Information Asset Register & Record of Processing Activities

Completing IAR & ROPA

This workbook provides the steps required to create an Information Asset Register (IAR) & a Record of Processing Activities (ROPA) for evidence item 1.1.2 in the DSPT.

It contains:

Overview

It is a requirement of the Data Protection Act (2018) and the General Data Protection Regulation (GDPR) that all personal and sensitive data has a legal basis for being held and being shared.

This means that care providers are legally obliged to keep a record of all the personal data they hold for staff, residents and families/carers, and what data they share with others.

To meet this requirement, it is easiest to have two lists:
1. Information Asset Register (IAR) – contains what type of information is held, where it is stored and how it is protected

2. Record of Processing Activities (ROPA) – contains where data is received from, where it is sent to and the legal basis for doing this

This workbook describes the steps to creating the records required for the IAR and the ROPA which are needed for evidence item 1.1.2 in the Data Security and Protection Toolkit

The process to generate the evidence for 1.1.2

1.4.1 **Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?**

These are the key stages:

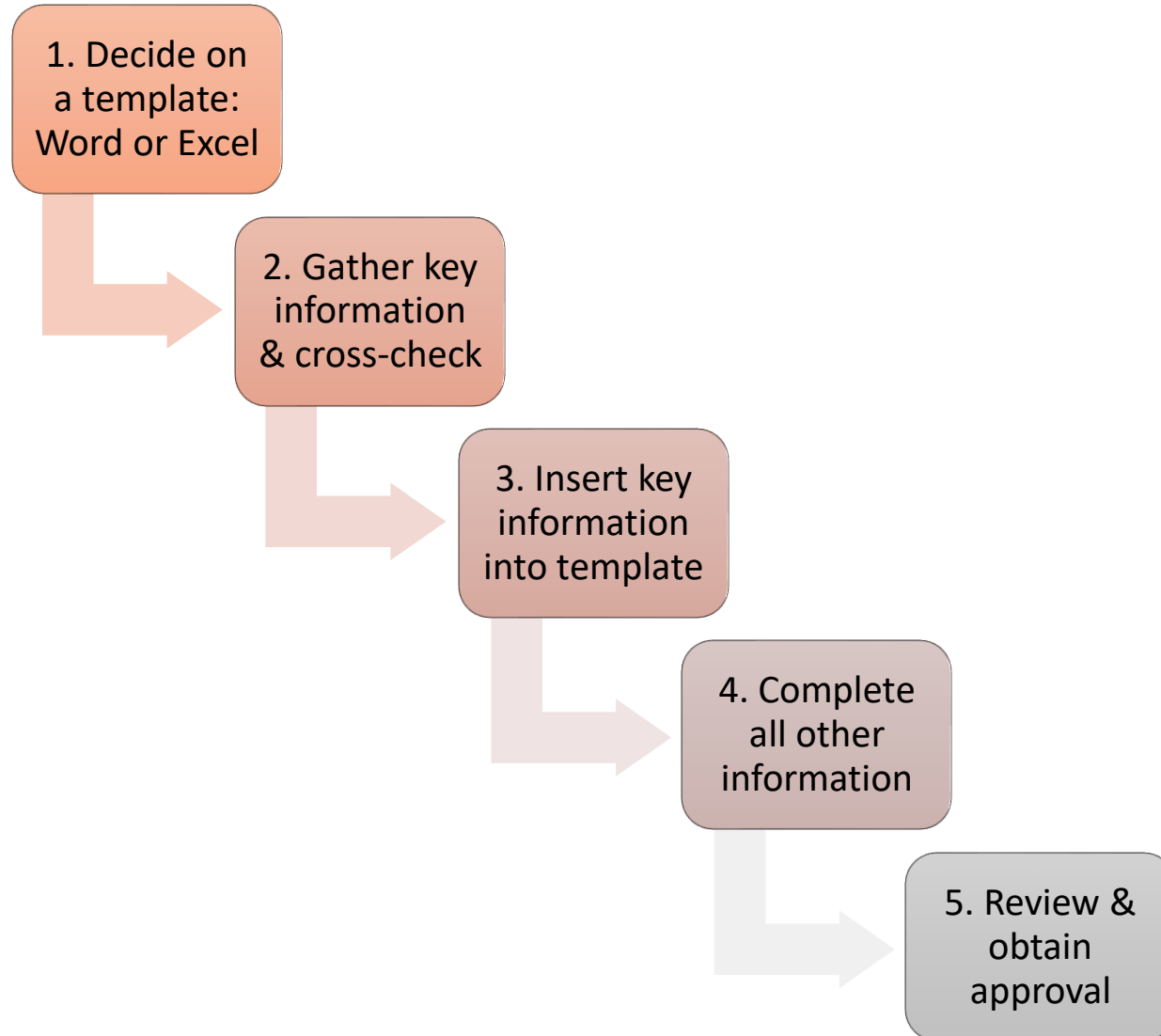Create IAR → Create ROPA → Get approval → Tick 1.1.2
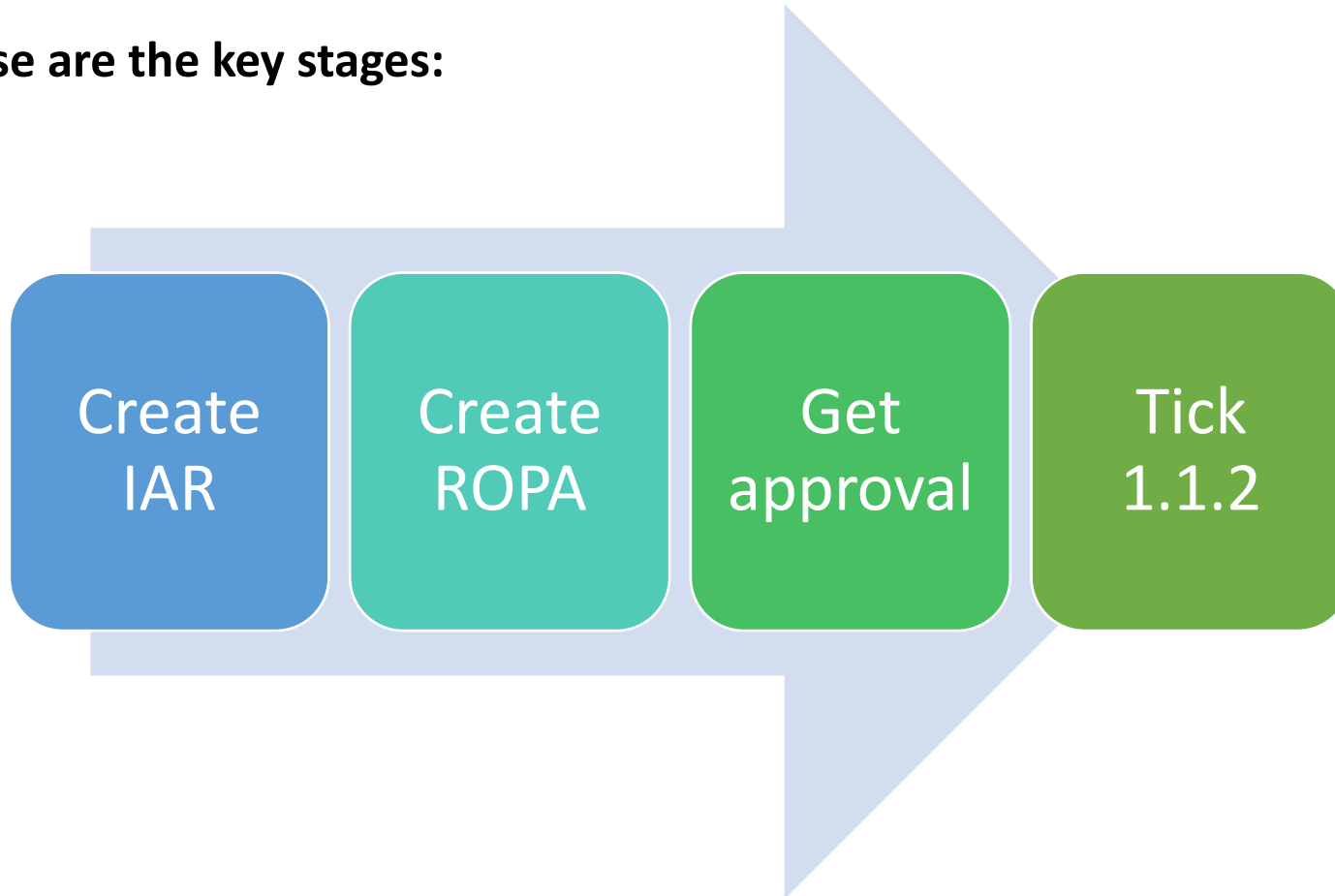
IAR = Information Asset Register   ROPA = Record Of Processing Activities

What is an Information Asset Register (IAR)?

An Information Asset Register is a list of all the places where information is stored, whether the information in that place is special category information, and how that information is kept safe

The process to generate the Information Asset Register (IAR)

1. Decide on a template: Word or Excel

2. Gather key information & cross-check

3. Insert key information into template

4. Complete all other information

5. Review & obtain approval

Step 1: Decide on a template

For **each** information asset, you must answer each question 1 to 15 in the table.
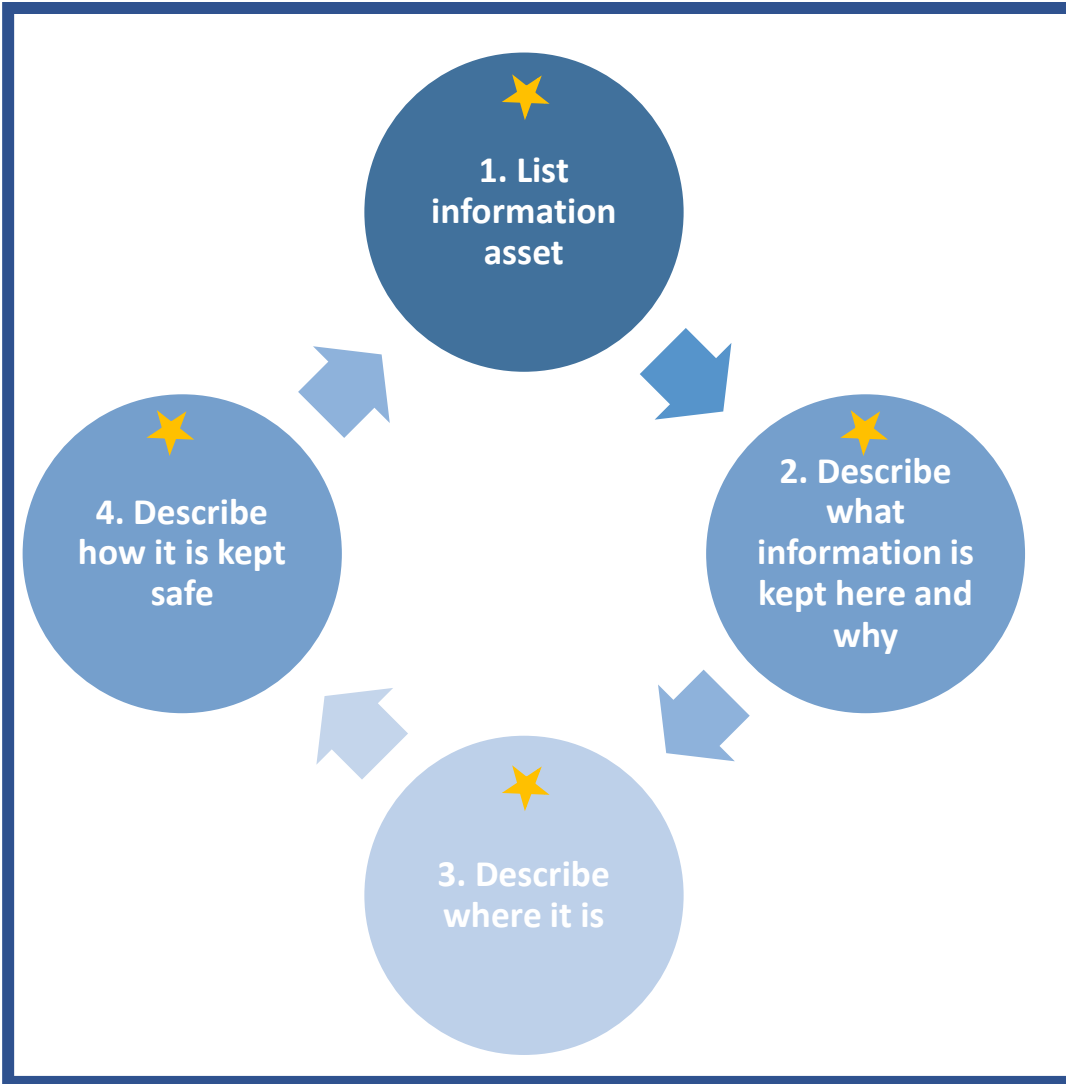
There are two templates available: in Word and in Excel.

They are available here: https://www.digitalcarehub.co.uk/resource/information-asset-register-template/ or from your local lead.

Review each type and decide which format works best for you.

The ⭐ information in the table is required for Step 2.

1. Information Asset Name ⭐
2a. Supplier Name
2b. Contract location
2c. Contract Start and End Dates
3. What Information is Kept Here and Why? ⭐
4. Location - Where is the Information Asset? ⭐
4. Does this contain special category data?
6. Who is the Information Asset Owner?
7. Is the Information Shared Externally? i.e. Do you receive it from someone outside your organisation or share it externally.
8. [Only if Yes to 7] is the Process Included on the Record of Processing Activities?
9. What Risks Are There if There is a Breach?
10. What Security Measures Have Been Put in Place? ⭐
11. Date Information Asset Issued (If applicable) [DD/MM/YY]
12. Date Information Asset Returned (If applicable) [DD/MM/YY]
13. Date of Last Audit [DD/MM/YY].
14. Has There Been a Breach Since the Last Audit? [Drop down list]
15. [Only if Yes to 14] Have All Actions Which Arose Because of the Breach been Taken?

Step 2a: Gather key information

- 1. List information asset
- 2. Describe what information is kept here and why
- 3. Describe where it is
- 4. Describe how it is kept safe

- Use the table on the next page to list each information asset and what is in there
- Keep carrying out the four steps until all the information assets are listed
- Walk around the building and offices to check all information assets are listed
- Use our checklist to make sure all personal information is allocated into an asset
- Then carry out a final check by reviewing all supplier contracts to see if they store any personal information

Use this table to note down key information for the IAR before completing a full IAR template

IAR

Key Questions in the Information Asset Register			
1. Information Asset Name	**3. What information is kept here and why?**	**4. Location - Where is the Information Asset?**	**10. What Security Measures Have Been Put in Place?**
Group information you hold in the same place. For example, staff information records file could hold all the personal information about staff. Consider all formats: paper, CD, electronic, tape, USB stick etc	Describe the type of information you keep in each information asset and why you keep the information.	Note down where you store the information asset: usually either a filing cabinet (locked!) or in a specific folder on your computer.	Outline the measures that you have put in place to minimise the risks of a data breach. This doesn't need to be too detailed.

Here's another table if you need more space

Key Questions in the Information Asset Register			
1. Information Asset Name	3. What information is kept here and why?	4. Location - Where is the Information Asset?	10. What Security Measures Have Been Put in Place?

Step 2b: Cross-check all information has been gathered

IAR

Here are examples of 'Information Assets' that could be holding personal information in your organisation.

Personal information can be held in/on things like:

- Cupboards
- Filing cabinets
- Devices
- Posters/Lists on walls
- CCTV footage
- Digital systems such as NHSmail, care planning system, eMAR and HR systems
- Offices
- Shelves

Review the list by ticking all the circles that are relevant. Check each one to see if personal information kept there is required.
Now return to the tables you've completed on the previous page/s and check that all the information you have ticked is in one or more of the information assets you have listed.

Care record filing system:
Paper ○
Computer ○
Smart phone ○
iPad ○

Posters/ lists of:
Residents' names ○
Rooms numbers ○
Birthdays ○

Devices:
Desk top computers ○
Laptops ○
Mobile phones ○
Tablets ○
Voicemail ○

Secure Email ○
NHSmail Shared mailbox ○

Employee finance records, pensions and bank details ○
Payroll systems ○

Prescriptions ○
MAR sheets ○
eMAR ○

Lists of:
Suppliers ○
Customers ○

Dietary requirements ○
Allergy lists ○

Employee rota
Employee HR information ○

Archived information ○

NHS Community Services records ○

CCTV video footage records ○

10

Step 3: Insert key information into the template

Now that you've collected the key information, you can insert it into the template

	Notes
1. Information Asset Name ⭐	Staff information records filing cabinet
2a. Supplier Name	
2b. Contract location	
2c. Contract Start and End Dates	
3. What Information is Kept Here and Why? ⭐	Staff records, including ID, sensitive information, recruitment documents, supervisions, appraisals, updated personal information, for evidence of compliance with recruitment guidance and for training and in case of emergencies.
4. Location - Where is the Information Asset? ⭐	In top floor locked storage room
4. Does this contain special category data?	
6. Who is the Information Asset Owner?	
7. Is the Information Shared Externally? i.e. Do you receive it from someone outside your organisation or share it externally.	
8. [Only if Yes to 7] is the Process Included on the Record of Processing Activities?	
9. What Risks Are There if There is a Breach?	
10. What Security Measures Have Been Put in Place? ⭐	The filing cabinet and storage room are both kept locked and can only be accessed by authorised individuals. All Information handling and record keeping procedures are followed.
11. Date Information Asset Issued (If applicable) [DD/MM/YY]	
12. Date Information Asset Returned (If applicable) [DD/MM/YY]	
13. Date of Last Audit [DD/MM/YY].	
14. Has There Been a Breach Since the Last Audit? [Drop down list]	
15. [Only if Yes to 14] Have All Actions Which Arose Because of the Breach been Taken?	

11

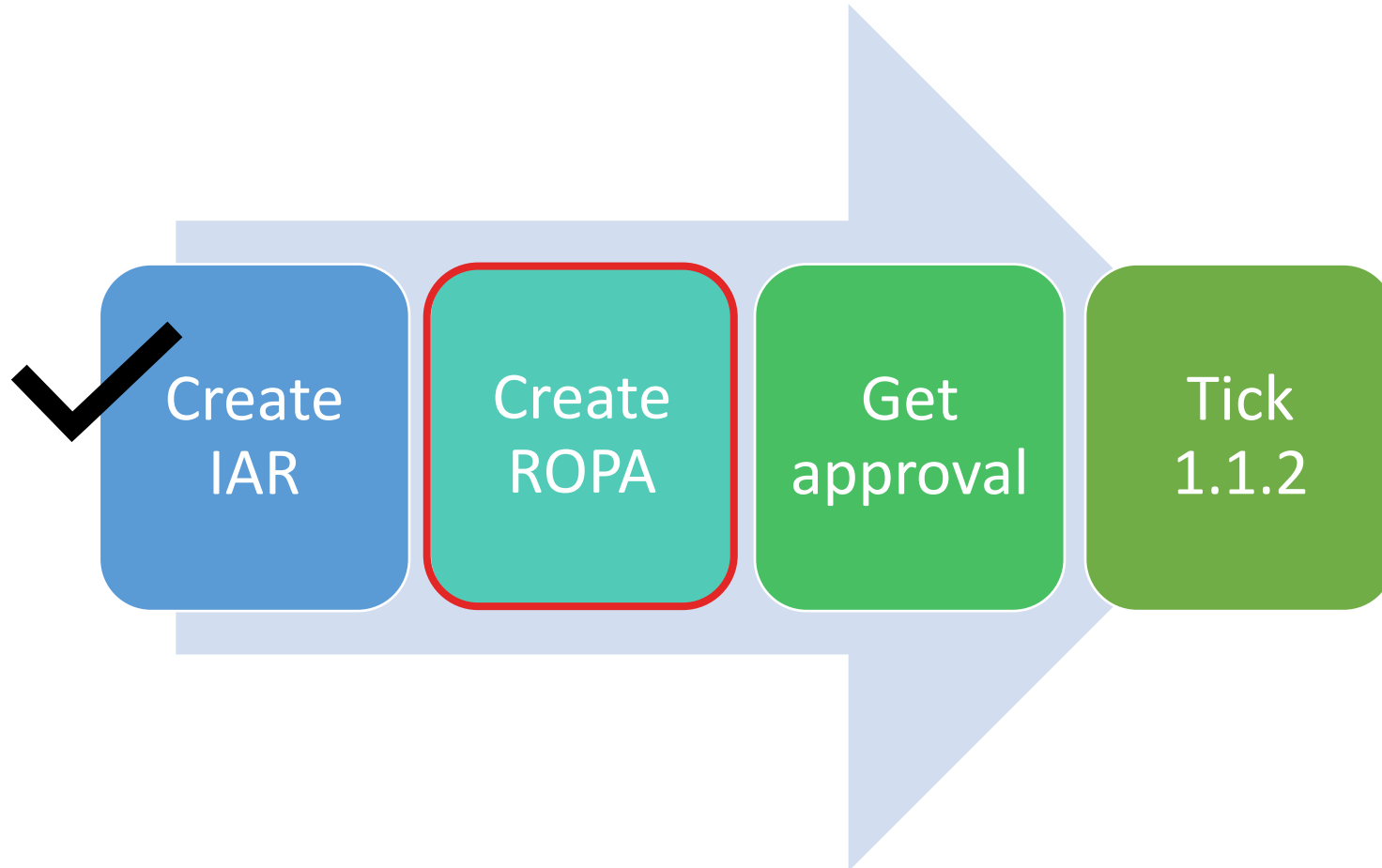# Step 4: Complete all other information in the template

IAR

Now you can complete the rest of the template. Your completed template should look like this:

	Notes
1. Information Asset Name	Staff information records filing cabinet
2a. Supplier Name	NA
2b. Contract location	NA
2c. Contract Start and End Dates	NA
3. What Information is Kept Here and Why?	Staff records, including ID, sensitive information, recruitment documents, supervisions, appraisals, updated personal information, for evidence of compliance with recruitment guidance and for training and in case of emergencies.
4. Location - Where is the Information Asset?	In top floor locked storage room
4. Does this contain special category data?	Yes
6. Who is the Information Asset Owner?	Home manager
7. Is the Information Shared Externally? i.e. Do you receive it from someone outside your organisation or share it externally.	Yes
8. [Only if Yes to 7] is the Process Included on the Record of Processing Activities?	Yes
9. What Risks Are There if There is a Breach?	Staff highly personal records would be seen. This could cause upset to staff, reputational damage to the company, and breach data protection legislation. The company could be fined or other penalties could be imposed.
10. What Security Measures Have Been Put in Place?	The filing cabinet and storage room are both kept locked and can only be accessed by authorised individuals. All Information handling and record keeping procedures are followed.
11. Date Information Asset Issued (If applicable) [DD/MM/YY]	NA
12. Date Information Asset Returned (If applicable) [DD/MM/YY]	NA
13. Date of Last Audit [DD/MM/YY].	01/04/2021
14. Has There Been a Breach Since the Last Audit? [Drop down list]	No
15. [Only if Yes to 14] Have All Actions Which Arose Because of the Breach been Taken?	NA

Step 5: Review the IAR and obtain approval

Review

IAR Completed

Obtain
Approval
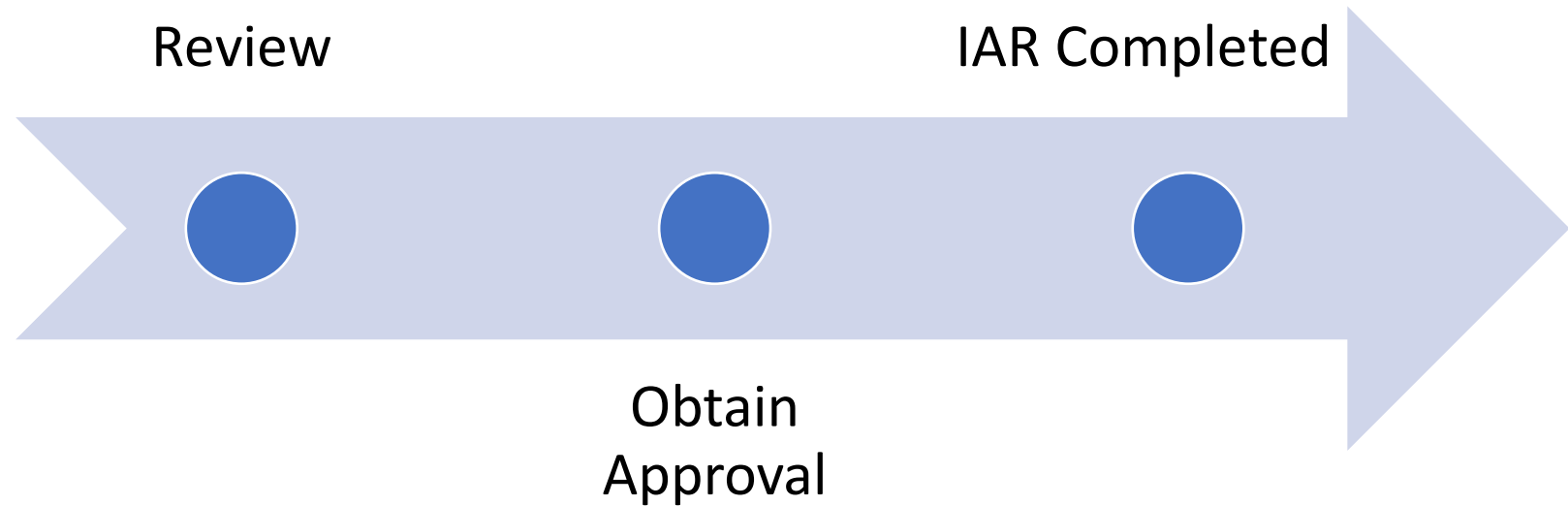
You are now half way to completing 1.1.2!

The process to generate the evidence for 1.1.2: ROPA Stage

IAR = Information Asset Register   **ROPA = Record Of Processing Activities**

What is a Record of Processing Activities (ROPA)?

A Record of Processing Activities (ROPA) is a list of confidential data, where it is received from or where it is sent to and the legal basis for doing this.
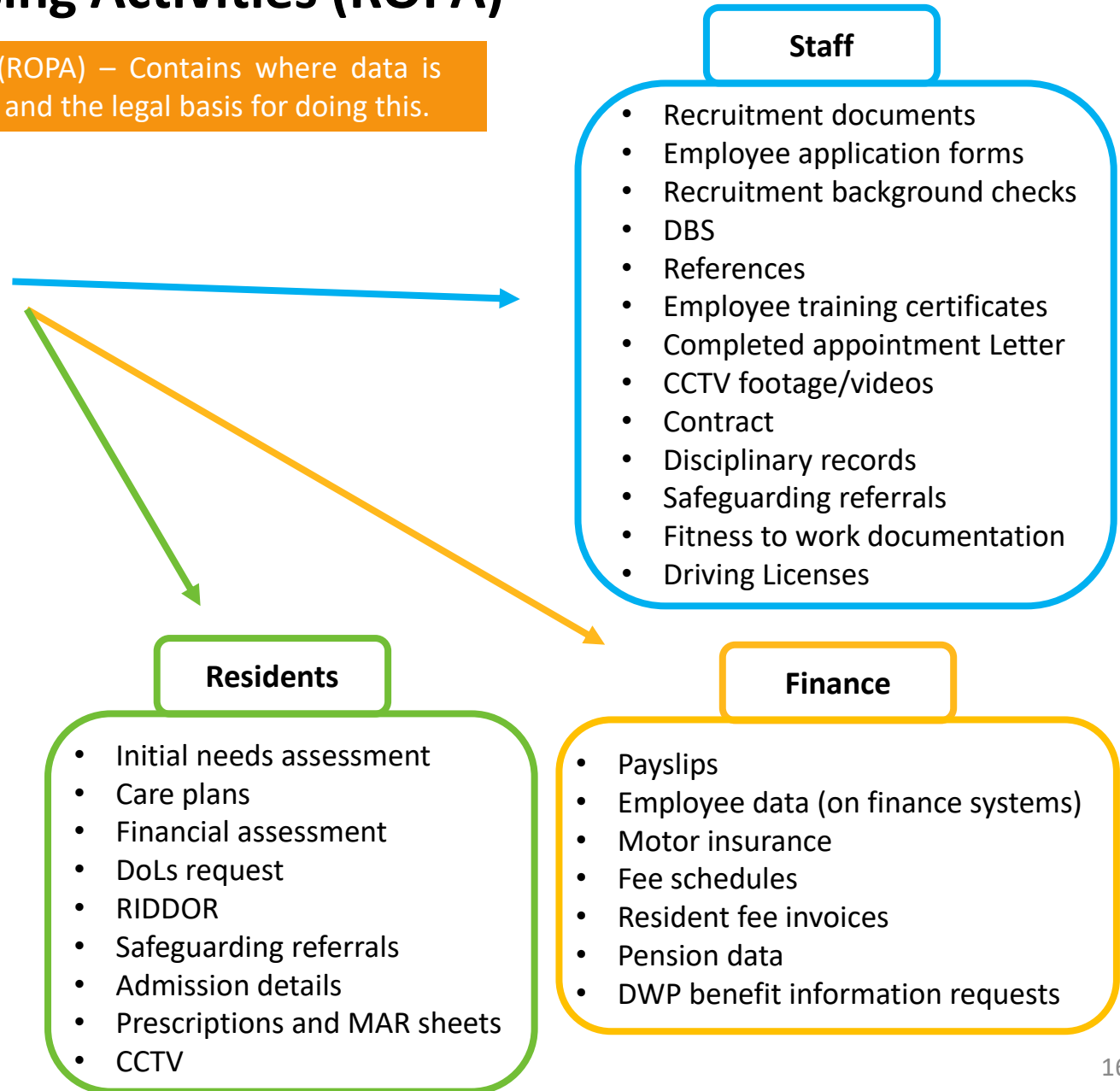
All data in the IAR marked as being received from or shared with external organisations needs to be included in your ROPA

Record Of Processing Activities (ROPA)

1.4.1

Record of Processing Activities (ROPA) – Contains where data is received from, where it is sent to and the legal basis for doing this.

These are examples of ROPA 'Data Items' in your care home

Data items in these lists can be grouped if they are used or shared in the same way, for example, initial needs assessment contains a lot of personal information about a potential resident and is used to accept or reject admission.

Staff

- Recruitment documents
- Employee application forms
- Recruitment background checks
- DBS
- References
- Employee training certificates
- Completed appointment Letter
- CCTV footage/videos
- Contract
- Disciplinary records
- Safeguarding referrals
- Fitness to work documentation
- Driving Licenses

Residents

- Initial needs assessment
- Care plans
- Financial assessment
- DoLs request
- RIDDOR
- Safeguarding referrals
- Admission details
- Prescriptions and MAR sheets
- CCTV

Finance

- Payslips
- Employee data (on finance systems)
- Motor insurance
- Fee schedules
- Resident fee invoices
- Pension data
- DWP benefit information requests

What you need to know before you start

Some data items are transferred in and transferred out, such as, prescriptions and MAR sheets, and therefore will need to be listed separately.

All data which is physically transferred – either electronically or in hardcopy - must be added to your ROPA. This could include: Computers, Tablets, Smart Phones, CDs, DVDs, Tapes, Answering Machines, (Digital) Photographs, Letters, Documents, Printouts, Notepads, Diaries etc.
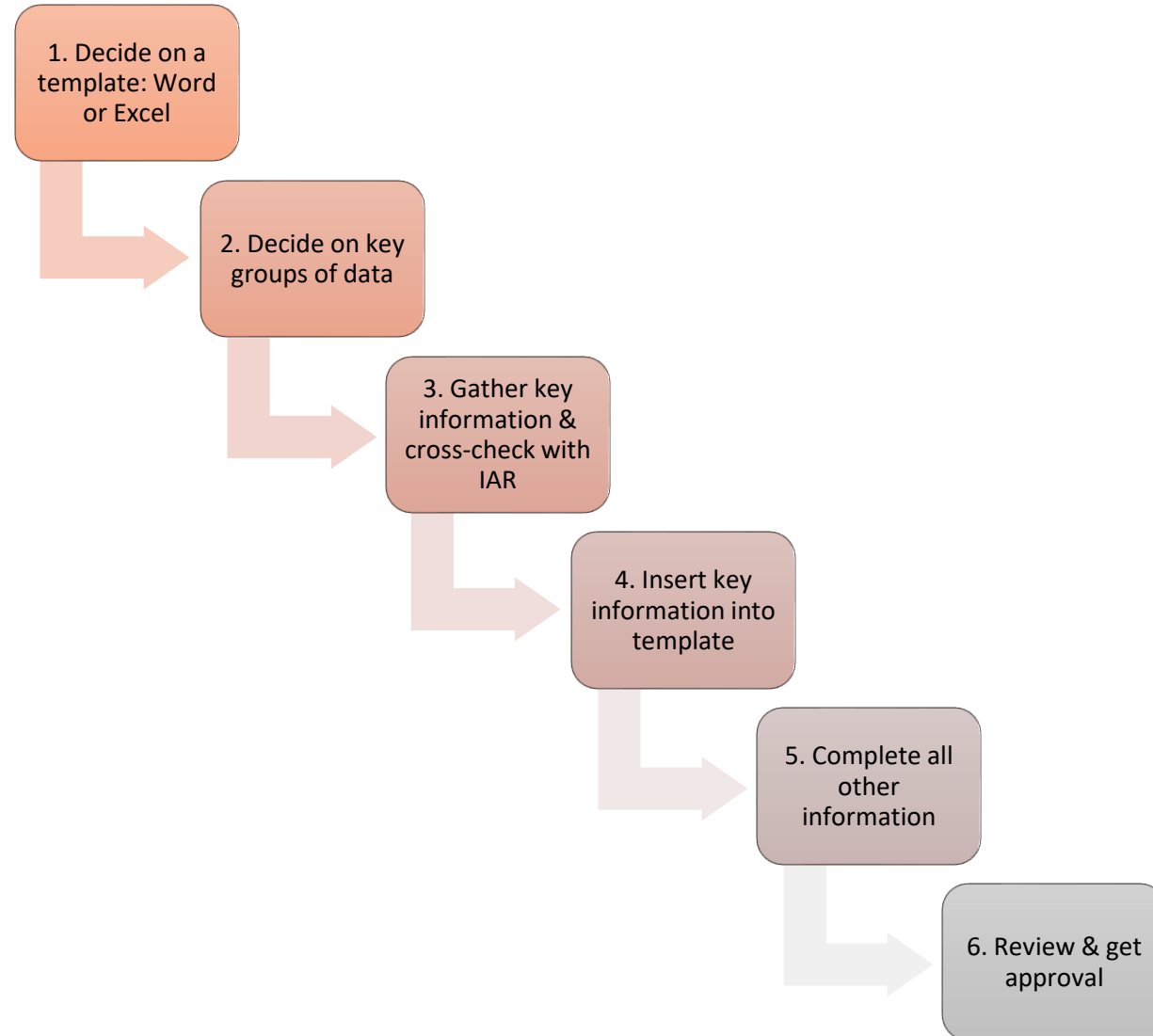
You do not have to record information shared through face to face discussions or telephone calls but if notes are made then this information may need to form part of your records.

If you have fewer than 250 employees, then you do not have to record all of the personal data which you process. You only need to record processing which
1. is not occasional i.e. you don't need to record a one-off exchange; or
2. is likely to result in a risk to the rights and freedoms of individuals; or
3. contains special category or criminal convictions data.

If you have 250 or more employees, you need to record all processing activities even if they only happen once or are unexpected.

Data must not be about an individual (i.e. Ms Smith's Initial Needs Assessment) but on a higher level (i.e. Initial Needs Assessments generally).

The process to generate the ROPA

1. Decide on a template: Word or Excel

2. Decide on key groups of data

3. Gather key information & cross-check with IAR

4. Insert key information into template

5. Complete all other information

6. Review & get approval

Step 1: Decide on a template

ROPA

For **each** data item, you must answer each question 1 to 20 in the table.

There are two templates available: in Word and in Excel.

They are available here: https://www.digitalcarehub.co.uk/resource/information-asset-register-template/ or from your local lead.

Review each type and decide which format works best for you.

The ⭐ information in the table is required for Step 2.

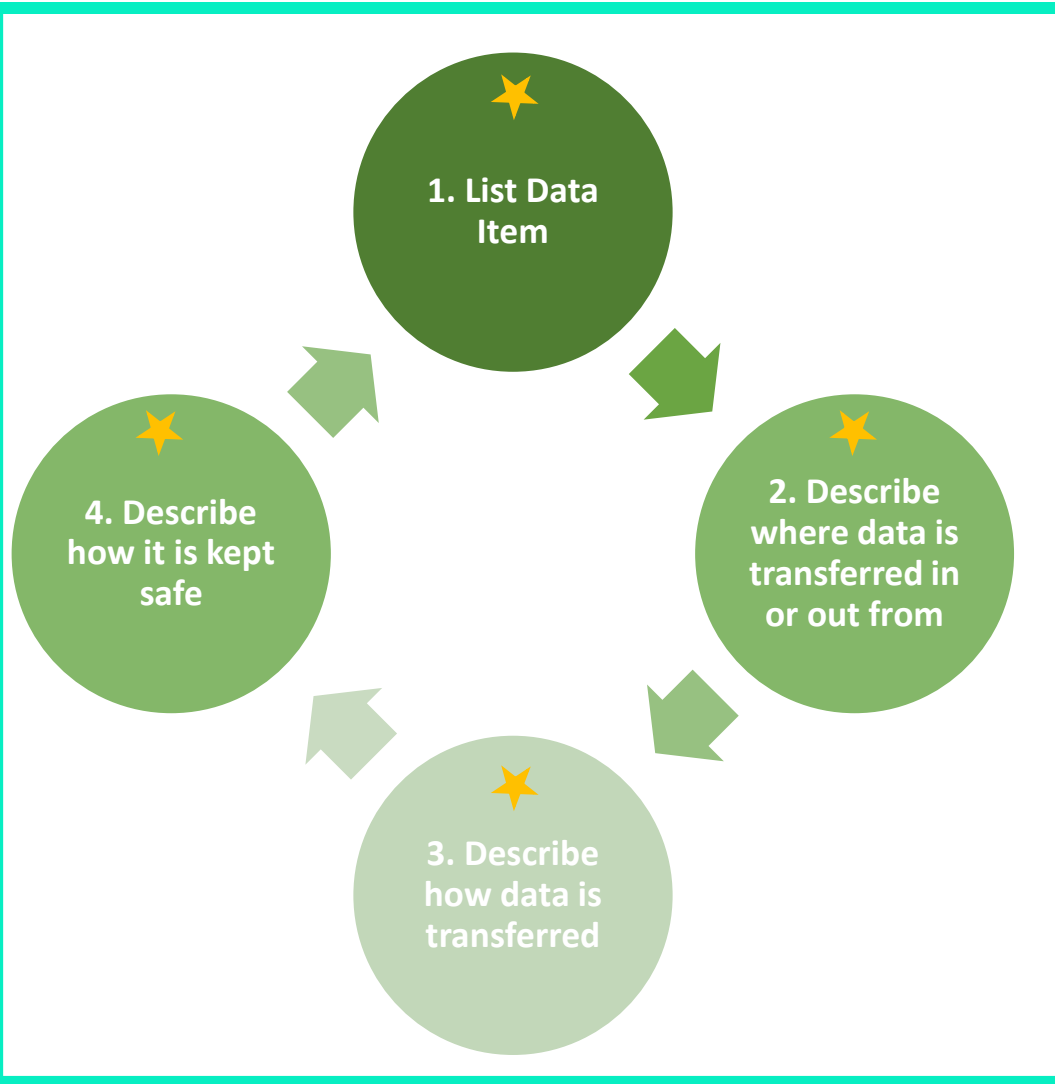| |
|---|
| 1. Data Item ⭐ |
| 2. Personal Data Category |
| 3. Data Subject |
| 4. Data Format |
| 5. Is the information being transferred into or out of the organisation? |
| 6. Where is the data received from (in) or transferred to (out)? ⭐ |
| 7. Is the data transferred outside of the EEA? |
| 8. (Only if YES for 7) Detail measures taken to protect data. |
| 9. How is the data transferred into or out of the organisation? ⭐ |
| 10. Description of why the data is being processed. |
| 11. Lawful Basis for Processing (Article 6 Provision) |
| 12. Is the Data Special Category? (|
| 13. Legal Basis for Processing Special Category (Article 9) or Criminal Records Data (DPA 2018) |
| 14. Link to/Location of Consent Form (only if consent is the legal basis for sharing) |
| 15. What Procedure(s) Has Been Put in Place to Ensure Data Security? ⭐ |
| 16. How Long is the Data Retained For? |
| 17. Date of Last Review of Processing Activity (at least annually) |
| 17a. Date of Last Change to Legal Basis for Processing |
| 18. Who is responsible for the data item [Information Asset Owner]? |
| 19. Has a Data Protection Impact Assessment been completed? |
| 20. Is this an active or inactive process? (mark as inactive if the data process is no longer happening) |

Create ROPA

ROPA

✓/x

This is a checklist of groups of data items that are generally processed in the same way.

Tick all items that are relevant to your organisation.

Review your organisation's IAR to check for other data.

Take a moment to think about other data processed by your organisation. Ask finance for what data external organisations process data on your organisation's behalf.

	✓/x
Initial needs assessments	
Payslips	
Care plan information **(OUT)**	
Care plan information **(IN)**	
Employee data	
Deprivation of Liberty Request	
Prescription & MAR Sheets **(OUT)**	
Prescriptions & MAR Sheets **(IN)**	
Staff Information Records, e.g references, recruitment docs, DBS	
Medical Discharge Summaries/letters; appointment letters; professional correspondence.	
Other	
Other	

20

Step 3: Gather key information

- **1. List Data Item**
- **2. Describe where data is transferred in or out from**
- **3. Describe how data is transferred**
- **4. Describe how it is kept safe**

- Use the table on the next page to list each data item you have identified
- Keep carrying out these four steps until all the data items are listed
- Review the IAR to check all data is listed
- Then carry out a final check by reviewing all supplier contracts to see if they store any personal information

Use this table to note down key information for the ROPA before completing a full template

ROPA

For the each of the relevant data items which you have previously ticked, complete the questions in the table…

| Record of Processing Activities Key Questions			
1. Data Item	**6. Where is the data received from (in) or transferred to (out)?**	**9. How is the data transferred into or out of the organisation?**	**15. What procedure(s) has been put in place to ensure data security?**
	Examples of item 6: ➢ Hospital/ Hospital Staff ➢ GP ➢ Social Workers ➢ CQC staff ➢ Safeguarding Leads ➢ Families ➢ Other care homes ➢ Local Authority ➢ DoLs ➢ Community Pharmacy ➢ DBS ➢ HR ➢ NMDS-SC ➢ Employees	**Examples of item 9:** ➢ Email ➢ Post ➢ By hand ➢ Uploading to a server or cloud program etc.	**Examples of item 15:** ➢ Passwords have been changed and there is a secure system in place for updating passwords. ➢ Anything that is conducted online should be done using a secure login or portal. ➢ There should be contractual terms that ensure data is only shared securely. ➢ Staff to be given guidance on how to send or receive the data securely.

Record of Processing Activities Key Questions			
1. Data Item	6. Where is the data received from (in) or transferred to (out)?	9. How is the data transferred into or out of the organisation?	15. What procedure(s) has been put in place to ensure data security?

Step 4: Insert key information into the template

Now that you've collected the key information, you can insert it into the template

|	Notes
1. Data Item	Initial Needs Assessments
2. Personal Data Category	
3. Data Subject	
4. Data Format	
5. Is the information being transferred into or out of the organisation?	
6. Where is the data received from (in) or transferred to (out)?	Hospital
7. Is the data transferred outside of the EEA?	
8. (Only if YES for 7) Detail measures taken to protect data.	
9. How is the data transferred into or out of the organisation?	By secure email
10. Description of why the data is being processed.	
11. Lawful Basis for Processing (Article 6 Provision)	
12. Is the Data Special Category? (	
13. Legal Basis for Processing Special Category (Article 9) or Criminal Records Data (DPA 2018)	
14. Link to/Location of Consent Form (only if consent is the legal basis for sharing)	
15. What Procedure(s) Has Been Put in Place to Ensure Data Security?	Information is only shared with people on a need to know basis with consent from the resident or their POA. Information handling procedures are followed.
16. How Long is the Data Retained For?	
17. Date of Last Review of Processing Activity (at least annually)	
17a. Date of Last Change to Legal Basis for Processing	
18. Who is responsible for the data item [Information Asset Owner]?	
19. Has a Data Protection Impact Assessment been completed?	
20. Is this an active or inactive process? (mark as inactive if the data process is no longer happening)	

Now you can complete the rest of the template. Your completed template should look like this:

	Notes
1. Data Item	Initial Needs Assessments
2. Personal Data Category	Health & Care
3. Data Subject	Resident
4. Data Format	Paper
5. Is the information being transferred into or out of the organisation?	In
6. Where is the data received from (in) or transferred to (out)?	Hospital
7. Is the data transferred outside of the EEA?	No
8. (Only if YES for 7) Detail measures taken to protect data.	N/A
9. How is the data transferred into or out of the organisation?	By secure email
10. Description of why the data is being processed.	To accept or refuse admission.
11. Lawful Basis for Processing (Article 6 Provision)	Legal Obligation
12. Is the Data Special Category? (	Yes
13. Legal Basis for Processing Special Category (Article 9) or Criminal Records Data (DPA 2018)	Provision of Health & Social Care
14. Link to/Location of Consent Form (only if consent is the legal basis for sharing)	N/A
15. What Procedure(s) Has Been Put in Place to Ensure Data Security?	Information is only shared with people on a need to know basis with consent from the resident or their POA. Information handling procedures are followed.
16. How Long is the Data Retained For?	8 years
17. Date of Last Review of Processing Activity (at least annually)	
17a. Date of Last Change to Legal Basis for Processing	n/a
18. Who is responsible for the data item [Information Asset Owner]?	Group Manager
19. Has a Data Protection Impact Assessment been completed?	No
20. Is this an active or inactive process? (mark as inactive if the data process is no longer happening)	Active

Step 6: Review the ROPA and obtain approval
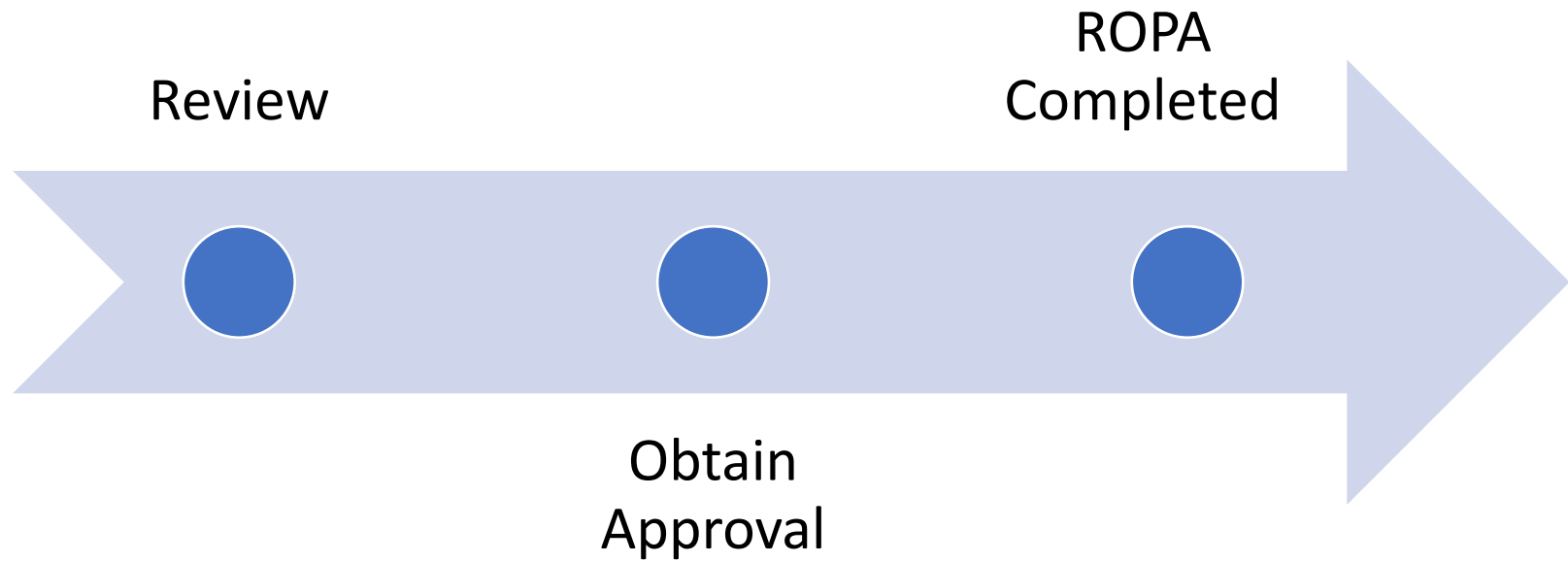
You are now nearly there to completing 1.1.2!
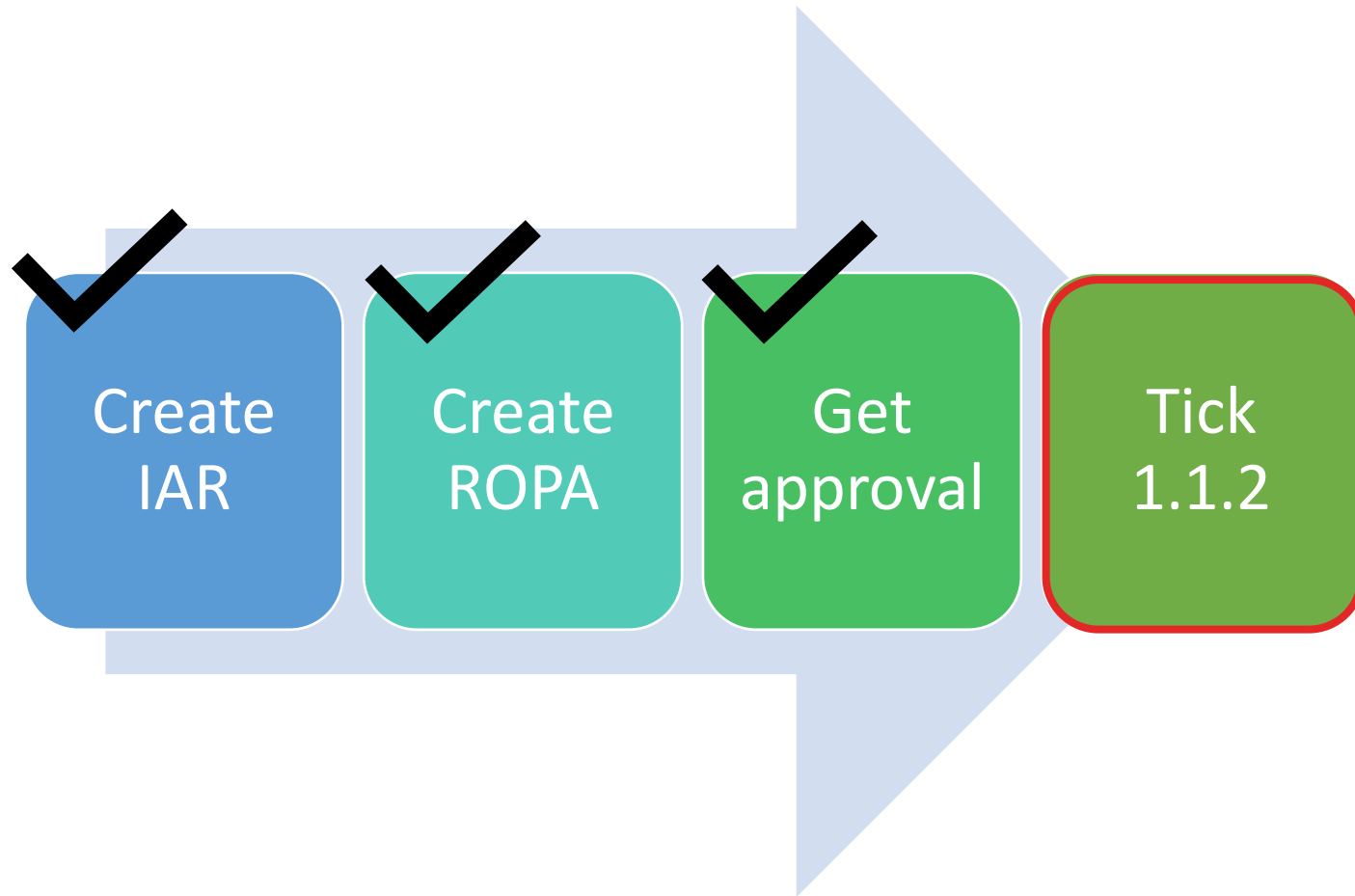
To complete this evidence item:

1. Choose the option that is most suitable:
   - Upload a document
   - Reference an existing uploaded document
   - Specify an intranet or internet link to a document
   - Enter text describing the document's location
2. Follow the instructions for that option. It is easiest to use the last option and state where the documents are, for example, in the DSPT folder on the manager's computer.
3. No information is required in the optional comments box
4. Click on the blue 'save' button

Evidence item 1.1.2

Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists.

The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved.

Example IARs and ROPAs are available from Digital Social Care.

	test	Remove	Edit

- Upload a document
- Reference an existing uploaded document
- Specify an intranet or internet link to a document
- Enter text describing the document's location

Comments (optional)

Save or Cancel

Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

IAR & ROPA

Overview: Care providers are legally obliged to keep a record of all personal and sensitive information they hold for staff and residents and how they share it.

Detail

To be compliant with data protection legislation your organisation must describe how it:

- holds personal and sensitive information
- shares personal and sensitive information with others

Examples of ways that information is 'held' are: filing cabinet, care planning system, laptop, allergy folder and medications trolley. The list that contains 'held' information is called an Information Asset Register (IAR).

Examples of the data that is shared with others are: needs assessments, prescriptions, payslips and care plans. The list that contains shared data is called a Record of Processing Activities (ROPA).

To record all the data, your organisation needs:

1. Information Asset Register (IAR) – contains what type of information is held, where and how it is stored and how it is kept safe
2. Record of Processing Activities (ROPA) – contains where data is received from, where it is sent to, the legal basis for doing this and how it is kept safe

Support

- Example IARs and ROPAs are available here: https://www.digitalcarehub.co.uk/data-security-protecting-my-information/how-to-document-your-data-processing/
- Senior leadership is required for this evidence item
- There is a separate workbook on the steps required to create the IAR and ROPA available

Evidence item 1.1.2

Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists.

The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved.

Example IARs and ROPAs are available from Digital Social Care.

📛	test		Remove	Edit

- Upload a document
- Reference an existing uploaded document
- Specify an intranet or internet link to a document
- Enter text describing the document's location

Comments (optional)

[   ]

Save   or Cancel

To complete this evidence item:

1. Choose the option that is most suitable:
   - Upload a document
   - Reference an existing uploaded document
   - Specify an intranet or internet link to a document
   - Enter text describing the document's location
2. Follow the instructions for that option. It is easiest to use the last option and state where the documents are, for example, in the DSPT folder on the manager's computer.
3. No information is required in the optional comments box
4. Click on the blue 'save' button