National Office of Clinical Audit

Clinical Audit through the lens of GDPR

GPDR & CLINICAL AUDIT

NOCA National Office of Clinical Audit

GDPR & Clinical Audit

NOCA National Office of Clinical Audit

Purpose of Today

High level view of the GDPR

What organizations have to do

Keep records of all processing of personal information

Institute safeguards for cross-border data transfers

Maintain appropriate data security

Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities

Get a parent's consent to collect data for children under 16

Consult with regulators before certain processing activities

Provide appropriate data protection training to personnel having permanent or regular access to personal data

Conduct Data Protection Impact Assessments on new processing activities

Implement Data Protection-by-Design *(Privacy "baked-in")*

Take responsibility for the security and processing activities of third-party vendors

Appoint a Data Protection Officer (if you regularly process lots of data, or particularly sensitive data)

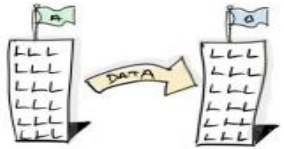
Be able to demonstrate compliance on demand

Notify data protection agencies and affected individuals of data breaches in certain circumstances

What individuals can do

Withdraw consent for processing

Request a copy of all of their data & request corrections if wrong



Request the ability to move their data to a different organization

Request that their information is deleted when there's no purpose to retain it

Object to automated decision-making processes, including profiling

What regulators can do

Ask for records of processing activities and proof of steps taken to comply with the GDPR

Impose temporary data processing bans, require data breach notification, or order erasure of personal data

Suspend cross-border data flows

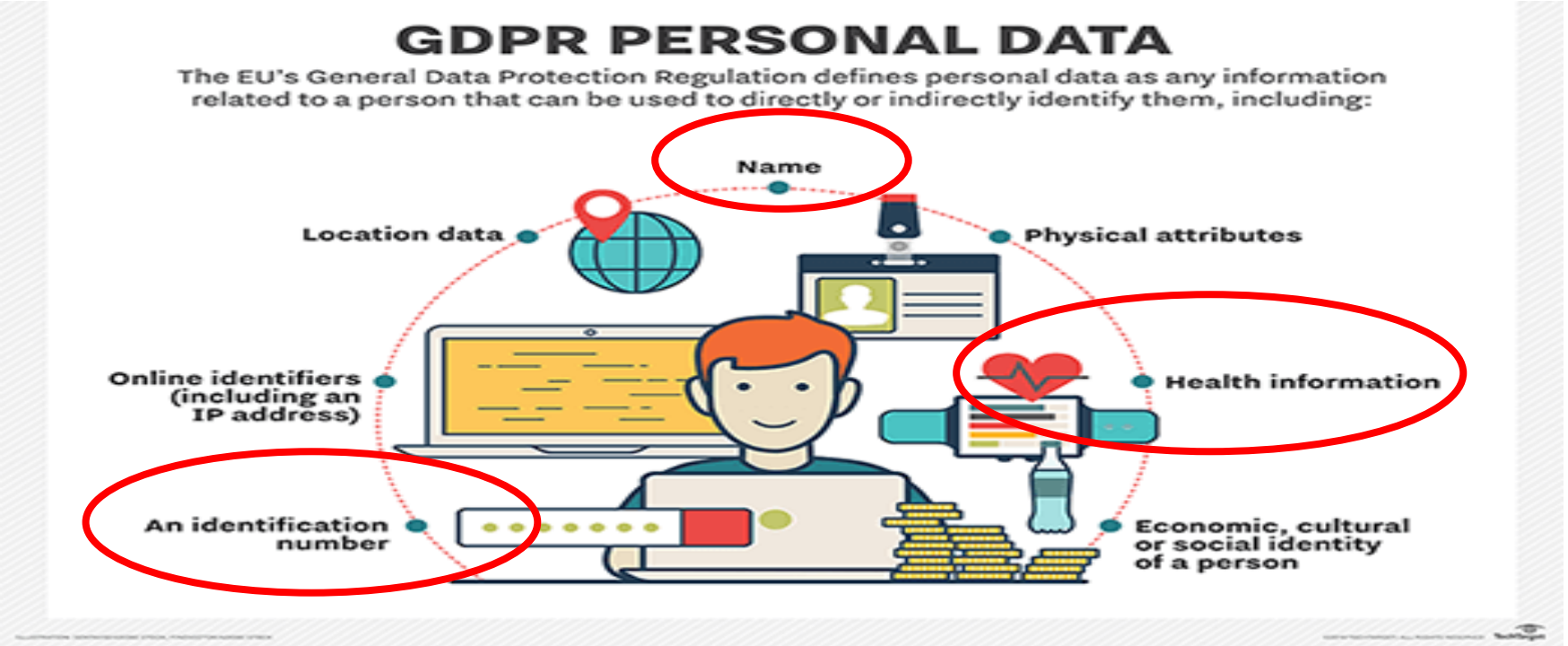
Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance

Inspired by IAPP's GDPR Awareness Guide. Please credit Tim Clements

***Source**: :* https://cfproventures.com/wp-content/uploads/2018/04/IAPP-Graphic-overview-of-GDPR.pdf
Credit: Tim Clements & IAPP *Accessed on 29/10/2019*

National Office of Clinical Audit

PERSONAL DATA



Source: *https://www.pinterest.ie/pin/721913015243394038/?lp=true* *Accessed on 29/10/2019*

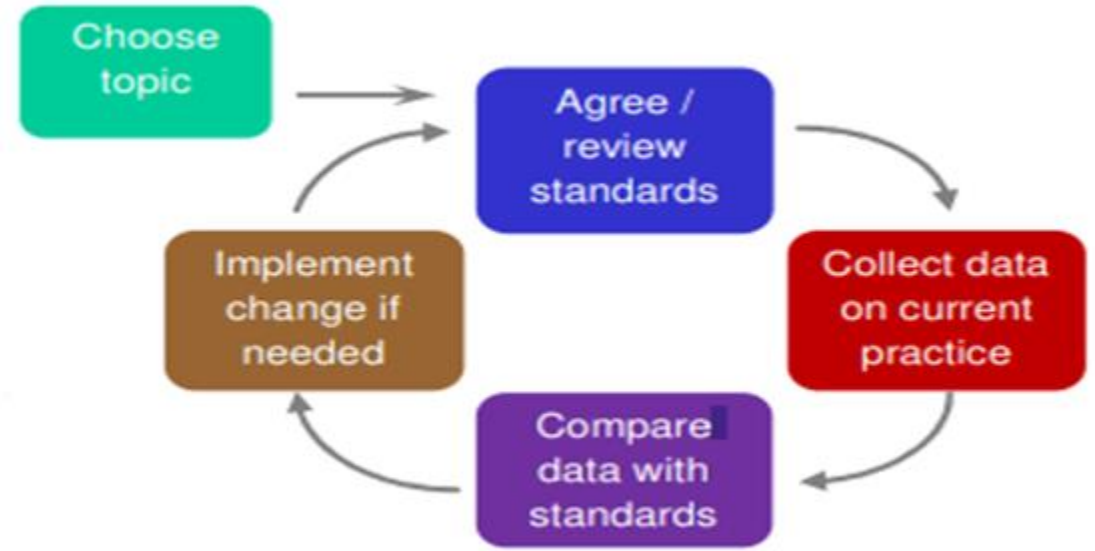
NOCA National Office of Clinical Audit

Who's who under GDPR

Source: https://cfproventures.com/gdpr-in-60-seconds *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

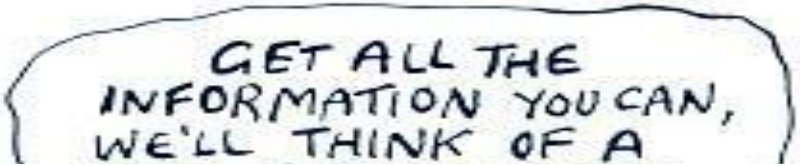
AUDIT PROCESS



Source: http://www.uhbristol.nhs.uk/files/nhs-ubht/1%20What%20is%20Clinical%20Audit%20v3.pdf *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

Planning



Always consider the data protection rights of the individual.

Source: https://i.pinimg.com/236x/23/1c/a5/231ca5733679cf9faec1cdaaea2f5226.jpg *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

CLINICAL AUDIT – MAPPED TO 7 GDPR PRINCIPLES

1. Inform Data Subjects how their data will be used especially when not relying on consent as lawful basis e.g. **Privacy Notices, Information Leaflets, Posters**
2. Only collect what is needed to meet the audit standards, data collection form.
3. Retain only the relevant data, anonymise/ pseudonymise where possible.
4. Check data quality, correct inaccuracies.
5. Only retain the personal data for as long as necessary
6. Keep the data secure and confidential. Important to watch out for small numbers
7. Good record keeping, listing all data usage activities. Report any breaches.

***Source**: https://blog.ipswitch.com/gdpr-eu-personal-data Accessed on 29/10/2019, Modified Image*

NOCA National Office of Clinical Audit

PRIVACY BY DESIGN & DEFAULT

Source: https://relentlessdataprivacy.com/top-ten-gdpr-principles-no-3-privacy-by-design-and-by-default/ *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

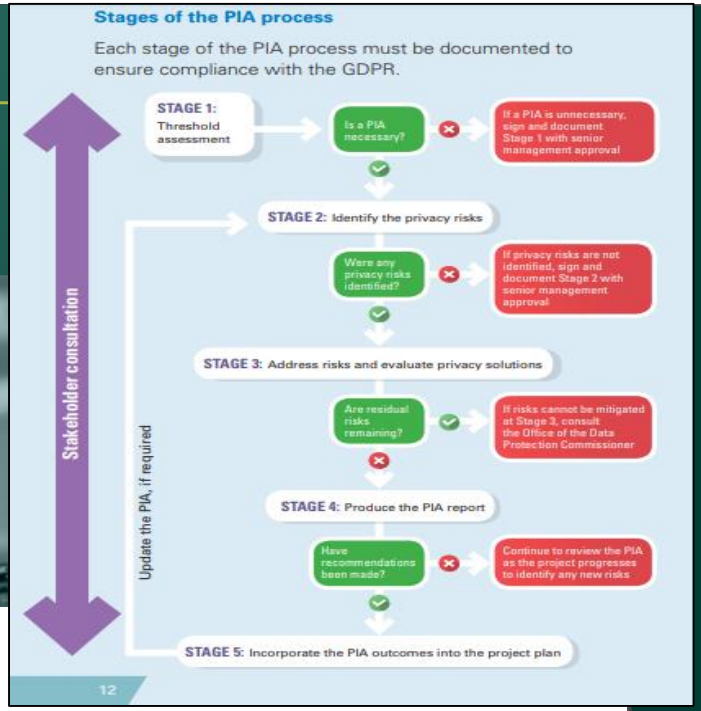
GDPR Aspects

Planning & Design	Implementation	Data Collection	Analysis & Review	Publishing findings
Data Protection Impact Assessment (DPIA) Select lawful basis Data Minimization	Data security Data sharing agreements Secure Storage Transparency HIQA Information standards	GDPR training for data collectors Pseudonymising the data Proportional processing Good record keeping	Data Quality – requirement under GDPR for data accuracy HIQA Data Quality Standards	Privacy of individuals Aggregated data - no individual identified Small numbers considered

NOCA National Office of Clinical Audit

DATA PROTECTION IMPACT ASSESSMENT

List of Types of Data Processing Operations which require a **Data Protection Impact Assessment.**

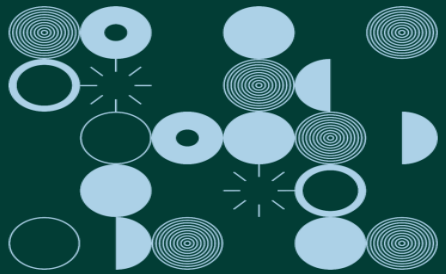


An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Guide to Data Protection Impact Assessments (DPIAs)

October 2019



Source: https://www.dataprotection.ie & http://www.higa.ie *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

DATA PROTECTION IMPACT ASSESSMENT

When do you carry out a DPIA?

- ❑ Any new IT system or new use of data resulting in high risk processing

  Or
- ❑ Any major change to an existing IT system or use of data

How do you know if a DPIA required?

- ❑ Complete the Threshold Assessment available from HIQA's website
- ❑ https://www.hiqa.ie/sites/default/files/2019-02/pia_threshold_assessment_0.pdf

NOCA National Office of Clinical Audit

BENEFITS OF DATA PROTECTION IMPACT ASSESSMENT

- Protecting the privacy rights of individuals
- Demonstrating compliance with legislation
- Building in privacy by design from the start
- Involving stakeholders, learning from experience
- Reducing risks to data subject's data

NOCA National Office of Clinical Audit

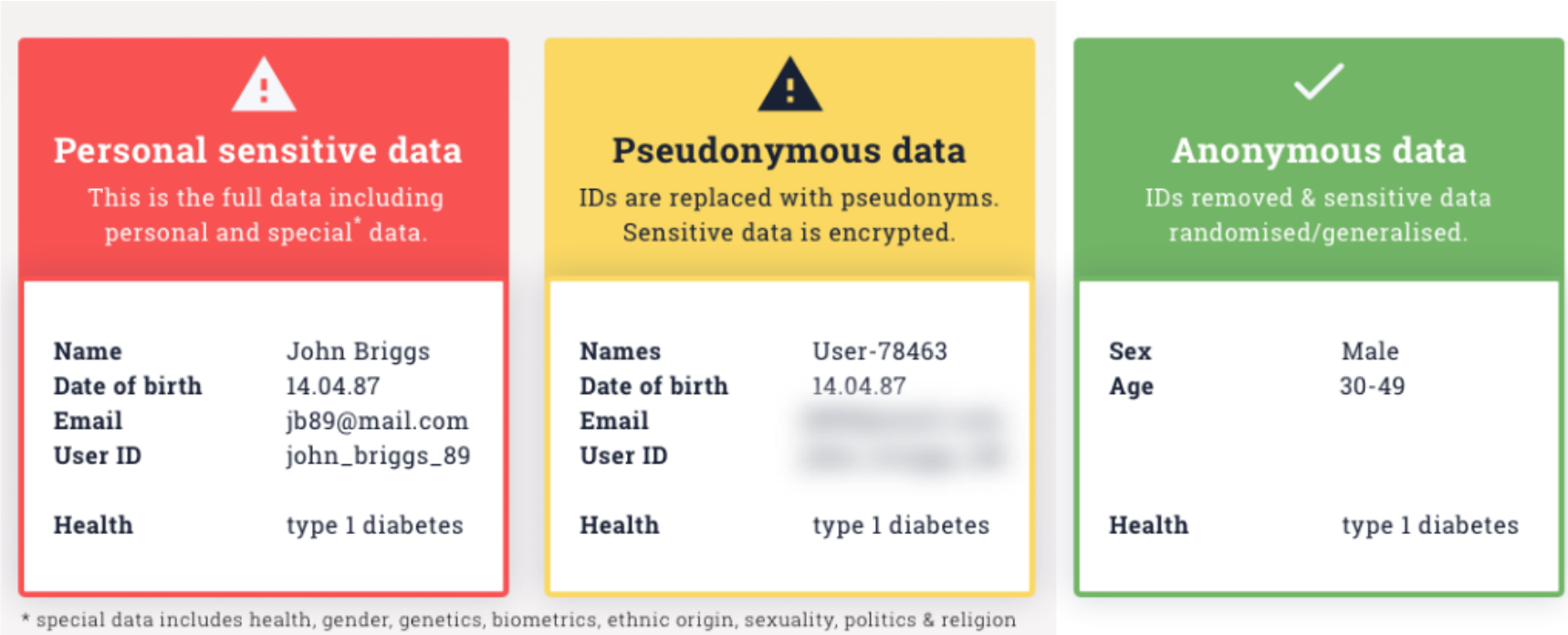
DATA MINISATION

- Only collect what you need to meet the Audit Standards – use a data collection form
- Pseudonymise or Anonymise where possible

Source: https://www.anonos.com/pseudonymisation-faq *Accessed on 29/10/2019*

NOCA National Office of Clinical Audit

DATA MINISATION



Source: https://www.chino.io/compliance/gdpr-hipaa-pseudonymization Accessed on 03/11/2019

NOCA National Office of Clinical Audit

DATA MINISATION - **Pseudonymisation techniques**

- Encryption
- Masking
- Scrambling
- Hashing
- Tokenization
- Data blurring

NOCA National Office of Clinical Audit

DATA MINISATION - **Pseudonymisation techniques**

Original Data

- Date of Birth – 02/11/1940
- Address, High St, Bray, Wicklow
- MRN– 876998
- Date of Surgery – 01/01/2018
- Height, Weight and BMI

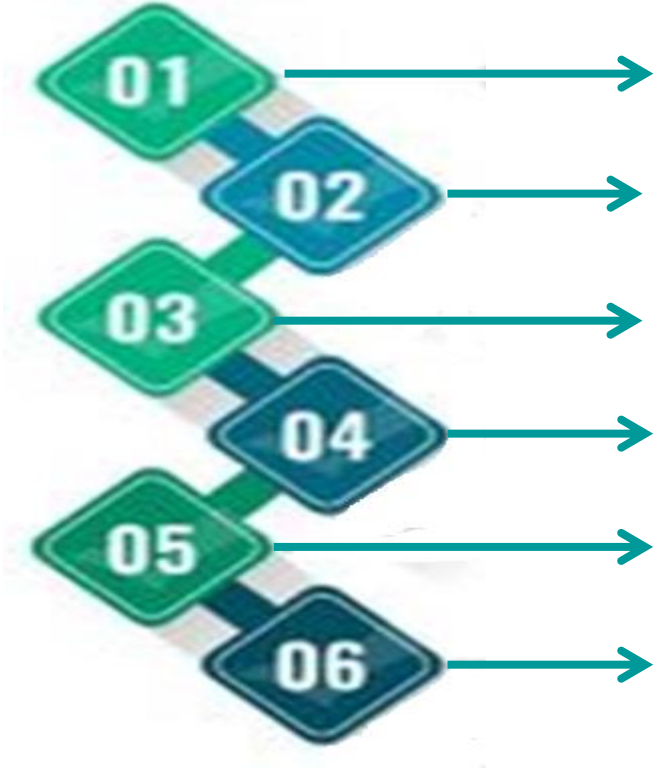
Pseudonymised Data

- Age or Age Range e.g. 79 or 70-79
- Use county or province e.g. Wicklow or Leinster
- Scramble Digits – xxx9xx8
- Use partial – Jan 2018 or Q1 2018
- Keep relevant data only - BMI

Use carefully and always review: *even using partial data, it may be possible to re-identify patient e.g. Date of Surgery – Jan 2018, they may have been only patient operated on in Jan 2018*

NOCA National Office of Clinical Audit

Data Collection

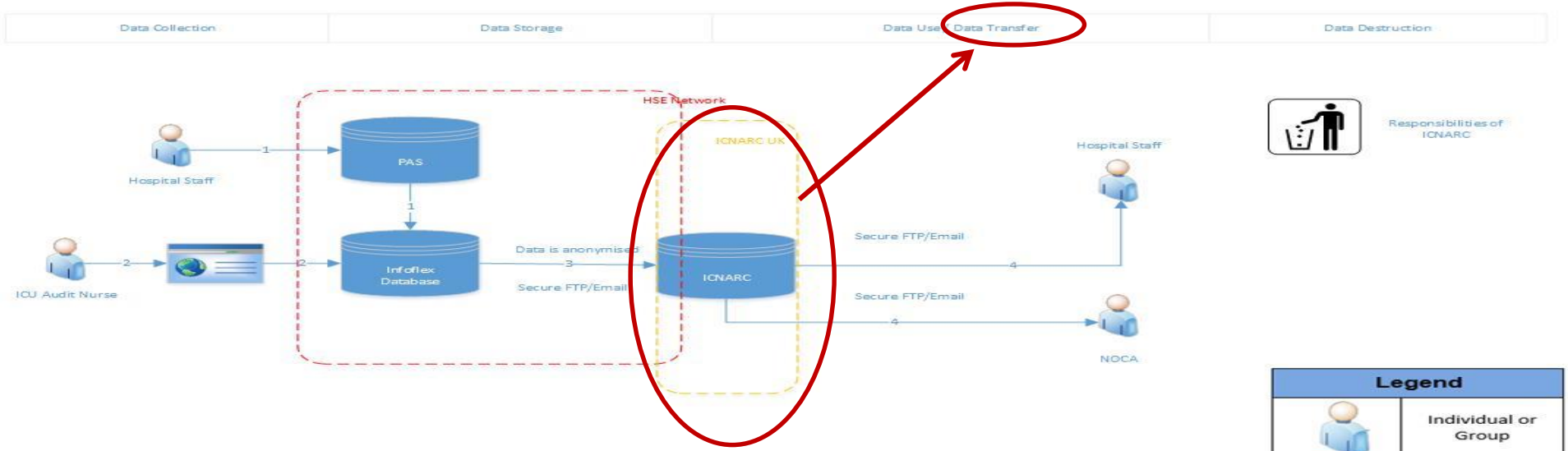


- Who is collecting the data?
- What personal data are they collecting?
- Where and how are the collecting the data?
- Are they entering the data onto electronic system, excel file, database etc.
- Where is the data stored (paper and electronic records)?
- As part of your audit, do you intend to share the data with anyone , if so where are they located?

National Office of Clinical Audit

Example of Data Collection/Storage/Transfer Flow

National ICU Audit – v1.0
Data Flow Lifecycle of the Recording and Monitoring of patient treatment with the Acute Hospitals ICU



Data Key
1. Patient Information: Name, address, date of birth, length of stay, initial surgeon seen, follow up care, transfer location
2. Validation of patient information
3. Patient Information Anonymised
4. Anonymised Statistical Reports

Legend	
	Individual or Group
	Database
	Webpage

NOCA National Office of Clinical Audit

Data Sharing – Under GDPR

Brexit

Data flows

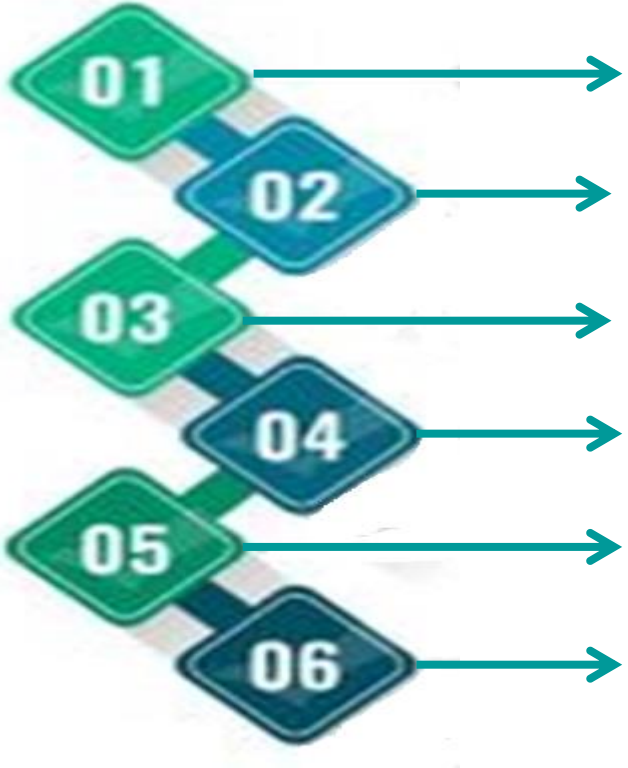
EEA to UK	Need appropriate safeguard in place	Standard Contractual Clause (SCC). Legally Binding Enforceable Instrument (LBEI) Derogation
UK to EEA	Continue as normal due to Statutory Instrument being in place	
EEA to USA	Check if part of privacy shield scheme, if not, have other appropriate safeguard in place (SCC, LBEI, Derogation)	
USA to EEA	Continue uninterrupted	
EEA to Rest of the world	No change	
Rest of the world to EEA	No change	

Contact your DPO

Source: https://www.england.nhs.uk/eu-exit/data - *Accessed on 29/10/2019, Modified for use in Irish Context.*

NOCA National Office of Clinical Audit

Data Security – Basics



- Password protect your computer and sensitive files
- Encryption on laptops and other devices e.g. USB key
- Personal identifiable information should not be emailed in plain text, use initials or partial data.
- Stored on a secure drive
- Adherence with local IT Policies
- Limiting what you share and only sharing data with authorised individuals.

NOCA National Office of Clinical Audit

Data Security – Basics

- Security applies to paper records too and everyone has a role to play!

***Source**:* https://www.shredit.com/getmedia/6e17f5be-4932-4531-99ae-f3587b0645d6/12-Information-Security-Office-Reminders.aspx?ext=.pdf *Accessed on 14/03/2018*

NOCA National Office of Clinical Audit

Reviewing your Data

- Data Quality
  - GDPR Requires you to hold accurate and relevant information
  - Reviewing audit data will support this, but remember anonymised data cannot be linked back or data quality improved.

NOCA National Office of Clinical Audit

Ethical Consideration - similar to GDPR Principles

- Clinical audit must always be conducted within an ethical framework.
- What does this mean?
  - Respecting the confidentiality and privacy rights of patients and staff
  - Designing your audit well so that the data is collected and stored appropriately.
  - Ensuring data is retained for no longer than is necessary

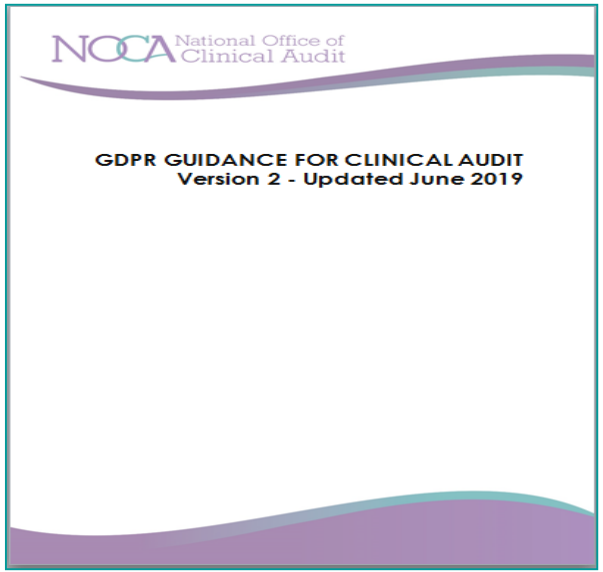
NOCA National Office of Clinical Audit

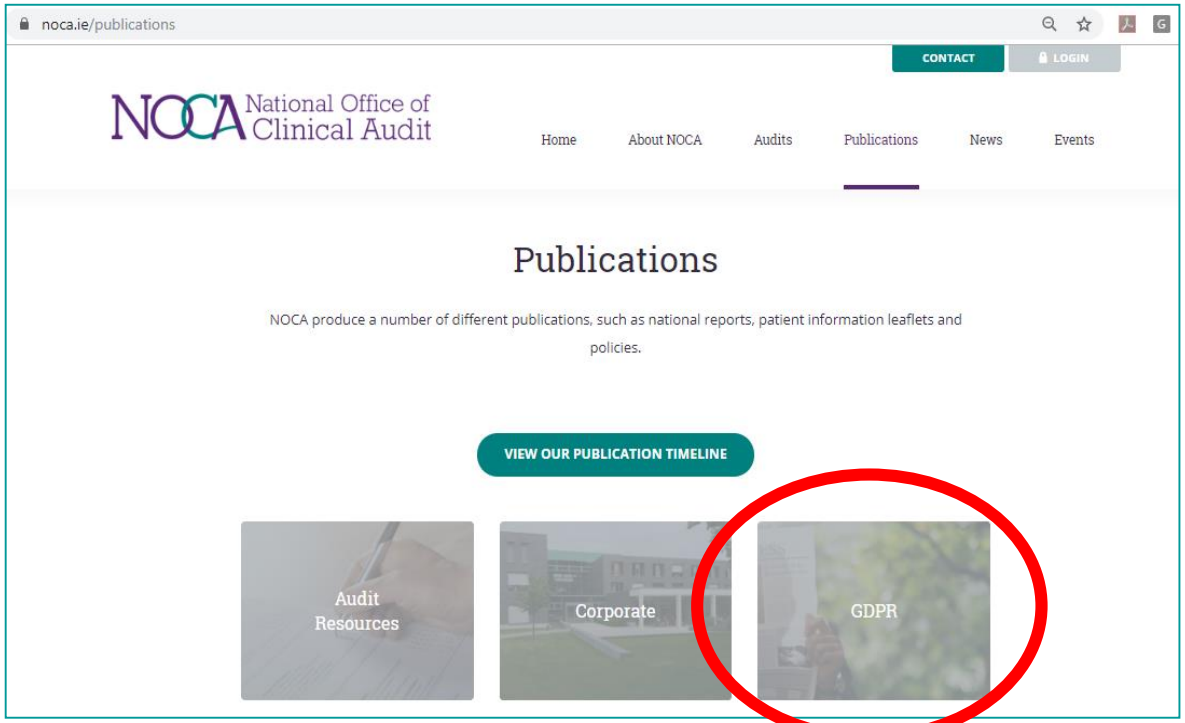
Summary

- Planning vital. Design your audit well and consider privacy of data
- Identify your lawful basis
- Ensure privacy notice or information leaflets/posters in place
- Only collect what is needed and keep data accurate
- Always keep data secure and don't share unless authorised to do so
- Report any breaches
- Stay GDPR aware and Keep auditing!

NOCA National Office of Clinical Audit

GDPR – Guidance and FAQs…





NOCA National Office of Clinical Audit

Some Acknowledgements

National Office of Clinical Audit

Any data protection queries?

Data Protection queries
Email: dpo@noca.ie

Brid Moran
Information Manager
Email: bridmoran@noca.ie
Tel: 087-2025437