you can

access NHSmail

(and other) services to

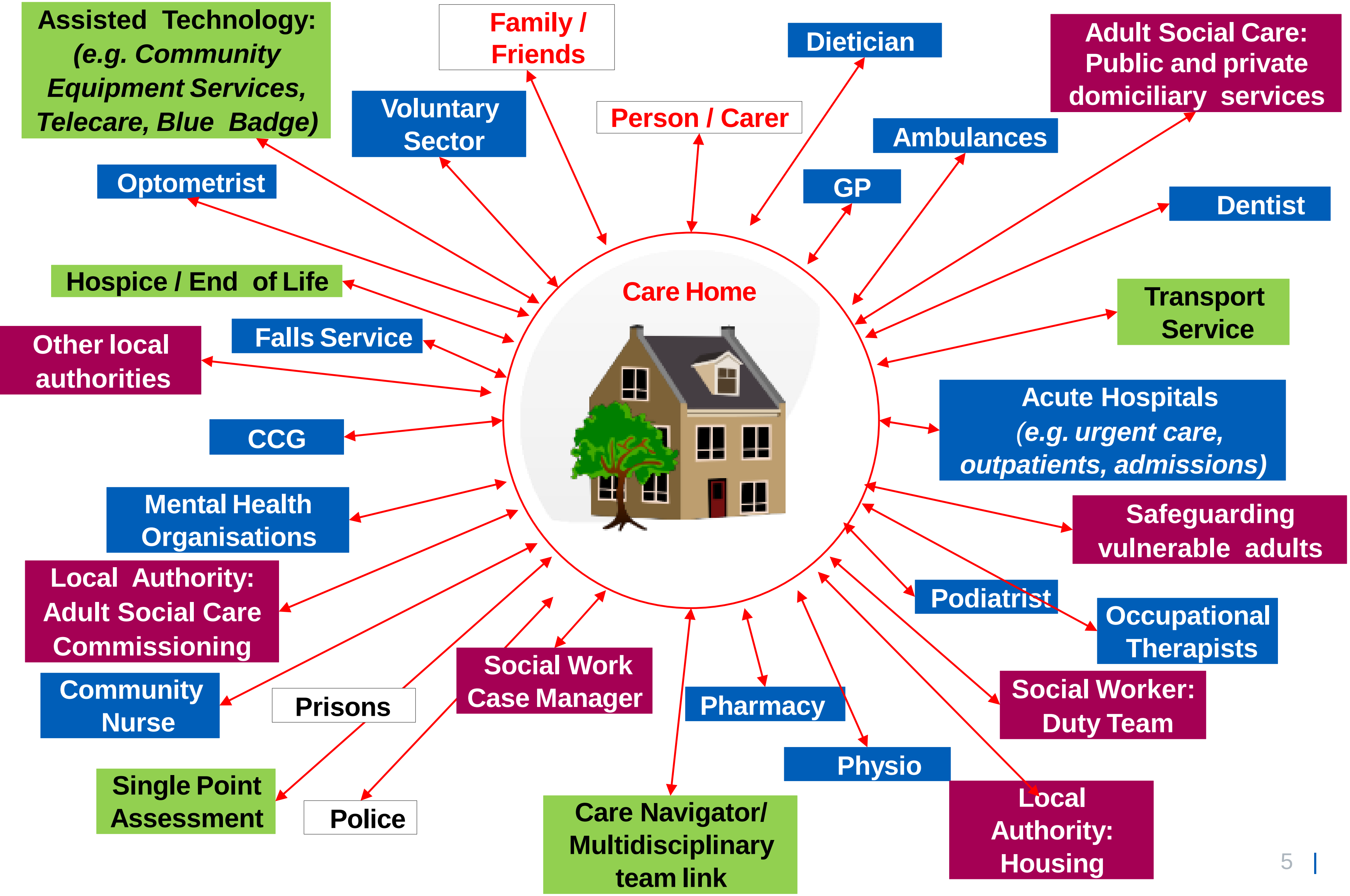
help improve the quality of care people receive

Outcomes / Objectives

1) Be able to explain the national offer of NHSmail for the Care Sector and the benefits this can give to residents and their organisation.
2) Be able to explain the processes they need to go through in order to access NHSmail for their organisation.
3) Be able to explain the importance and benefits of meeting the data security and protection assertions.
4) Be able to explain how to access the Data Security and Protection toolkit.
5) Have an understanding of the principles of the General Data Protection Regulation and the responsibilities their organisation has.
6) Understand the types of information their organisation needs to produce as evidence to meet the Data Security and Protection toolkit assertions.

Common information flows

NHS



Care Home

Assisted Technology: *(e.g. Community Equipment Services, Telecare, Blue Badge)*

Family / Friends

Person / Carer

Dietician

Adult Social Care: Public and private domiciliary services

Voluntary Sector

Ambulances

GP

Optometrist

Dentist

Hospice / End of Life

Transport Service

Falls Service

Other local authorities

CCG

Acute Hospitals *(e.g. urgent care, outpatients, admissions)*

Mental Health Organisations

Safeguarding vulnerable adults

Local Authority: Adult Social Care Commissioning

Podiatrist

Occupational Therapists

Social Work Case Manager

Community Nurse

Prisons

Pharmacy

Social Worker: Duty Team

Physio

Single Point Assessment

Police

Care Navigator/ Multidisciplinary team link

Local Authority: Housing

What is NHSmail?

The **secure** national email service for health and social care providing:

- Email
  - ➢ Microsoft Exchange 2013
  - ➢ 4GB mailbox per user account
- Accessible via:
  - ➢ Desktop email applications
  - ➢ Outlook Web Access (OWA) and on mobile devices
- NHSmail provides:
  - ➢ user and local administrator tools to manage accounts including audit and reporting functions
  - ➢ Access to NHS Directory (contacts for health and social care
  - ➢ Searchable options include name, clinical speciality, organisation and location
  - ➢ Instant Messaging
  - ➢ Quickly message other service users
  - ➢ Presence (whether another user is free, busy or in a meeting)

Why do I need DSP and secure email?

- General Data Protection Regulation (GDPR) / Data Protection Act 2018
- Prosecution of “data breaches” by the Information Commissioner’s Office (ICO)
- CQC Inspection KLOEs (2.8 – Well Led)
- NHS Standard Contract has [always had] it as a requirement
- NHS England Data Security & Protection (DSP) duty:

Any organisation wishing to access

ANY information held by the NHS or NHS system

(e.g. patient discharge information, summary care records, NHSmail)

MUST provide annual assurance that they have the expected standard of data security & protection in place

CQC KLOE 2.8 – Well Led

“How does the service assure itself that it has **robust arrangements** (including appropriate internal and external validation) **to ensure the security, availability, sharing and integrity of confidential data**, and **records** and data management **systems**, **in line with data security standards**?

Are lessons learned when there are data security breaches?”

ICO Prosecutions 2017-18

Sector	Monetary Penalties	Enforcement Notices	Undertakings	Prosecutions	Total
Central government	1	1	-	-	**2**
Charitable & Voluntary	13	-	-	1	**14**
Criminal Justice	4	-	8	1	**13**
Education &childcare	1	-	-	-	**1**
Finance insurance & Credit	12	6	2	1	**21**
General Business	4	5	-	7	**16**
Health	3	-	6	5	**14**
Land or property services	3	5	-	1	**9**
Legal	2	-	-	1	**3**
Local government	6	2	5	-	**13**
Marketing	26	9	-	-	**35**
Online technology & telecoms	7	-	1	1	**9**
Retail and manufacture	3	2	-	-	**5**
Transport and leisure	4	-	1	-	**5**
Utilities	1	-	-	-	**1**
TOTAL	**90**	**30**	**23**	**18**	**161**

Examples of Prosecutions

- **Bupa Insurance Services Limited** (Bupa) fined £175k for failing to have effective security measures in place to protect customers' personal information.
- **Michelle Harrison** (MKUHFT) inappropriately accessed records of 12 patients outside of her role (receptionist); fined £230-
- **Marian Waddell**, nursing auxiliary Royal Gwent Hospital accessed records of her neighbour = £412-
- **Bayswater Medical Centre** fined £35k: left highly sensitive medical information in an empty building for >18 months including: medical records, prescriptions and patient-identifiable medicine
- **NHS Digital** avoided further action after demonstrating they had taken appropriate steps to put plans in place to address the ICO's undertaking requirements
- **Care Homes:** c.100 care homes in late 2018 were given 2 weeks to register with the ICO (c.£40) or face a £600 fine

More details (including how to pay registration fee) available on ICO website: https://ico.org.uk/

NHSmail Offer (per site)

Each site receives:

- 1 generic account (e.g. theoaks.dudley@...)
- Up to 10 individual linked user accounts

Set-up & management options:

- National Administration Service;
- Via web-portal; or
- Self-management

For free & open to…

Residential Nursing Domiciliary

Regardless of funding source

Case Study 1: Stanfield Nursing Home

Background

- 41 residents aged 60+ with higher needs requiring nursing, specialist dementia and rest of life care
- RNs spent an average of 2 hrs a day on the telephone to GP surgeries, MH teams etc.
- Practice staff would hand write messages for the GP resulting in inaccurate information being recorded and the need for further telephone conversations between clinicians.
- Limited access to up-to-date medical notes and test results impacting on care and information available to residents.
- Prescription deliveries often lacked why they had been provided.

Benefits identified

- Direct, timely, accurate and secure communication now available between home staff and GPs / NHS MH & CHC teams
- 10 hrs/wk RN clinical time released
- Improved audit trail
- Increased patient safety
- Greater convenience and ease of sending information between organisations and to families/carers
- Challenges
- Resistance to using NHSmail at some GP practices
- Not yet adopted by hospital discharge teams

https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/Stanfield+case+study.pdf

Case Study 2: Swanton Care

Background

- Social Care provider with a national footprint of 850 staff operating from 28 locations.
- Provides residential and supported living care; specialist autism care, learning disability support, acquired brain injury and neuro-rehabilitation.
- No secure email service required information to be shared by post, fax or telephone taking a considerable amount of time and effort and impacted on majority of information sharing activities with LAs, NHS, Police and probation services

Benefits Identified

- Organisation now meets partners' expectations of a secure email service
- More efficient processes for receiving essential information (e.g. referrals, discharge summaries)
- Time saved from posting, faxing and chasing information
- Greater ease and convenience of sending information

https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/Swanton+case+study.pdf

Common Benefits of NHSmail

- Supports CQC inspection KLOEs
- Secure transfer of information
- Timely sharing of information
- Reduced risk of error in communications
- Improved safety for residents
- Time saved…increased time for care

How to Access NHSmail

1) **Check your GDPR arrangements, including registering with the ICO:** https://ico.org.uk/

2) **Find your ODS code / register with the Open Exeter Helpdesk:**

   exeter.helpdesk@nhs.net

3) **Register on the DSP toolkit:**

   www.dsptoolkit.nhs.uk/Account/Register

4) **Start completing the DSP toolkit:**

   www.dsptoolkit.nhs.uk/Account/Login

5) **Provide sufficient evidence to meet the “expected standard of assurance”**

   “Entry Level vs Standards Met

6) **Request access to the national NHSmail offer via the National Administration Service or web-site:**

   https://portal.nhs.net/Registration#/careprovider

7) **Contact local NHS organisations (e.g. CCG) and begin using as your email addresses…**

General Data Protection Regulation

[A summary of GDPR and DPA requirements]

Background

- General Data Protection Regulation & Data Protection Act 2018 form the legislation within the UK (replaces DPA 1998)
- Key definitions:
  - **Controller**: determines the purposes and means of processing personal data
  - **Processor:** responsible for processing personal data on behalf of a controller
- Applies to processing carried out by organisations operating within the EU AND those outside the EU that offer goods or services to individuals in the EU.
- Does not apply to certain activities including processing:
  - Covered by the Law Enforcement Directive,
  - For national security purposes; and
  - Carried out by individuals purely for personal/household activities.

For more information read the ICO website pages that start here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

What is covered (1)

- GDPR applies to the processing of personal data that is:
  - ➢wholly or partly by automated means; or
  - ➢the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.
- Personal data only includes information relating to natural persons who:
  - ➢can be identified or who are identifiable, directly from the information in question; or
  - ➢can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

What is covered (2)

- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.
- Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

7 Principles of GDPR

The following principles apply to all types of data covered by the law

1) Lawfulness, fairness and transparency
2) Purpose limitation
3) Data minimisation
4) Accuracy
5) Storage limitation
6) Integrity and confidentiality (security)
7) Accountability

For more information see the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

(1) Lawfulness

- You must identify valid grounds for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair.
    - ➢ You must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

(2) Purpose Limitation

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear basis in law.

(3) Data Minimisation

You must ensure the personal data you are processing is:

- **Adequate** – sufficient to properly fulfil your stated purpose;
- **Relevant** – has a rational link to that purpose; and
- **Limited to what is necessary** – you do not hold more than you need for that purpose.

(4) Accuracy

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

(5) Storage Limitation

- You must not keep personal data for longer than you need it.
- You need to be able to justify how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

(6) Integrity & Confidentiality (Security)

You must ensure that you have appropriate security measures in place to protect the personal data you hold. This requires you to:

- Consider things like risk analysis, organisational policies, and physical and technical security measures.
- Take into account additional requirements about the security of your processing.
- Consider the effectiveness and costs of implementation when deciding what measures to take (they must be appropriate both to your circumstances and the risk your processing poses).
- Look to use measures such as pseudonymisation and encryption where appropriate/possible.
- Ensure the ‘confidentiality, integrity and availability’ of your systems and services and the personal data you process within them.
- Be able to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- Have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

(7) Accountability

- You take responsibility for what you do with personal data and how you comply with the other principles.
- You must have appropriate measures and records in place to be able to demonstrate your compliance.

Our Individual Rights

People have the following specific rights:

1) The right to be informed
2) The right of access
3) The right to rectification
4) The right to erasure
5) The right to restrict processing
6) The right to data portability
7) The right to object
8) Rights in relation to automated decision making and profiling.

A very rough summary…

We all need to have:

- ✓ Policies & processes in place to deliver “data protection by design and default”

We need to be able to evidence:

- ✓ What data we have (personal/special category);
- ✓ Why we have/share it (lawful reasons);
- ✓ Where it comes from and where it goes to;
- ✓ When we destroy it (retention);
- ✓ Who has access to it; and
- ✓ How we use it/keep it safe.

Summary: Personal Information

- Any information through which an individual can be identified or is identifiable if you can distinguish them from other individuals
- GDPR provides a non-exhaustive list that includes:
  - ➢ Name
  - ➢ Unique identification number
  - ➢ Location data (address)
  - ➢ IP address
  - ➢ Cookies

Special Category Information

The following types of data / information are considered more sensitive and therefore require a higher level of protection:

- Biometrics (where used for ID purposes)
- Ethnic origin
- Genetics
- **Health**
- Politics
- Race
- Religion
- Sex life
- Sexual orientation
- Trade union membership

Lawful Processing (Personal Information)

There must be a lawful basis for processing any personal information (**Article 6 conditions**):

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or those of a third party. A good reason to protect the individual's personal data overrides those legitimate interests.

Basic Principle of Processing

The question to always consider:

Is the processing

objectively necessary for the stated purpose,

NOT

because it is a necessary part of our chosen methods.

Lawful Basis: Special Category Information

Special Category data requires a greater protection (**Article 9 conditions**)

a) Explicit consent

b) Employment, social security, social protection law

c) Vital interests when an individual is legally or physically unable to give consent

d) Legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim

e) The personal data has been manifestly made public by the individual

f) For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) Substantial public interest

h) The provision of health or social care, treatment or the management of health or care systems and services or the assessment of the working capacity of an employee

i) Public health interests

j) For archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes

How to do GDPR…

[A Four Step Process]

The four step process

1) Assign key roles and responsibilities
2) Record the types of information you hold / receive and why you have it
3) Record how and why this information is shared
4) Agree the appropriate policies, procedures and practical implementation you need

For more information see CPA guidance “How to document your data processing” and supporting IAR/RoPA templates: www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

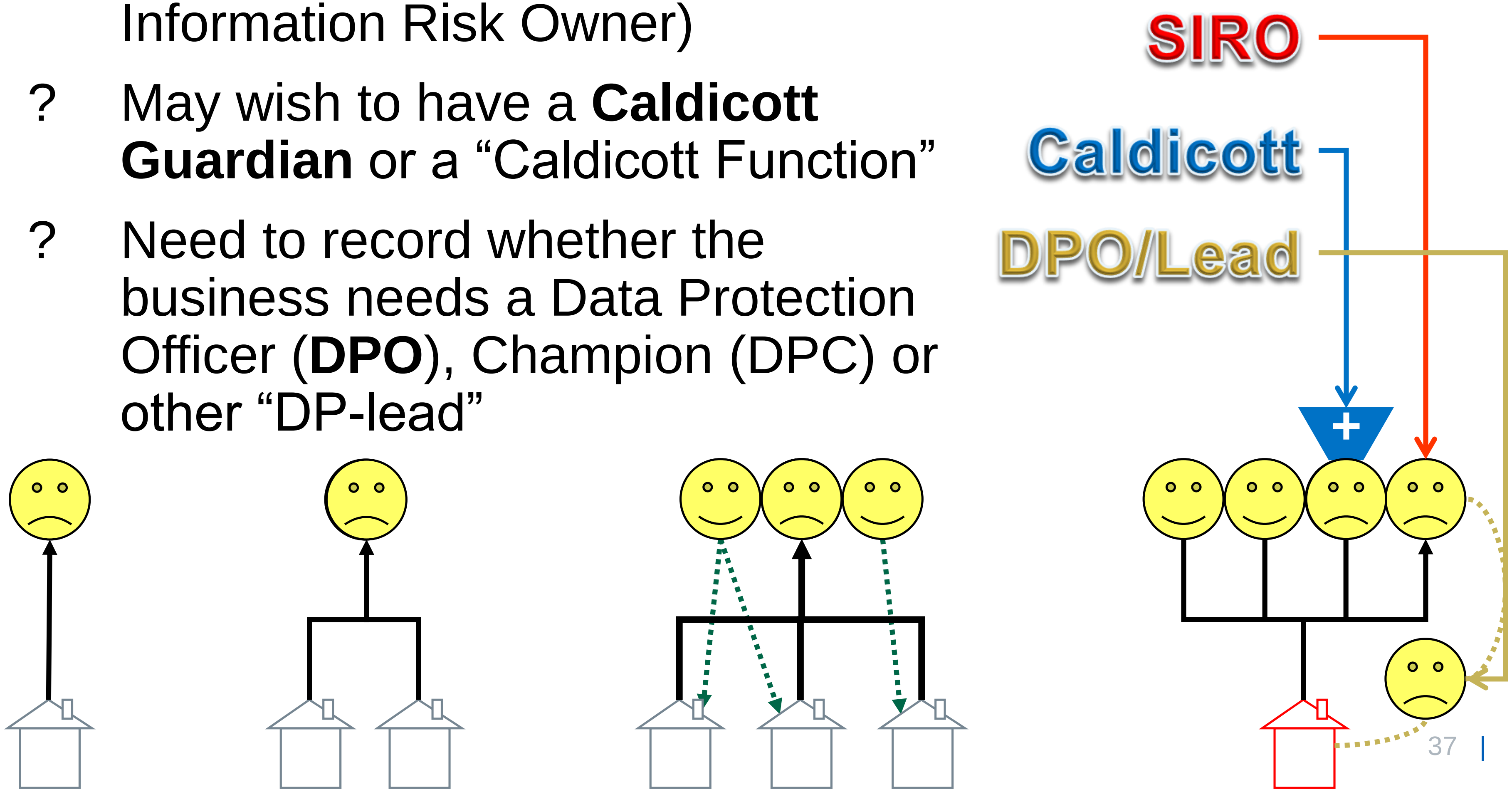
Step 1: Agree who is responsible for Data Security & Protection

At Board / Owner level, every organisation:

✓ Needs to have a **SIRO** (Senior Information Risk Owner)

? May wish to have a **Caldicott Guardian** or a “Caldicott Function”

? Need to record whether the business needs a Data Protection Officer (**DPO**), Champion (DPC) or other “DP-lead”



Key Roles

Senior Information Risk Owner (SIRO)

- Needs to be the owner or an Executive Director / other senior board member [e.g. Chief Information Officer Director of Operations]
- Overall accountable for ensuring appropriate policies, procedures etc are in place and followed

Caldicott Guardian

- Only a requirement for public authorities; not mandatory for social care providers – although encouraged.
- Should be independent of SIRO; however, depending on the size of organisation this is not always possible.; and, in order of priority: a director, senior manager; a senior health / social care professional; or, the person with responsibility for promoting clinical governance
- Consider adopting a "Caldicott Function" rather than full blown UK Caldicott Guardian Council membership

Data Protection Officer (DPO):

- Must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- They can be an existing employee or externally appointed or appointed across a number of organisations
- They must be registered with the ICO.
- They: inform and advise organisations about complying with GDPR and other data protection laws; monitor compliance with GDPR and data protection laws – including staff training and internal audits; advise on and monitor data protection impact assessments; co-operate with the ICO / being the first contact point for the ICO and citizens.

For more details see NHS Digital "Key Roles and DPO Guide": www.dsptoolkit.nhs.uk/Help/2

Do I need a DPO?

The law says that you must appoint a Data Protection Officer (DPO) if:

a) You are a public authority or body (except for courts acting in their judicial capacity);

b) Your core activities require **large scale**, regular and systematic monitoring of individuals (for example, online behaviour tracking); or

c) Your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

THERE IS NO DEFINITION OF "LARGE SCALE"

CPA & NHS Digital DPO Advice:

- Assign someone to have a "data protection champion" (DPC) role i.e. responsible for data security and data protection (e.g. someone familiar with DSP topics).
- The DPO should not be Registered Manager as considered a conflict of interest.

If you decide your organisation doesn't need a DPO or chooses to adopt a Data Protection Champion / Lead (or not)
*****Document your reasons why in policy and the DSP toolkit*****

Step 2: Record the types of information you have

Audit and list…

- □ What types of personal information do you have?

  [“information assets”. These include any software, hardware and smart devices]

- □ Where do you keep each “asset”?

  [Location & security in place]

- □ Who has access to them?

  [By role/title, for software include level of access]

- □ Why do you need each one?

- □ Risk assess each asset / system i.e.:
  - ➢ Ask yourself what would the impact on the person be if there was a breach?
  - ➢ How might this occur and could anything else be done to help stop a breach?

Information Asset Register

Step 3: Record how information is shared

For each asset type you process [receive/share], record:

□ Your “lawful reason” for the processing

[Article 6 & Article 9]

□ Whose data it is and what kind of data it is

[e.g. staff – financial information; residents – care plans; Personal or Special Category]

□ The people / organisations you share the information with

[e.g. GP Practices, Hospitals]

□ Whether the data goes outside of the EEA (and the extra precautions you therefore take)

[Out of EEA requires greater measures in place]

□ How long you keep each type of information before destroying it

[Records retention period]

□ A description of the technical & organisational security measures used to protect the data

Record of Processing Activities

NOTE

If you have fewer than 250 employees:

- Only record processing that:
  - Is done regularly i.e. you don’t need to record a one-off exchange; or
  - Is likely to result in a risk to the rights and freedoms of individuals; or
  - Contains special category or criminal convictions data

If you have more than 250 employees:

- You must include any ad-hoc / less regular processing activities

Step 4: **Policy**, Procedure & Practical Implementation

Produce a policy or policies to cover:

- **Data Protection:** how you will implement legal requirements to ensure data protection by design and by default
- **Data Quality:** how you will ensure you keep the data you hold accurate and correct any errors
- **Record Keeping:** how the data you hold will be looked after, what rights data subjects (e.g. residents) have and how you will facilitate access
- **Data Security:** how you prevent data breaches from occurring and what you will do if there is a breach
- **Network Security:** how you will ensure any devices that are used to access data electronically will be protected and data kept safe

See CPA website for templates: www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

Step 4: Policy, **Procedure** & Practical Implementation

Written procedures could include:

- ❑ Information Asset Register
- ❑ Record of Processing Activities
- ❑ Leaver-Starter arrangements
- ❑ Portable device assignment forms
- ❑ Reporting (suspected) data security breaches
- ❑ Business continuity plan i.e. what to do if essential records are destroyed (fire), or can’t be accessed (IT failure), or you have a significant data breach (media attention)

See CPA website for templates: www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

Step 4: Policy, Procedure & **Practical Implementation**

Information to support **staff** awareness and behaviour should include:

- ❑ Staff Data Security and Protection Code of Conduct, acceptable use of IT etc
- ❑ Guidance on what data they can share, with whom and how to do so safely
- ❑ The rights for individuals and how to handle Subject Access Requests
- ❑ How to ensure the quality of data they record
- ❑ What to do if they suspect a breach has happened
- ❑ Explicit reference to GDPR in their contract of employment

See CPA website for templates: www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

Step 4: Policy, Procedure & **Practical Implementation**

Information to support **residents** should include:

- ❑ Advice / information on how you keep their personal information safe
- ❑ Who you will share their information with and under what conditions
- ❑ Their rights to access any information you hold on them
- ❑ When they can chose to refuse sharing
- ❑ Access to your privacy notice

See CPA website for templates: www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html

Hints and Tips…

- Use the Care Provider Alliance templates
- GDPR is an **ongoing process**, not a one-off…registers / records can be added to
- Start with the obvious (e.g. care plans, staff records)
- Create IAR/RoPA by directorate/department
- For IAR/RoPA, walk room by room and/or send a pre-populated template for homes to amend.
- Understand the concerns staff, residents and their families have.

From your GDPR you will have…

- ✓ Data Security and Protection responsibilities agreed
- ✓ Data Protection Policy
- ✓ Data Quality Policy
- ✓ Data Security Policy
- ✓ Data Security breach reporting process
- ✓ Record Keeping Policy
- ✓ Network / IT Security Policy
- ✓ Business Continuity Plan for data loss / breach
- ✓ Information Asset Register (IAR)
- ✓ Record of Processing Activities (RoPA)
- ✓ Guidance for staff
- ✓ Privacy notice
- ✓ Registered with the ICO
- ✓ Staff that know what to do

To complete your DSP toolkit you will also need:

- ❖ Copies / access to your policies etc.
- ❖ A reliable internet connection

Data Security & Protection (DSP) Toolkit

Contents:

1) Background

   [What is it and why I have to do it]

2) How to register
3) What it is like

   [Demonstration /orientation of the toolkit]

4) What I need to complete it
5) How to present my evidence

   [How to answer the questions]

Overview

- An online self-assessment tool to demonstrate compliance GDPR.
- An annual assurance process running from 1st April to 31st March.
- Helps to evidence CQC KLOE 2.8 (Well Led).
- Based on the ten National Data Guardian data security standards for health and social care organisations (i.e. GDPR expectations for the health and social care organisations)

Any organisation wishing to access

ANY information held by the NHS or NHS system

MUST provide annual assurance that they have the expected standard of data security & protection in place

The steps…

1) **Check your GDPR arrangements, including registering with the ICO:** https://ico.org.uk/

2) **Find your ODS code / register with the Open Exeter Helpdesk:**

   exeter.helpdesk@nhs.net

3) **Register on the DSP toolkit:**

   www.dsptoolkit.nhs.uk/Account/Register

4) **Start completing the DSP toolkit:**

   www.dsptoolkit.nhs.uk/Account/Login

5) **Provide sufficient evidence to meet the “expected standard of assurance”**

   “Entry Level vs Standards Met

If you have any problems with your ODS codes, businesses/sites missing from your toolkit page email **Exeter Helpdesk**: exeter.helpdesk@nhs.net

ODS Codes

Just a unique identifier – every organisation interacting with the NHS has [at least] one.

- Head Quarters have one (“A...”)
- Every site has one (“V…”)
- Additional services may have ones allocated

Search for yours here: https://odsportal.hscic.gov.uk/Organisation/Search

Or contact **Exeter Helpdesk**: exeter.helpdesk@nhs.net; 0300 303 4034

They will ask for:

- Your name
- Your contact telephone number
- Your contact email address
- Your organisation’s name and business address(es)
- The service you would like (i.e. “I’d like to know my ODS code”)

They may also ask for:

- CQC Registration ID
- Type of provider (residential, nursing or domiciliary)

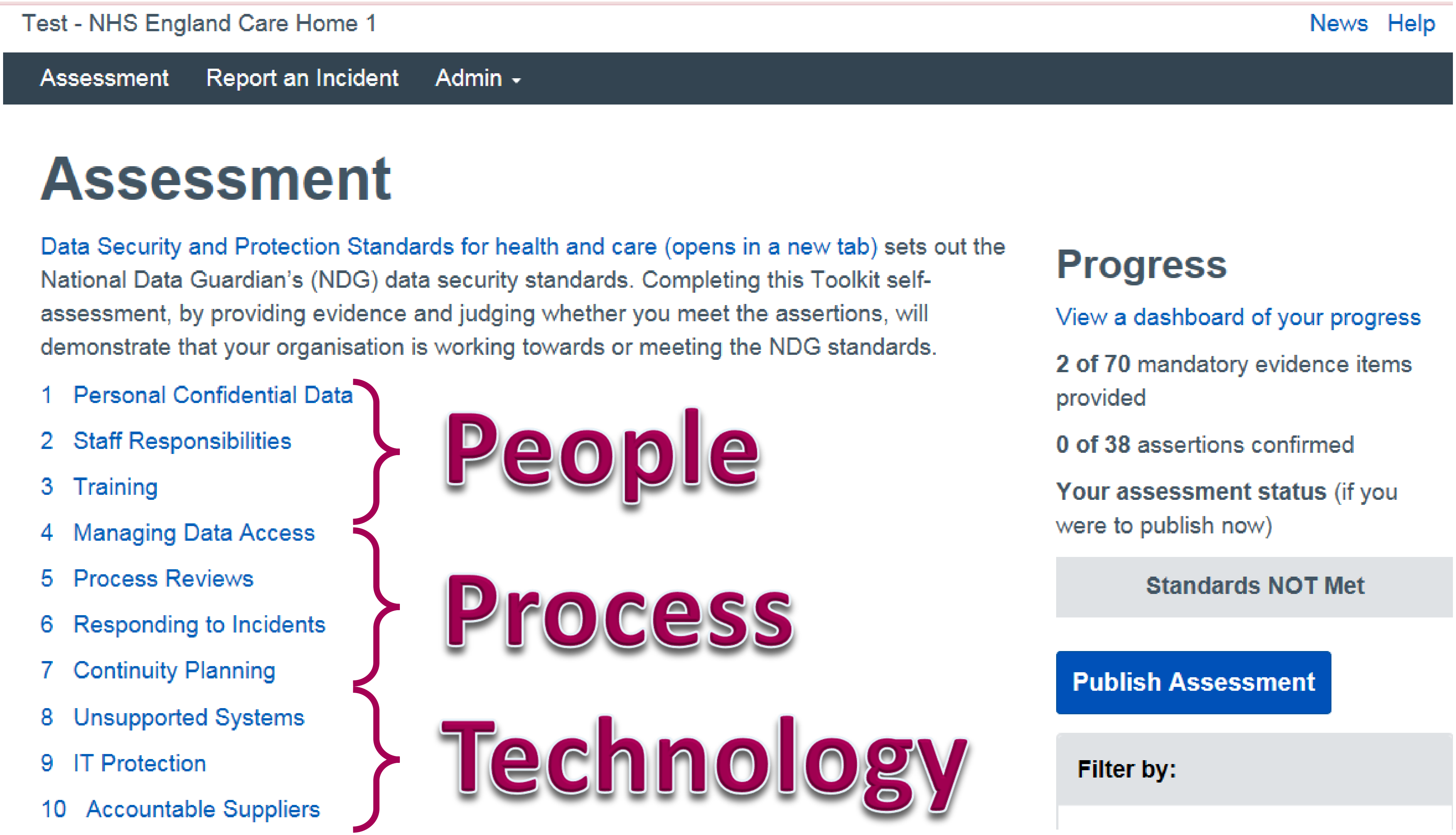
Registering on the DSP Toolkit

1) Go to: www.dsptoolkit.nhs.uk/Account/Register
2) Click the blue "**Continue to questions**" button.
3) Enter your **ODS code** (the **HQ** one **[A…]**) then click the blue "**Continue**" button
4) Enter the "**Captcha**" code displayed
5) Enter your **current email address**
6) Click "**Submit**" and check your email for the automatic response email
7) To **confirm registration** – click on the link in the automatic email **within 24 hours**

Organisation Profile

- Log in to the toolkit at: www.dsptoolkit.nhs.uk/Account/Login
- Click the blue “**Continue to questions**” button
- **Choose your organisation type – you will either be a “Care Home”, or a “Domiciliary Care Organisation”**. If you do both: choose the larger / core one for your business.
- Enter the name and details for your “**Caldicott Guardian**” or “**Not Appropriate**”; add an email address even if entering “N/A”
- Enter the name and details for your “**Senior Information Risk Owner**”
- Enter the name and details for your “**Information Governance Lead**” or “**Not Appropriate**”; add an email address even if entering “N/A”
- Enter the name and details for your “**Data Protection Officer**” or “**Not Appropriate**”; add an email address even if entering “N/A”
- Is NHSmail the only email system? Select: **Yes / No / Not Sure**
- Do you have Cyber Essentials PLUS certification for last 12 months? Select: **Yes / No / Not Sure**
- Click the blue “**Accept and Submit**” button
- The Administrator can change any of these answers at any time.

Main Screen



Assessment

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

1 Personal Confidential Data
2 Staff Responsibilities
3 Training
4 Managing Data Access
5 Process Reviews
6 Responding to Incidents
7 Continuity Planning
8 Unsupported Systems
9 IT Protection
10 Accountable Suppliers

People

Process

Technology

Progress

View a dashboard of your progress

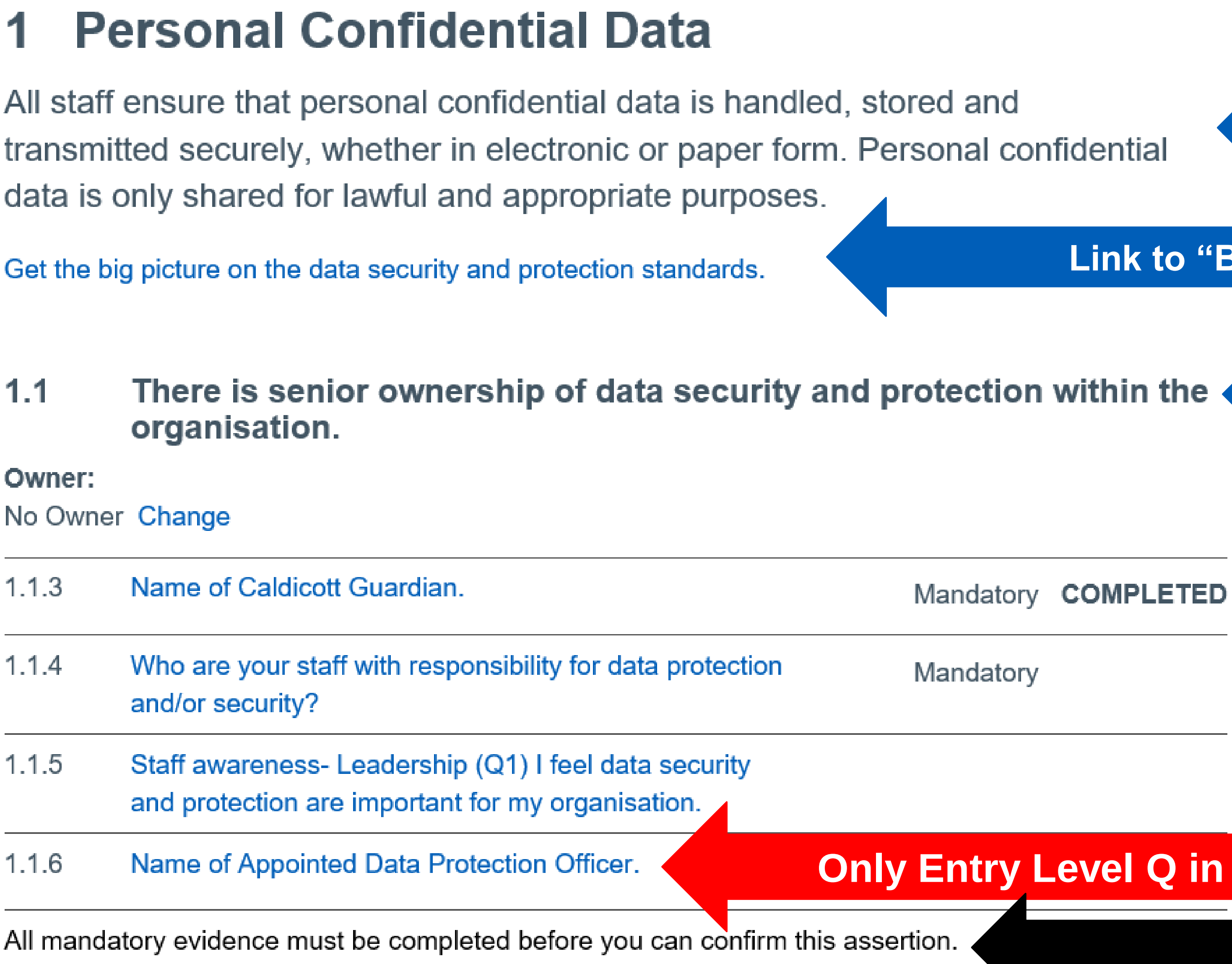
2 of 70 mandatory evidence items provided

0 of 38 assertions confirmed

Your assessment status (if you were to publish now)

Standards NOT Met

Example Assertion & Question Set



1 Personal Confidential Data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Get the big picture on the data security and protection standards.

1.1 There is senior ownership of data security and protection within the organisation.

Owner:

No Owner Change

1.1.3	Name of Caldicott Guardian.	Mandatory	**COMPLETED**
1.1.4	Who are your staff with responsibility for data protection and/or security?	Mandatory	
1.1.5	Staff awareness- Leadership (Q1) I feel data security and protection are important for my organisation.		
1.1.6	Name of Appointed Data Protection Officer.		

All mandatory evidence must be completed before you can confirm this assertion.

NDG Standard

Link to “Big Picture” guide

Your Assertion

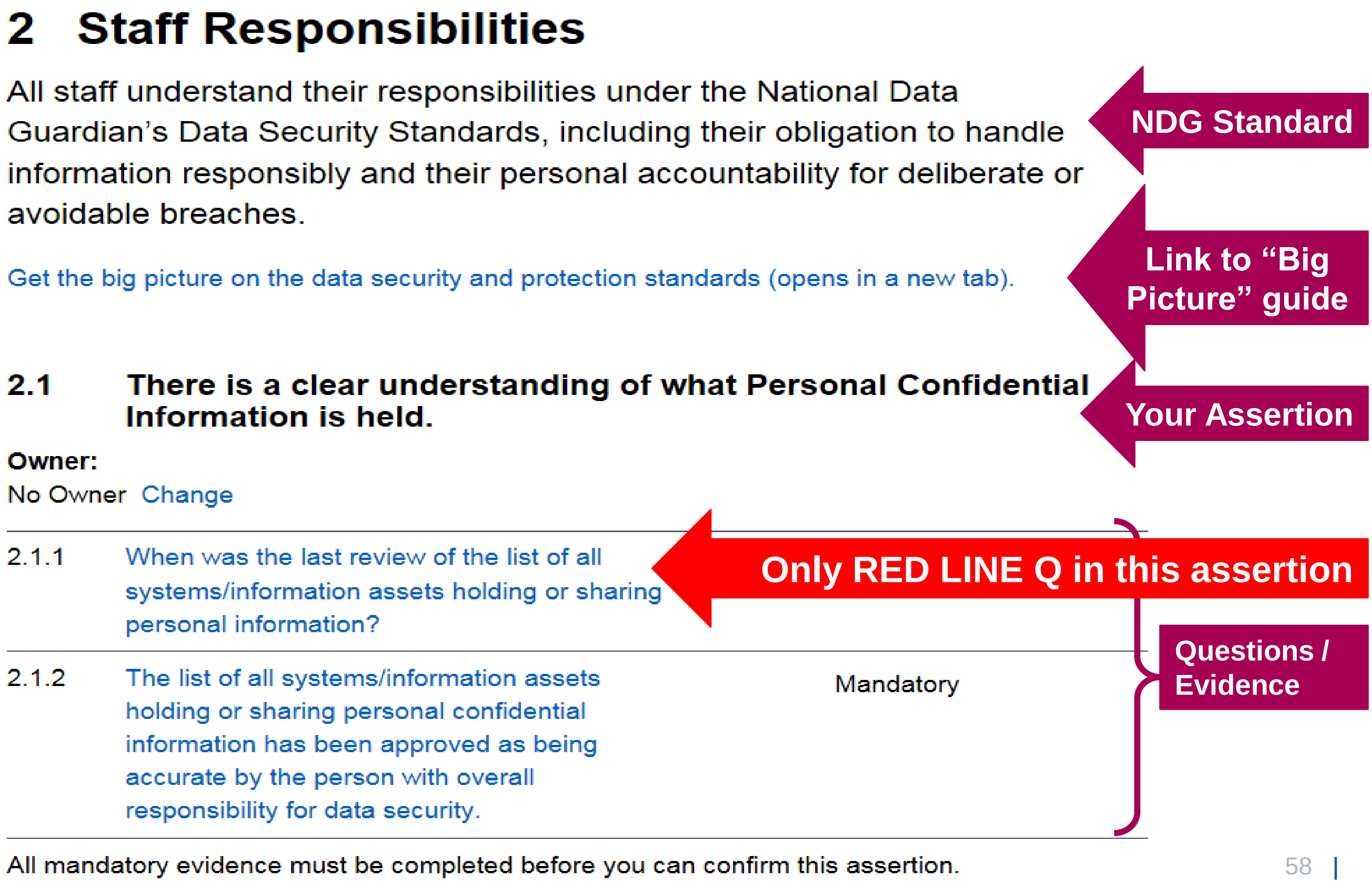
Already done

Questions / Evidence

Only Entry Level Q in this assertion!

Not quite true…

You will see…



2 Staff Responsibilities

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Get the big picture on the data security and protection standards (opens in a new tab).

2.1 There is a clear understanding of what Personal Confidential Information is held.

Owner:

No Owner Change

2.1.1	When was the last review of the list of all systems/information assets holding or sharing personal information?	
2.1.2	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security.	Mandatory

All mandatory evidence must be completed before you can confirm this assertion.

NDG Standard

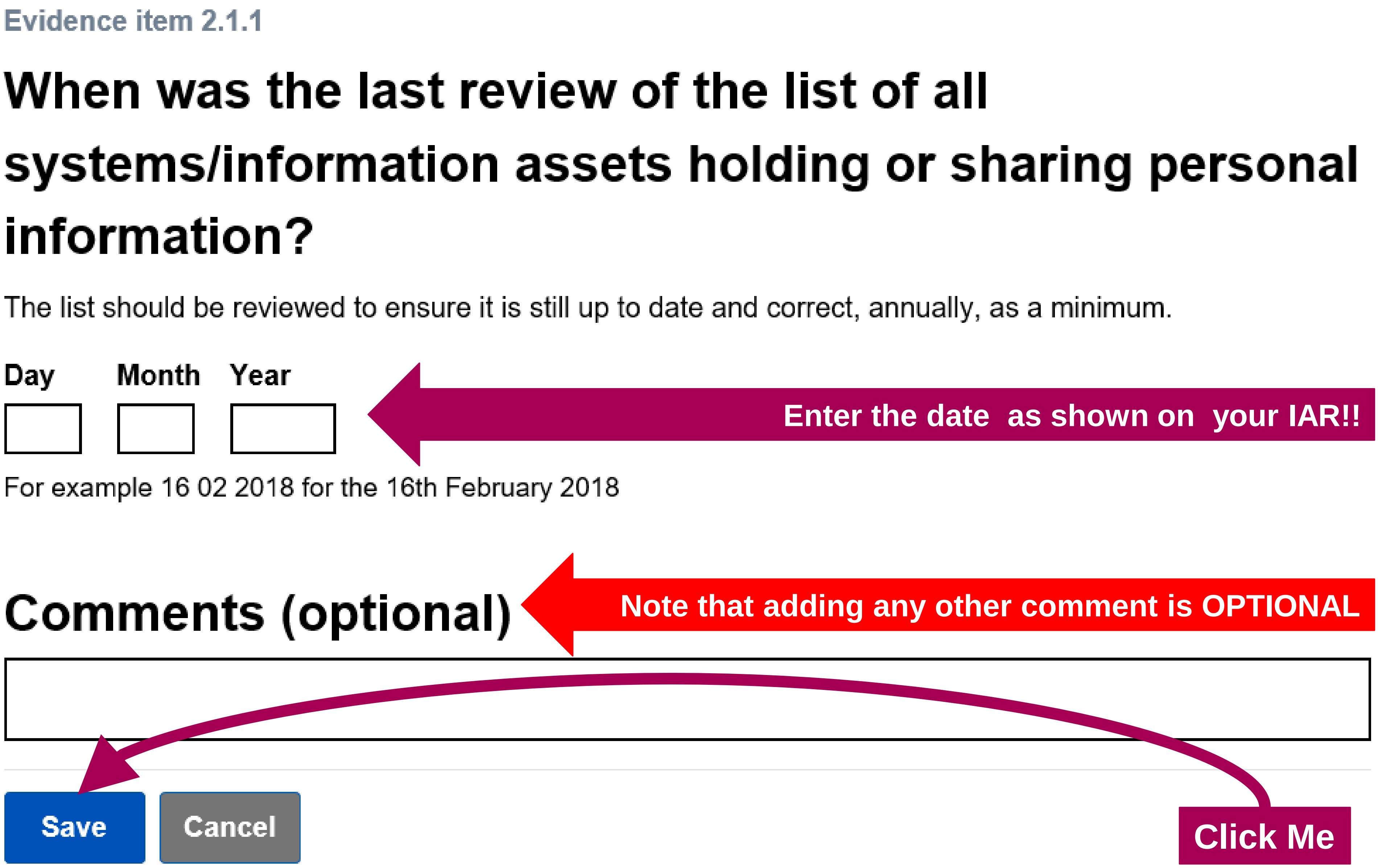
Link to "Big Picture" guide

Your Assertion

Only RED LINE Q in this assertion

Questions / Evidence

You will see…



Evidence item 2.1.1

When was the last review of the list of all systems/information assets holding or sharing personal information?

The list should be reviewed to ensure it is still up to date and correct, annually, as a minimum.

Day	Month	Year
□	□	□

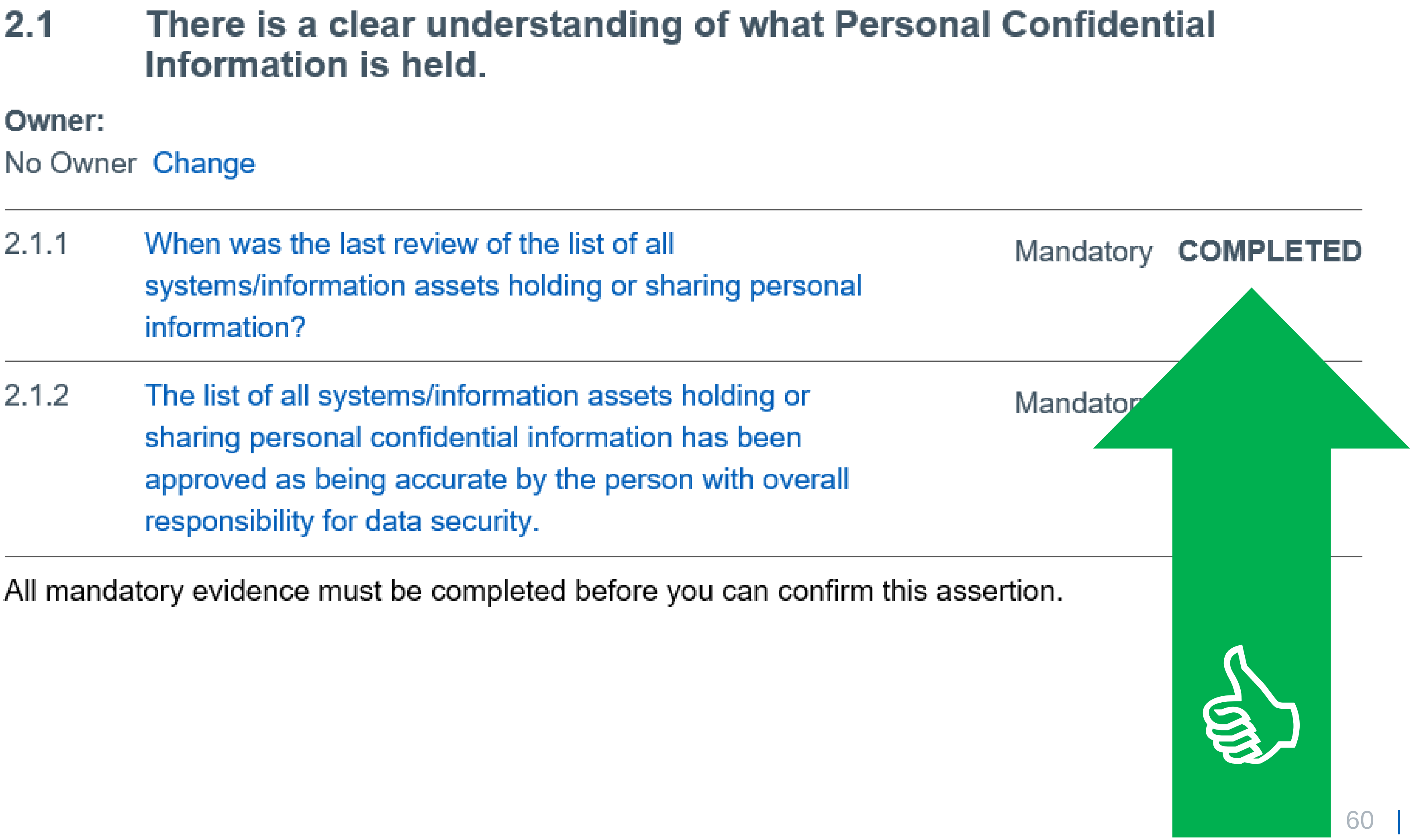
For example 16 02 2018 for the 16th February 2018

Enter the date as shown on your IAR!!

Comments (optional)

Note that adding any other comment is OPTIONAL

Now you will see…



2.1 There is a clear understanding of what Personal Confidential Information is held.

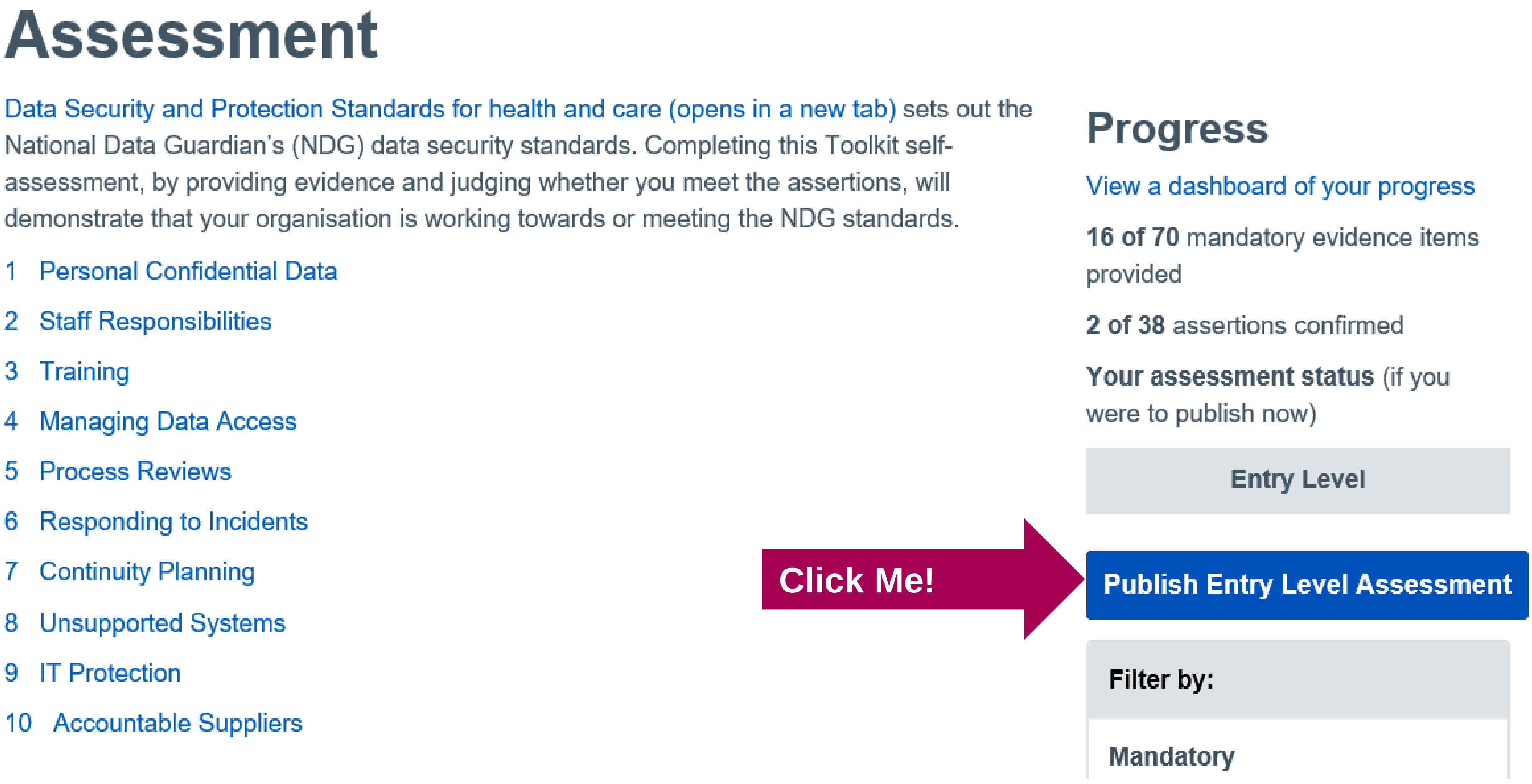
Owner:

No Owner Change

2.1.1	When was the last review of the list of all systems/information assets holding or sharing personal information?	Mandatory	**COMPLETED**
2.1.2	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security.	Mandator	

All mandatory evidence must be completed before you can confirm this assertion.

After 16 evidence statements…



Assessment

Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

1 Personal Confidential Data

2 Staff Responsibilities

3 Training

4 Managing Data Access

5 Process Reviews

6 Responding to Incidents

7 Continuity Planning

8 Unsupported Systems

9 IT Protection

10 Accountable Suppliers

Progress

View a dashboard of your progress

16 of 70 mandatory evidence items provided

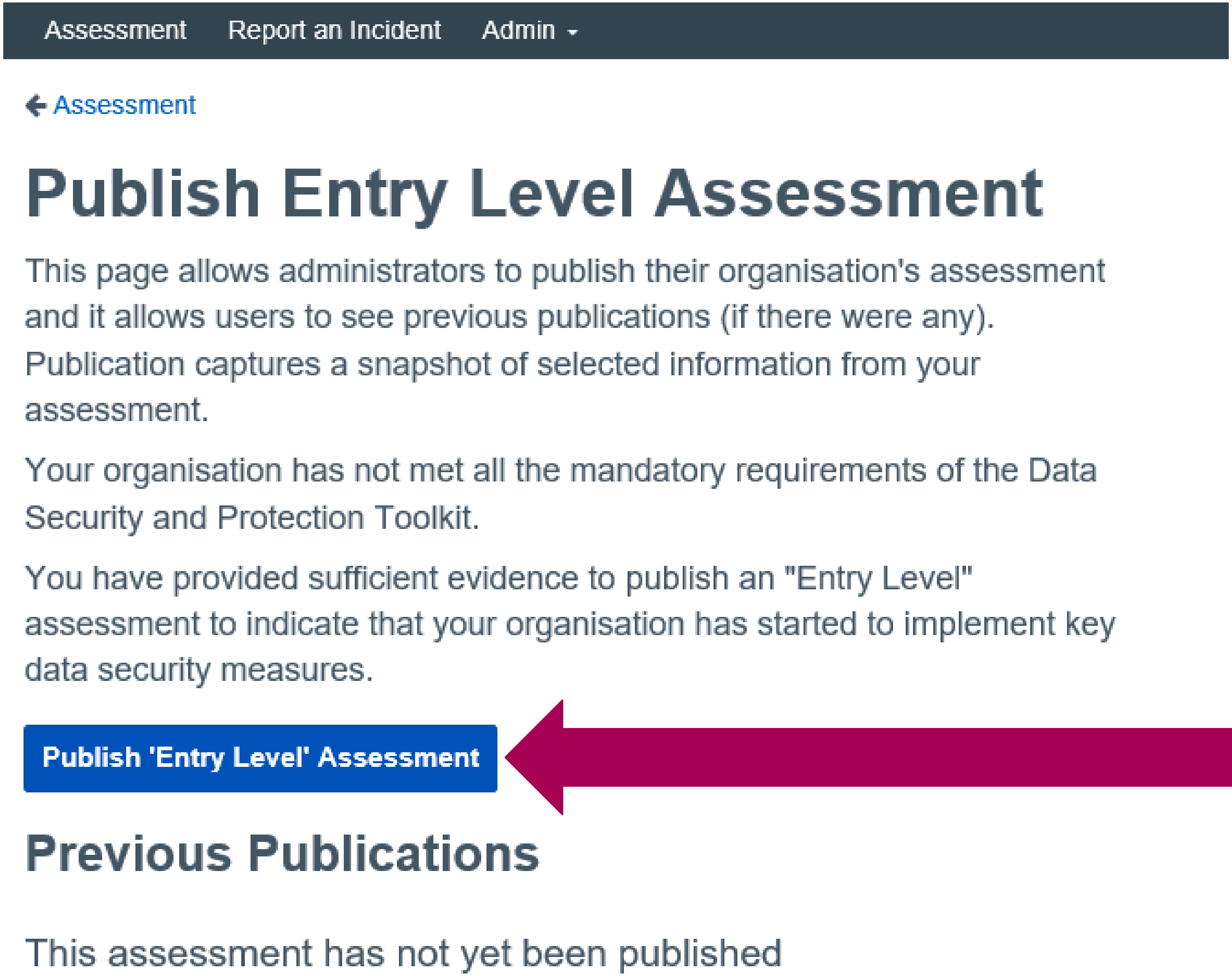
2 of 38 assertions confirmed

Your assessment status (if you were to publish now)

Entry Level

Click Me!

Then…



Publish Entry Level Assessment

This page allows administrators to publish their organisation's assessment and it allows users to see previous publications (if there were any). Publication captures a snapshot of selected information from your assessment.

Your organisation has not met all the mandatory requirements of the Data Security and Protection Toolkit.

You have provided sufficient evidence to publish an "Entry Level" assessment to indicate that your organisation has started to implement key data security measures.

Click Me!

Previous Publications

This assessment has not yet been published

Entry Level Questions (1)

Ref	Assertion	Question / Evidence	Suggestion
1.1.6	There is senior ownership of data security and protection within the organisation.	Name of Appointed Data Protection Officer	Name of your DPO (if appropriate)
1.2.1	There are clear data security and protection policies in place and these are understood by staff and available to the public.	There is a data security and protection policy or policies that follow relevant guidance.	See the list of policy templates; copies available from the Care Provider Alliance (CPA)
1.2.3		Policy has been approved by the person with overall responsibility for data security.	Make sure your policies are in-date and signed by the responsible person (e.g. your SIRO)
1.3.1	Individuals' rights are respected and supported (GDPR Article 12-22)	ICO Registration Number	Your Information Commissioner Office registration number
1.3.3		How have individuals been informed about their rights and how to exercise them?	Details of how residents / service users have been told about their rights and how to exercise them (see leaflet)
1.4.1	Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)	A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing.	Your Information Asset Register and Record of Processing Activities produced during GDPR readiness (see CPA templates)
1.5.1	Personal information is used and shared lawfully.	There is approved staff guidance on confidentiality and data protection issues.	List or link to what is there for your staff e.g. guidance documents (see CPA templates), contract clauses (see CPA template) and training records.

Entry Level Questions (2)

Ref	Assertion	Question / Evidence	Suggestion
1.6.1	The use of personal information is subject to data protection by design and by default	There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	See the CPA Data Protection Policy template
1.6.7		There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.	See 6.3 & 7.2.3 of the CPA Data Protection Policy template Use the ICO DPIA form / process
1.6.11		All high-risk data processing has a Data Protection Impact Assessment carried out before processing commences.	These are best considered when completing your RoPA as only applies to High-Risk processing activities
1.7.1	Effective data quality controls are in place	There is policy and staff guidance on data quality.	See CPA staff guidance templates
2.1.1	There is a clear understanding of what Personal Confidential Information is held.	When was the last review of the list of all systems/information assets holding or sharing personal information?	See CPA Data Security Policy 4.5, 5.7,& 7.3 and your IAR This should be reviewed (minimum) annually.
2.3.2	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.	All employment contracts contain data security requirements.	See CPA template draft clause, engage with staff as part of training and update contracts

Entry Level Questions (3)

Ref	Assertion	Question / Evidence	Suggestion
4.1.1	The organisation maintains a current record of staff and their roles.	The organisation maintains a current record of staff and their roles.	You should have one of these already for payroll.
6.1.1	A confidential system for reporting security breaches and near misses is in place and actively used.	A data security and protection breach reporting system is in place.	See : • CPA Data Security Policy template section 8 • CPA Network Security Policy template section 21 • CPA Breach Reporting template
10.1.1	The organisation can name its suppliers, the products and services they deliver and the contract durations.	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	This could be part of your IAR

Next Steps…

Before registering for NHSmail

- Once you have received the confirmation of your DSP submission (Entry Level or Standards Met) you can immediately apply for the NHSmail.
- Large providers (i.e. you have your own IT department) wishing to pursue a “self-management” approach should contact feedback@nhs.net to discuss options with NHS Digital
- Smaller Providers should collect the following information:
  1) Name, address, ODS site code, CQC location ID and name of registered manager and their CQC registration code for each site.
  2) Name, role and MOBILE PHONE number* of each member of staff at each site with a need for an email address (Note: check spelling, use the name they are known as e.g. Bob Jones vs Robert Jones)
  3) Identify 2 people to authorise changes (i.e. Owner & Manager)
  4) Register the first accounts for the HQ first (i.e. use the HQ ODS code)

For more information see: https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/HowtocompletetheNHSmailSocialCareRegistrationPortal.pdf

* Mobile numbers are essential for password resets. They can be hidden from view on the NHS directory if staff wish

Step 1 - Registering for NHSmail

- With the information from previous slide to hand, go to: https://portal.nhs.net/Registration#/careprovider
- Complete the “Care Provider Pre-Requisite Questionnaire” as follows:

1) Do you already have an NHSmail account? **NO**
2) Have you completed the Data Security and Protection Toolkit to entry level or higher? **YES**
3) Have you already received an email or a letter containing a One-Time Passcode within the past 2 weeks? **NO**
4) Do you know your CQC Contact ID (or Registered Manager’s ID or Manager ID)? **YES**
5) Enter the Postcode of your home. **Start with the HQ postcode**
6) Check the Organisation Name and ODS code shown is correct, (HQ codes start [A...], site codes [V…] there may be other business linked to the postcode e.g. GP practices, pharmacists etc
7) Enter the **CQC Location ID** for the site chosen
8) Enter the **Registered Manager ID** for the site chosen

For more information see: https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/HowtocompletetheNHSmailSocialCareRegistrationPortal.pdf

Step 2 – Creating Accounts

It is very important to consider the data you enter now. Once names etc are set it is unlikely to be possible to change them

1. Enter **Town Name**: this is the town/village where the site is located. It will form part of the generic email name i.e. care.town.homename+ODScode@nhs...
2. Enter the **name of the first person who is going to authorise changes**. For a small owner-provider, this should be the owner or registered manager. If their name is Mr Michael Mouse, their email address will become michael.mouse@nhs.... If they prefer to be known as "mickey" enter their name as Mickey Mouse to get mickey.mouse@nhs....; if there is more than one Mickey Mouse, it will be mickey.mouse2@...etc
3. Add their **current email address**, **mobile phone number** and select the most **appropriate role** from the dropdown list.
4. Click "**Add Member**"
5. Tick "**Add to shared mailbox**" and "**Mark as Mailbox Admin**"
6. Repeat adding the details for the second person in the same way as above – it strongly recommended that at least 2 people are marked as "**mailbox admin**" to reduce risk /issues if one of them leaves!
7. Continue to click "**Add Member**" and repeat above for everyone you need accounts for. You can choose whether or not they are linked to the generic business account or have admin rights – we recommend they see the generic account if they have a need to do so!
8. **ONLY CLICK "Confirm and Finish"** when you have completed details for that site.
9. Once the registration request has been submitted, **an email will be sent to the individual email addresses supplied, advising of usernames and steps to take to activate accounts**.
10. Temporary **passwords will be sent via SMS** to the mobile number provided. Individuals will be required to change this when they log in.

Step 3 - Ongoing Support

- For businesses “self-management”, making amendments will be familiar to your IT department colleagues.
- For businesses using the National Administration Service (NAS), queries and issues should be raised with the helpdesk by emailing: careadmin@nhs.net

Note: There is currently an ongoing problem with data sets used by NHSmail to check your information held by the NHS and CQC.

It is likely that providers delivering care through multiple limited companies will find CQC and NHS data sets are not yet reflecting your structures.

Where this is the case, I recommend…

1) Establishing each home/site independently on NHSmail using the site code [V…]
2) If not already done so for your DSP toolkit submission, email Exeter Help desk with a clear list of “HQ” and linked “site” ODS codes, CQC IDs and addresses to request they are linked together. It helps if there is an overarching limited company (“parent”) accountable for the group of businesses (“children”)
3) Once Exeter Helpdesk have confirmed the structures, contact the NAS and request the same structure is reflected in the NHSmail directory

Useful links

Information	Link / Source
Care Provider Alliance templates / guidance	https://www.careprovideralliance.org.uk/data-security-and-protection-toolkit.html
ICO GDPR (Guidance)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
Key Roles & DPO Guide	www.dsptoolkit.nhs.uk/Help/2?AspxAutoDetectCookieSupport=1
DSP Toolkit (Guidance)	www.dsptoolkit.nhs.uk/Help?AspxAutoDetectCookieSupport=1
DSP Toolkit (Registration)	www.dsptoolkit.nhs.uk/Account/Register
DSP Toolkit (Login)	www.dsptoolkit.nhs.uk/Account/Login
NHSmail (Guidance)	https://portal.nhs.net/Help/joiningnhsmail
NHSmail (Registration)	https://portal.nhs.net/Registration#/careprovider
NHSmail (Login)	https://portal.nhs.net/
Information Commissioner's Office	www.ico.org.uk/
Cyber Essentials PLUS Certification	www.cyberessentials.ncsc.gov.uk/