WEBINAR 8

Embracing Change

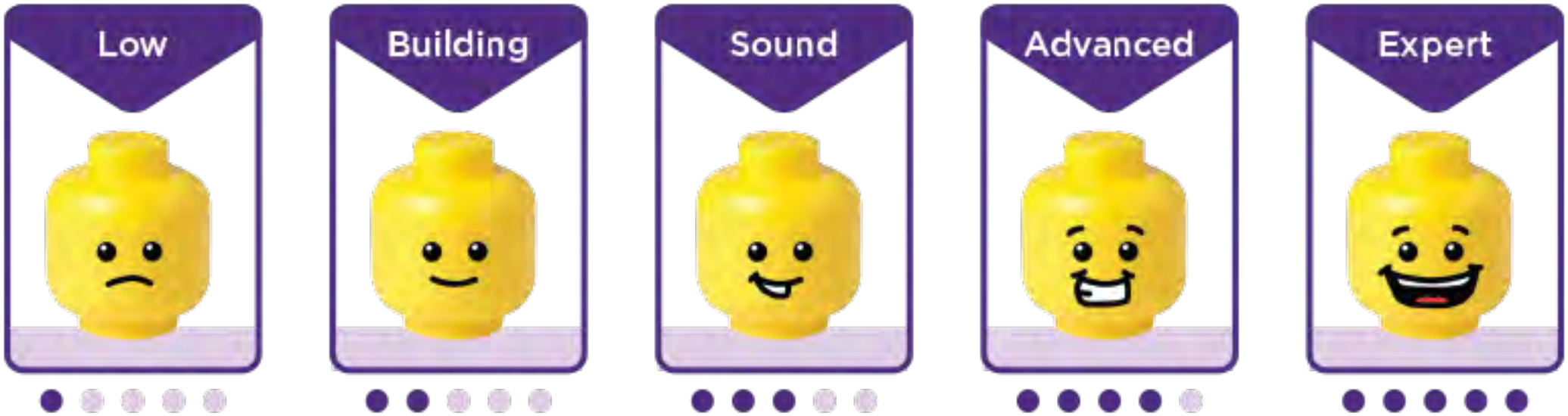
Applying the NDIS Practice Standards in Psychosocial Disability Services

Governance, Information Management and Privacy for registered NDIS providers

NDIS Practice Standards and Quality Indicators

LIVE POLL

How would you rate your knowledge of
the NDIS Practice Standards and registration requirements?



1 2 3 4 5

Overview of the Embracing Change Webinar Series

Webinar 1 — **24 October 2019**

Pain Points and Priorities for Providers In Applying the Practice Standards In Psychosocial Disability Services

Webinar 2 — **28 November 2019**

Core Module 1 Rights & Responsibilities

Webinar 3 — **5 March 2020**

Core Module 2 Governance and Operational Management

Webinar 4 — **28 May 2020**

Core Module 2 Governance and Operational Management Continued

Webinar 5 — **2 July 2020**

Provision of Supports and the Provision of Supports Environment

Webinar 6 — **27 August 2020**

Understanding Behaviour Support Arrangements

Webinar 7 — **29 October 2020**

Worker Screening and Worker Requirements for NDIS service providers

Webinar 8 — **3 December 2020**

Governance, Information Management and Privacy

Webinar 9 — **25 February 2021**

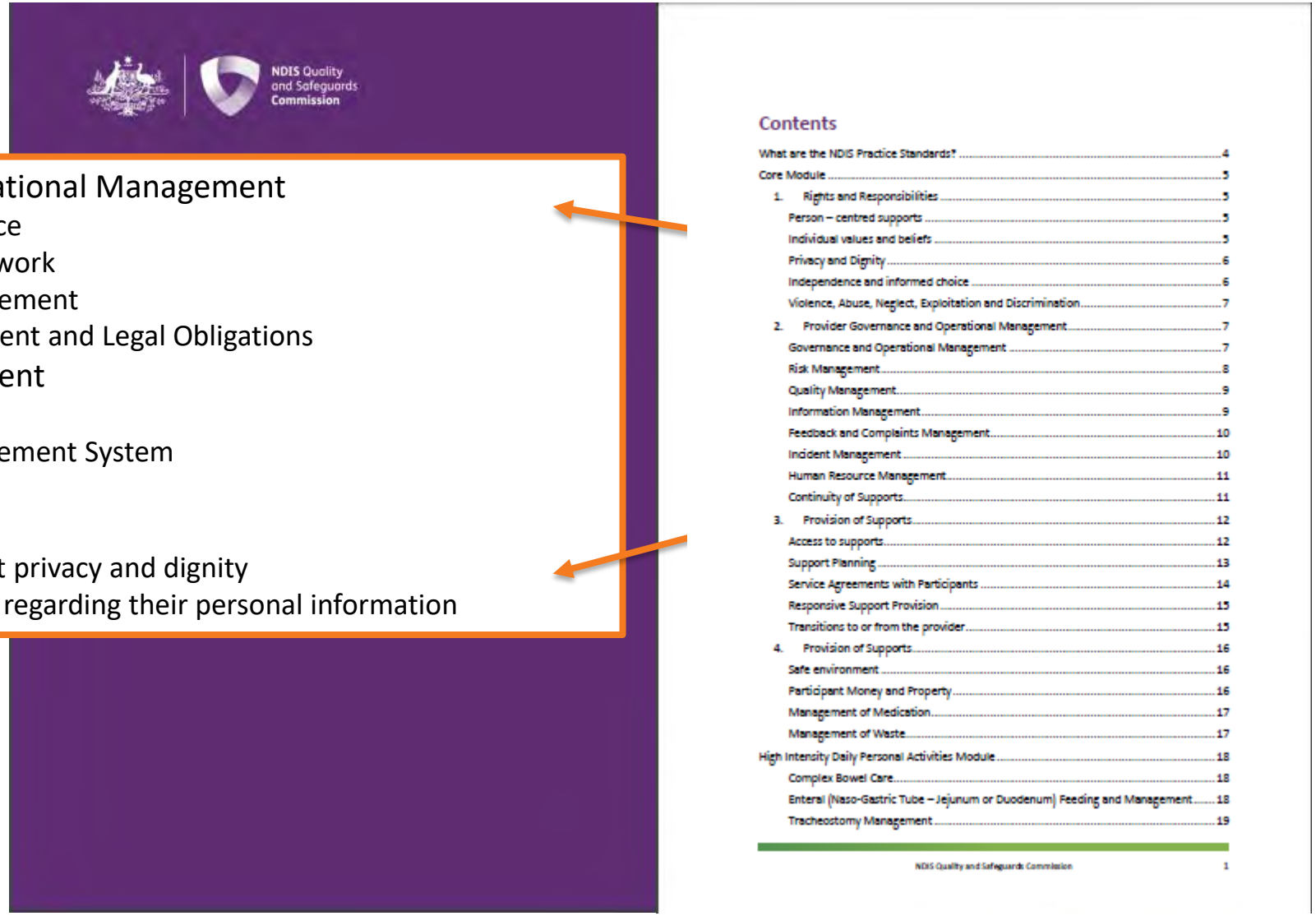
Quality Management and Continuous Quality Improvement

Webinar 10 — **24 June 2021**

Learnings and Next Steps for NDIS Quality & Safety in Psychosocial Services

Today we will cover:

- Governance and Operational Management
  - Inclusive Governance
  - Governance Framework
  - Operational Management
  - Financial Management and Legal Obligations
- Information Management
  - Participant consent
  - Information Management System
  - Record Storage
- Privacy and Dignity
  - Ensuring participant privacy and dignity
  - Participant consent regarding their personal information



NDIS Quality and Safeguards Commission

Contents

Learning Objectives

After this webinar participants will be able to:

- Articulate the Governance, Information Management and Privacy requirements for NDIS service providers;
- Apply Privacy Law principles relevant to NDIS service provision;
- Describe systems and processes which give effect to the Governance, Information Management and Privacy requirements;
- Identify relevant documentation (policies and procedures) and practices specific to psychosocial service providers that can meet these outcomes and quality indicators;
- Identify pitfalls to avoid in preparing your self-assessment and onsite audit/s against the NDIS Practice Standards; and
- Understand benefits to participants and the organisation of a successful implementation of a Quality System aligned with the NDIS Practice Standards.

NDIS Practice Standards - Governance, Information Management and Privacy

Katrina Broadbent

pwc

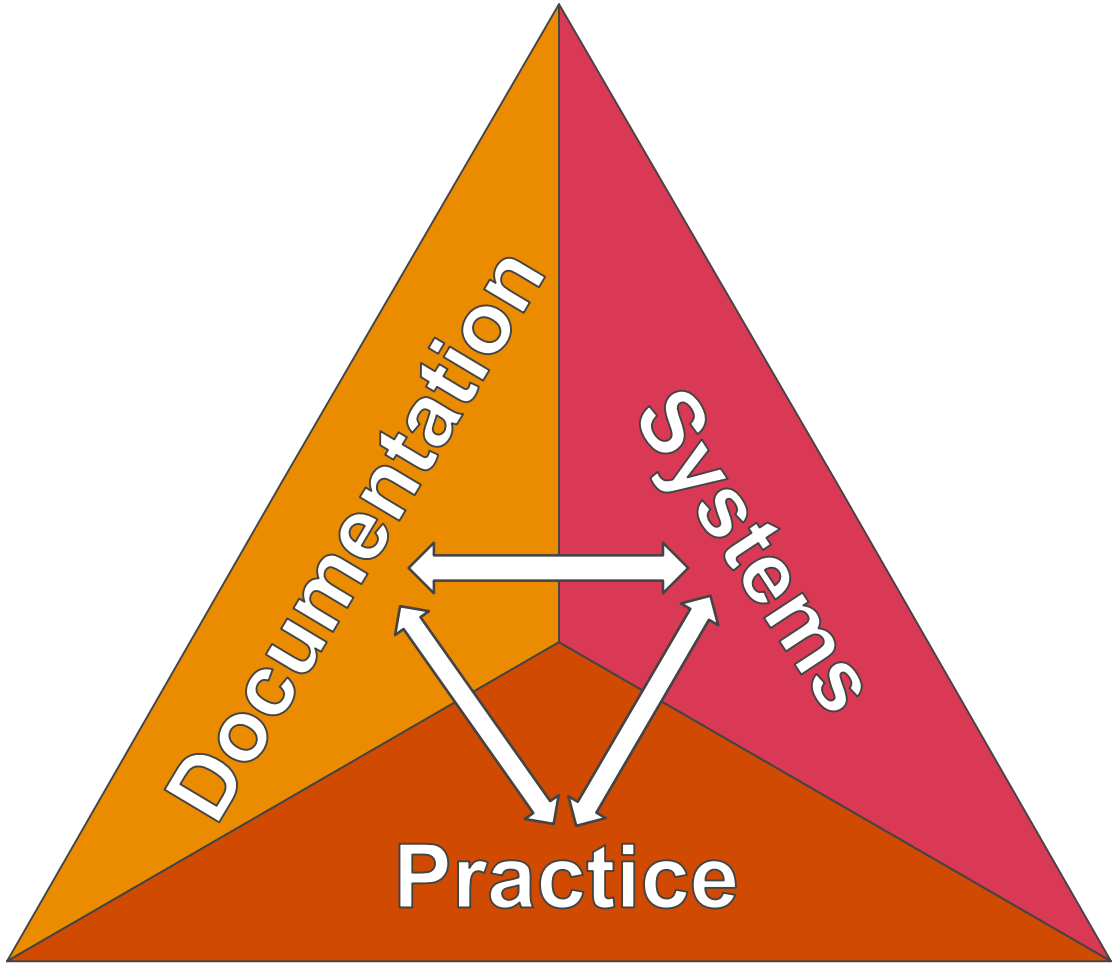
Approved Quality Auditors
National Disability Insurance Scheme

1

Governance & Operational Management

Katrina Broadbent
Manager – NDIS Account Management
PwC's Certification and Compliance Services

Policies align to practice



Governance and Operational Management

Outcome:

- Each participant's support is overseen by robust governance and operational management systems relevant ***(proportionate)*** to the **size**, and **scale** of the provider and the **scope** and **complexity** of supports delivered.

Governance and Operational Management

Indicator:

1. Opportunities are provided by the governing body for people with disability to contribute to the governance of the organisation and have input into the development of organisational policy and processes relevant to the provision of supports and the protection of participant rights.

Governance and Operational Management

Indicator:

2. A defined structure is implemented by the governing body to meet a governing body's financial, legislative, regulatory and contractual responsibilities, and to monitor and respond to quality and safeguarding matters associated with delivering supports to participants.

Governance and Operational Management

Indicator:

3. The skills and knowledge required for the governing body to govern effectively are identified, and relevant training is undertaken by members of the governing body to address any gaps.

Governance and Operational Management

Indicator:

4. The governing body ensures that strategic and business planning considers legislative requirements, organisational risks, other requirements related to operating under the NDIS (for example Agency requirements and guidance), participants' and workers' needs and the wider organisational environment.

Governance and Operational Management

Indicator:

5. The performance of management, including responses to individual issues, is monitored by the governing body to drive continuous improvement in management practices.

Governance and Operational Management

Indicator:

6. The provider is managed by a suitably qualified and/or experienced persons with clearly defined responsibility, authority and accountability for the provision of supports.

Governance and Operational Management

Indicator:

7. There is a documented system of delegated responsibility and authority to another suitable person in the absence of a usual position holder in place.

Governance and Operational Management

Indicator:

8. Perceived and actual conflicts of interest are proactively managed and documented, including through development and maintenance of organisational policies.

2

Information Management & Privacy

Katrina Broadbent
Manager – NDIS Account Management
PwC's Certification and Compliance Services

Information management

Outcome:

Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers.

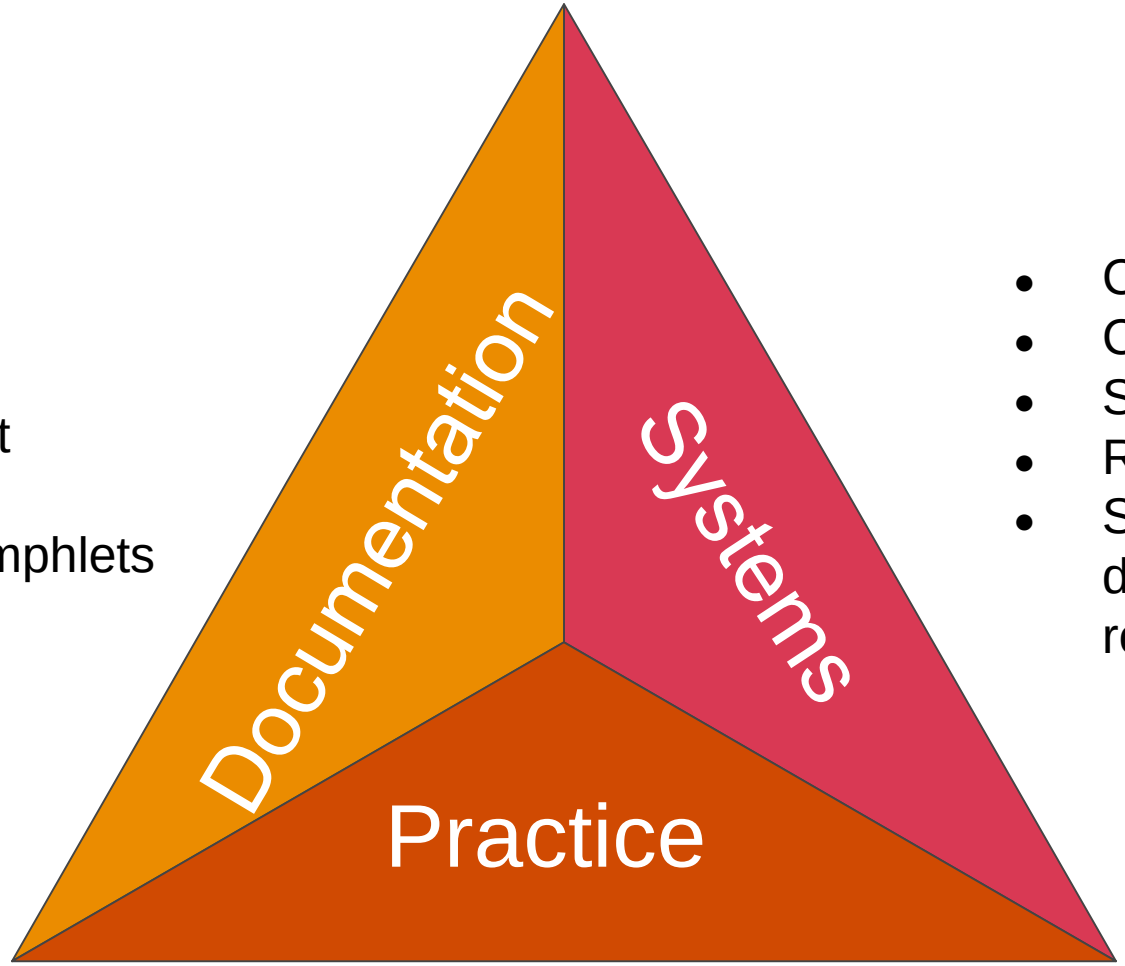
What an auditor may look at:

- The type of information that is being collected
- Where it is stored?
- Who has access to this information, for example - is it restricted to specific clinicians and management personnel or do all staff have access?
- How do these controls work?
- Data storage arrangements
  - Is the data stored in Australia or off shore?
  - Is there compliance with state based and Commonwealth Privacy requirements and law?

Policies align to practice

Examples:

- Policies
- Procedures
- Code of Conduct
- Agreements
- Brochures & pamphlets
- Website



- CMS
- Client intake
- Surveys and feedback
- Recruitment of staff
- Staff training, development, appraisals, reviews

- Service delivery
- Client & carer feedback
- Staff understanding
- Physical environment

Privacy

Outcome:

Each participant accesses supports that respect and protect their dignity and right to privacy.

What an auditor may look at:

- Code of conduct
  - How the 7 elements of the code of conduct underpin your policies
- confidentiality policies and information is made available to participants
- accessibility of information
- clear and documented consent,
- open communication and information surrounding confidentiality
- focus on individual participant privacy

Thank you

pwc.com

Privacy and data laws for NDIS providers

3 December 2020

Mae Tanner, lawyer

Not-for-profit Law

justice connect

justice connect

www.nfplaw.org.au

Resources

Enquiries

Referrals

Advocacy

Training

Privacy laws and your

May 18, 2017

CHARITY DIGITAL NEWS

Home | Categories | Resources | Announcements | Marketplace | Events | Advertise With Us

> Data security > Charities urged to protect themselves from cyber attacks

Charities urged to protect themselves from cyber attacks

16 May 17 | Author Austin Clark | Data security Tips & Advice

Recommend 5 | Share 1 | Tweet | G+1 1

Charities are being reminded of the need to have sufficient and effective measures in place to protect against cyber attacks.

The ongoing 'WannaCry' ransomware attack has highlighted the damage caused by attacks if IT systems and protection aren't kept up-to-date. While it's unclear if any charities have been targeted by this attack, charities could be a prime target for future cyber criminals.

Speaking at the Charity Finance Group's Annual Conference earlier this year, James Mulhern, chief information security officer at Eduserv outlined how charities are a target because they tend to store large amounts of stakeholder data.

"Charities are a big target for cyber criminals because they have valuable data, including personal information which is of huge value to attackers," he said.

Third Sector

British Pregnanc
appeal against fi

22 April 2014 by Sam Burne Jame

The charity pays £160,000
after the personal details
unnecessarily on its websi

bpas

The Alzheimer's Society describes itse
charity" Photo: Alamy

Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles

Home | Politics

Shop | Earth

Magazine

£200,000

ach that revealed

ontacted the
ancy issues.

t realised its site

and telephone number of people who asked for a call back for advice on pregnancy issues.

The British Pregnancy Advice Service didn't realise their website was storing this information,

Search

SET LOCATION
for local news & weathe

More

Health News

know what makes you tick?

s of silence: The new way to
out of life

know the signs of heat

TORIES

lasts intelligence reports
ficial press conference

eton loses position as
or after bankruptcy

appears in court for
ssault trial

g daughter found
after going missing

water people evicted
er with nowhere to

estling's
country pubs and

Privacy laws and your organisation

Health Hub Ltd

Penelope meets with Jerome to discuss his disability and treatment plan.

General legal information only and not legal advice

Privacy laws and your organisation

Do the APPs apply to your organisation?

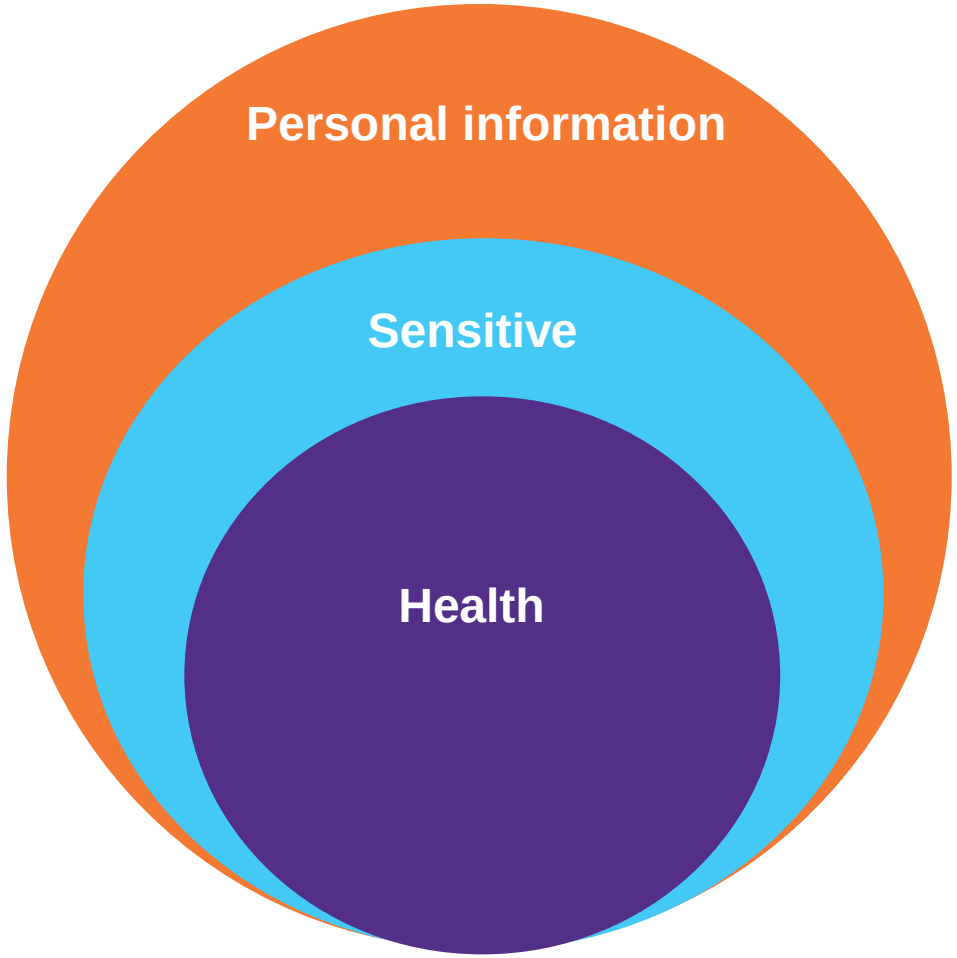
- Annual turnover >$3m
- Contract
- Health service
- Trades in personal info
- Credit provider
- Opt-in

Privacy laws and your organisation

What information is protected by privacy laws?

Examples:

- Racial/ethnic origin
- Political opinions
- Religious beliefs
- Sexual orientation
- Criminal record



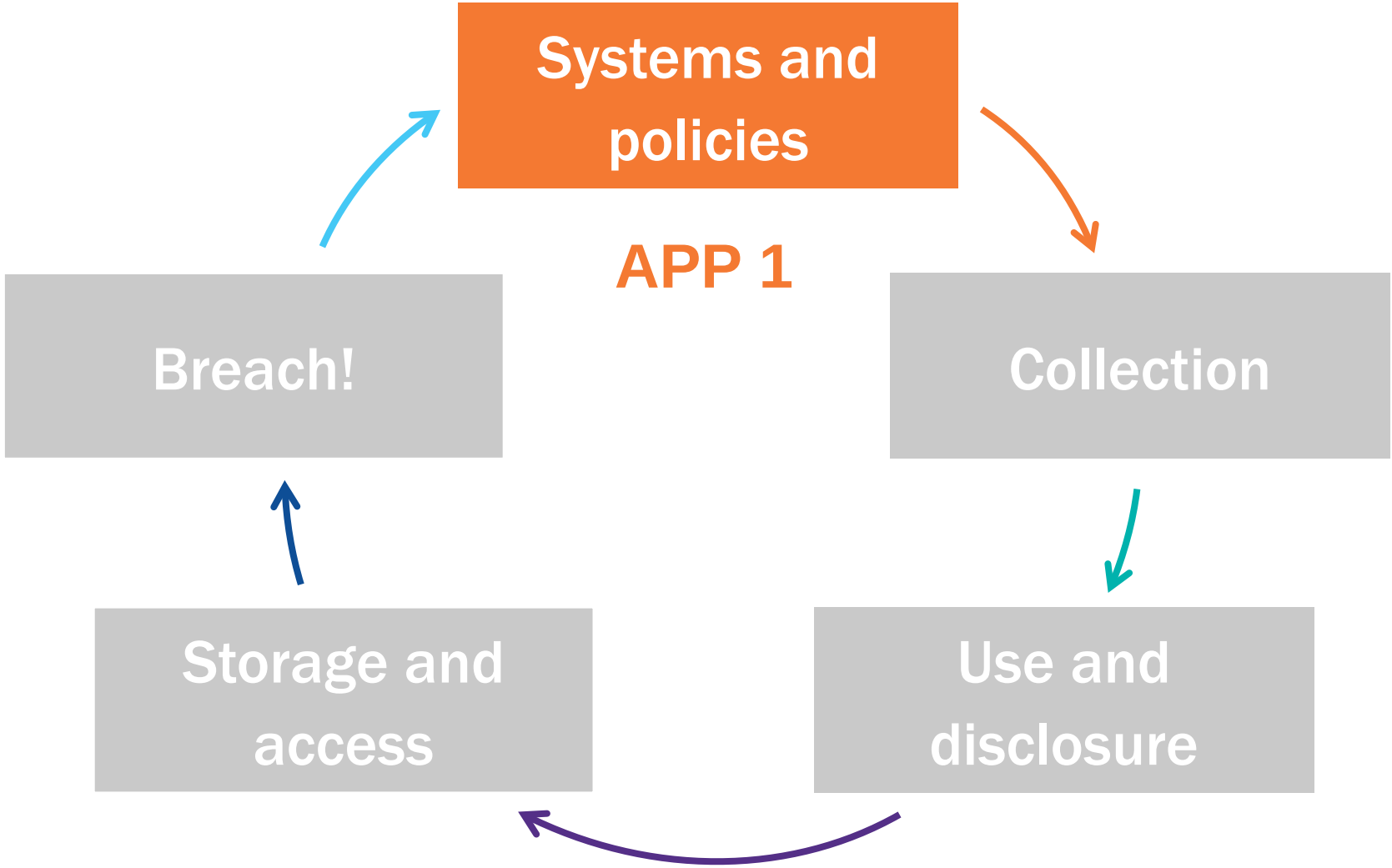
Examples:

- Name
- Signature
- Contact details
- Photos

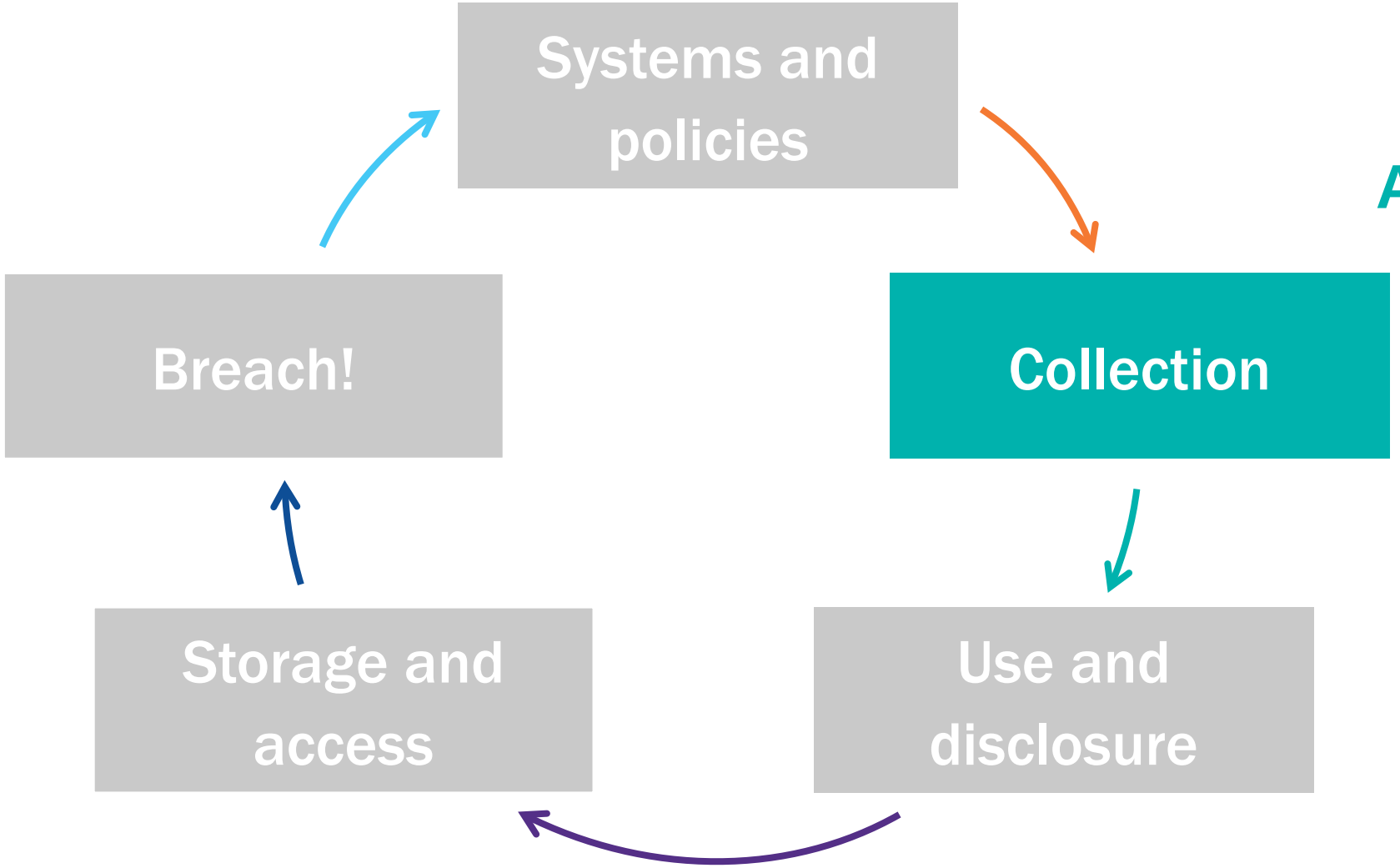
Examples:

- Mental health
- Disability
- Bodily donations
- Genetics

APPs and the personal information lifecycle



APPs and the personal information lifecycle



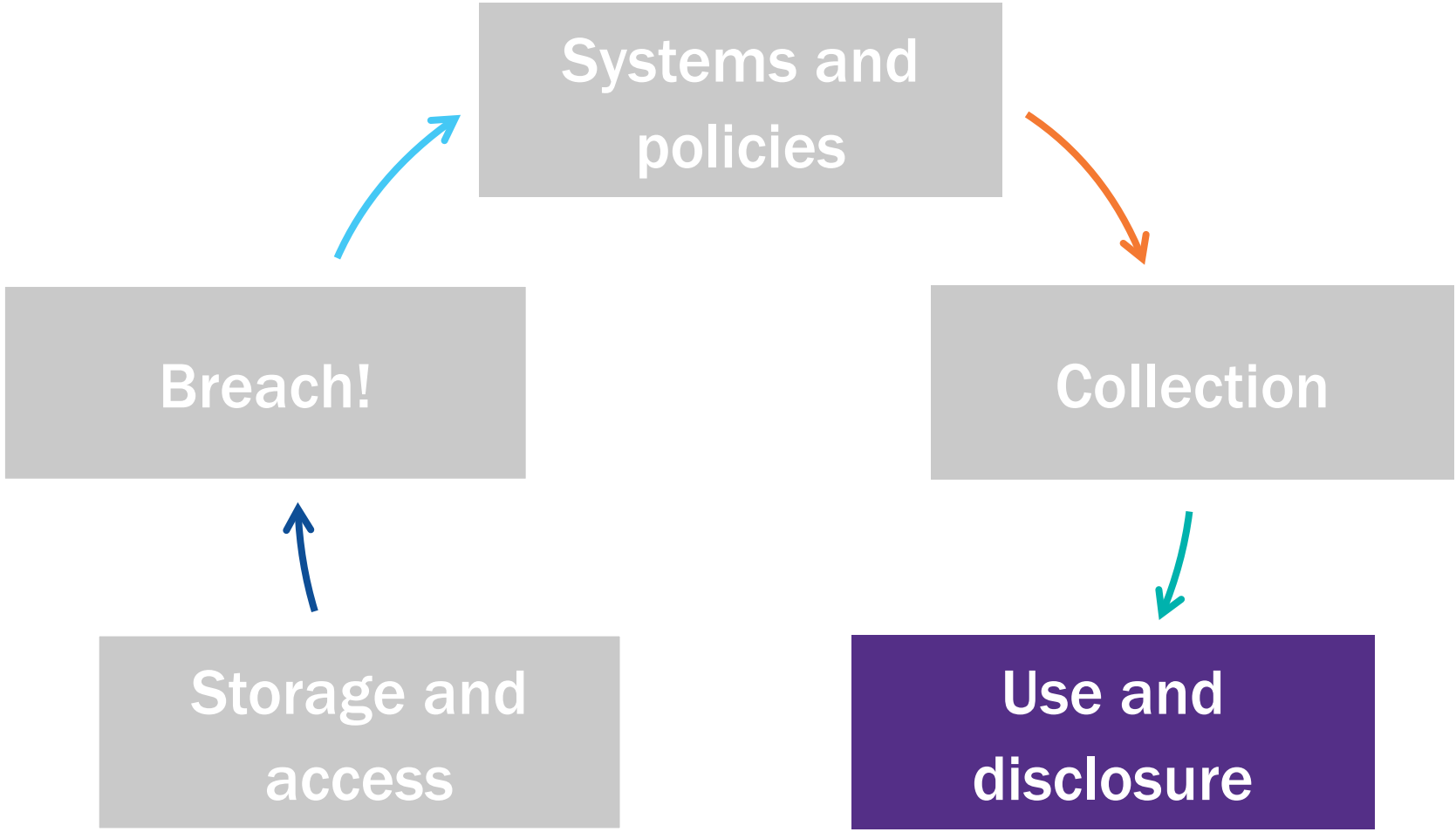
APPs 2 – 5

APPs and the personal information lifecycle

Case study – Health Hub Inc

Penelope wants to refer Jerome to another service for different help.

APPs and the personal information lifecycle

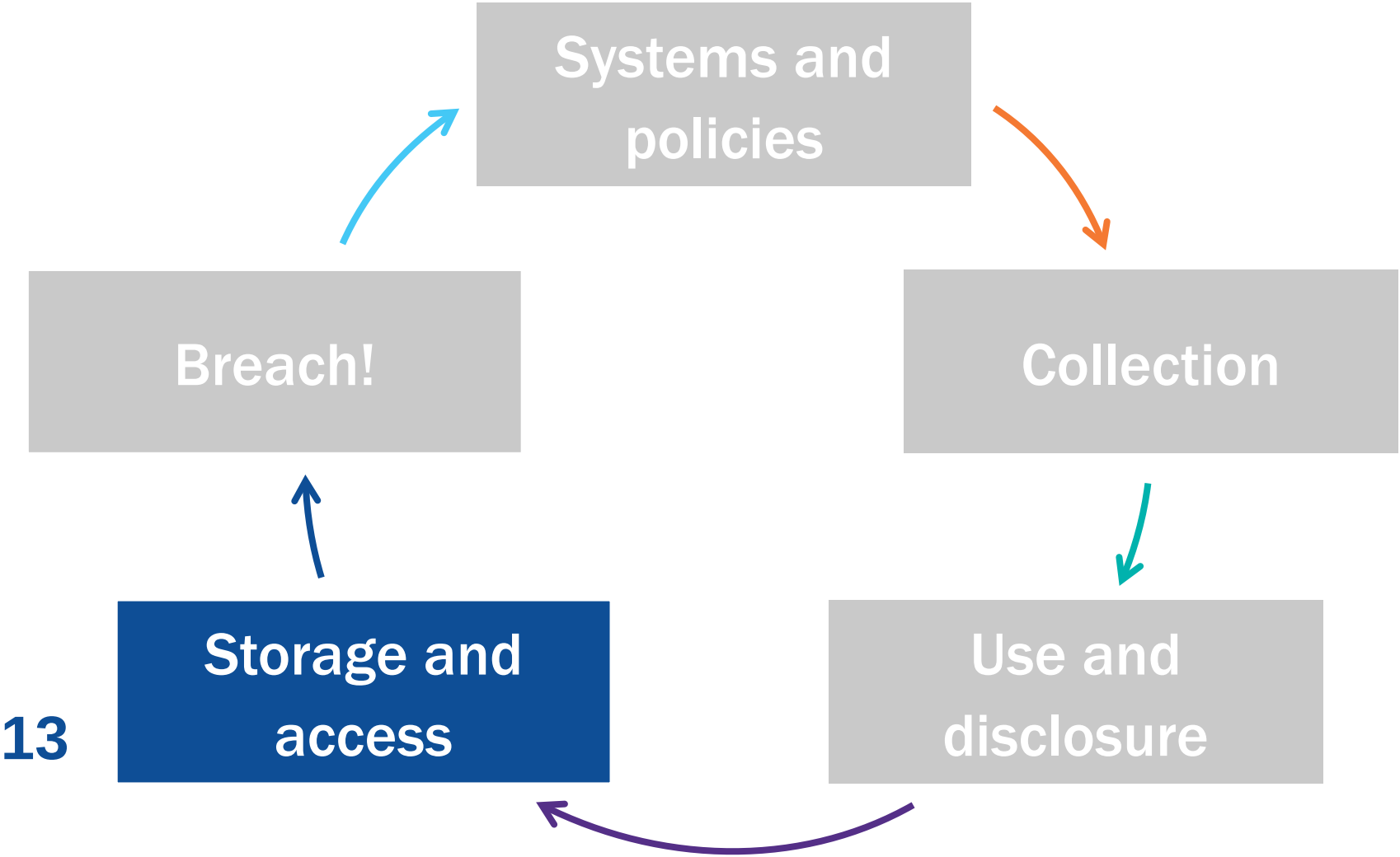


APPs and the personal information lifecycle

Case study – Health Hub Inc

Jerome asks to see his file.

APPs and the personal information lifecycle



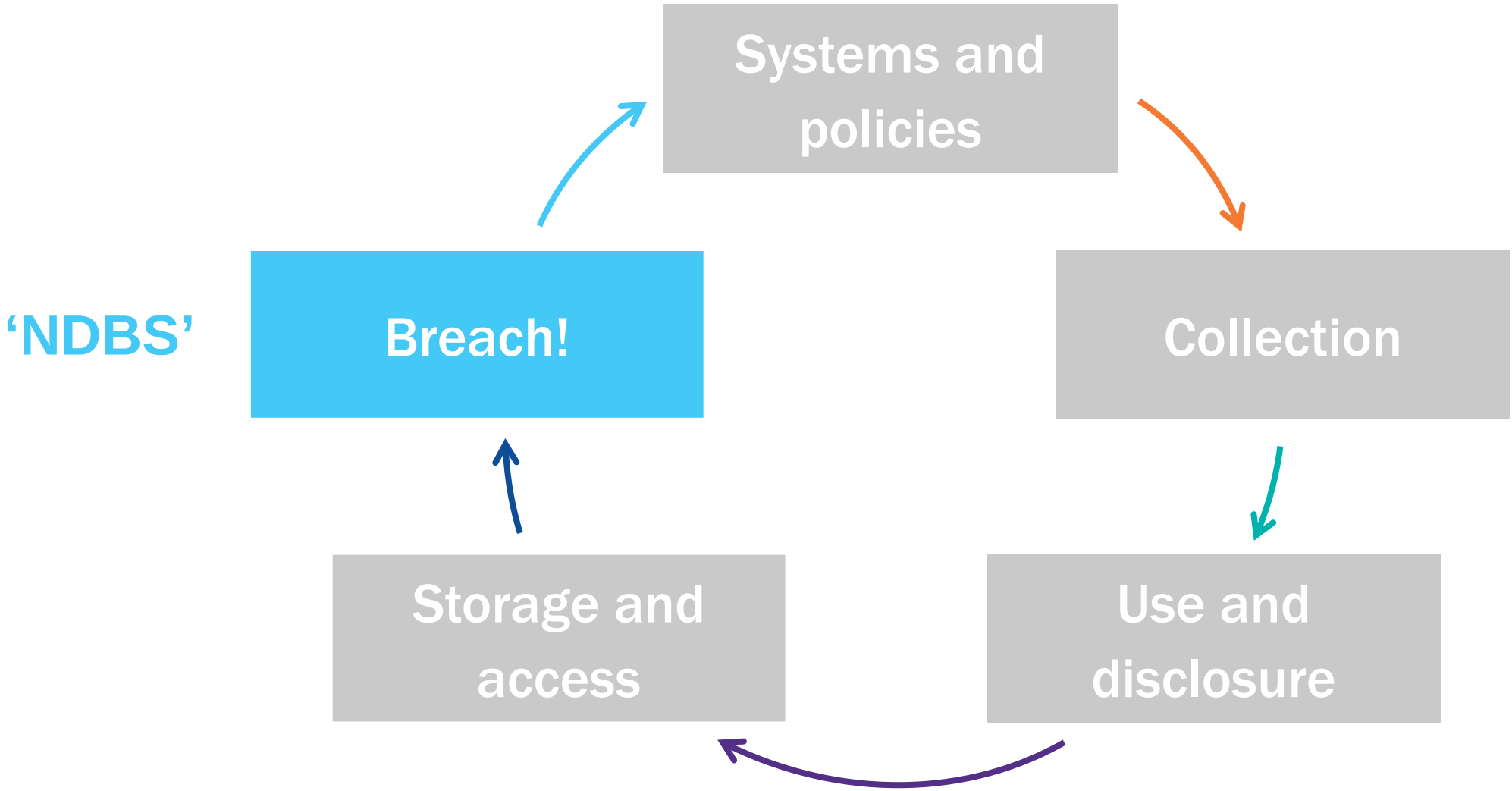
APPs 10 – 13

APPs and the personal information lifecycle

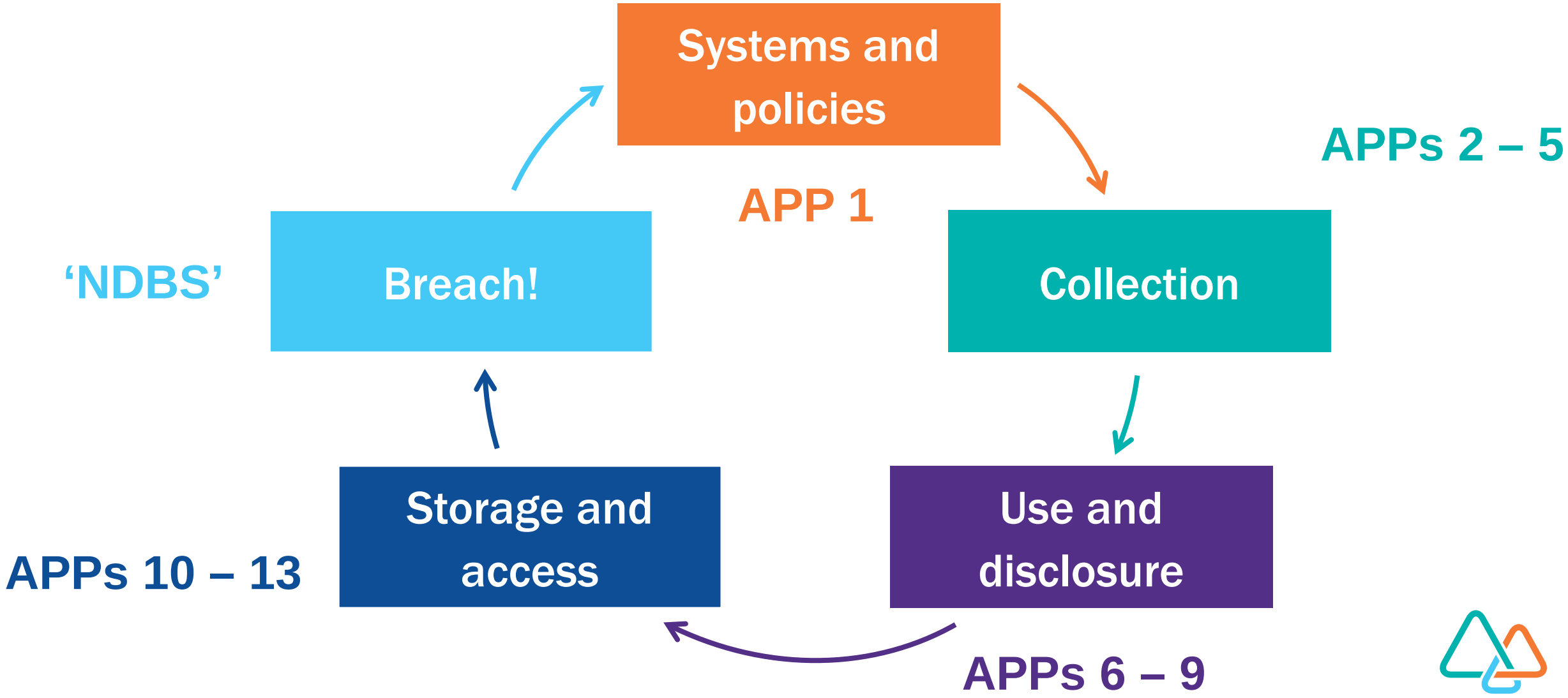
Case study – Health Hub Inc

Penelope shares information about Jerome with a former colleague.

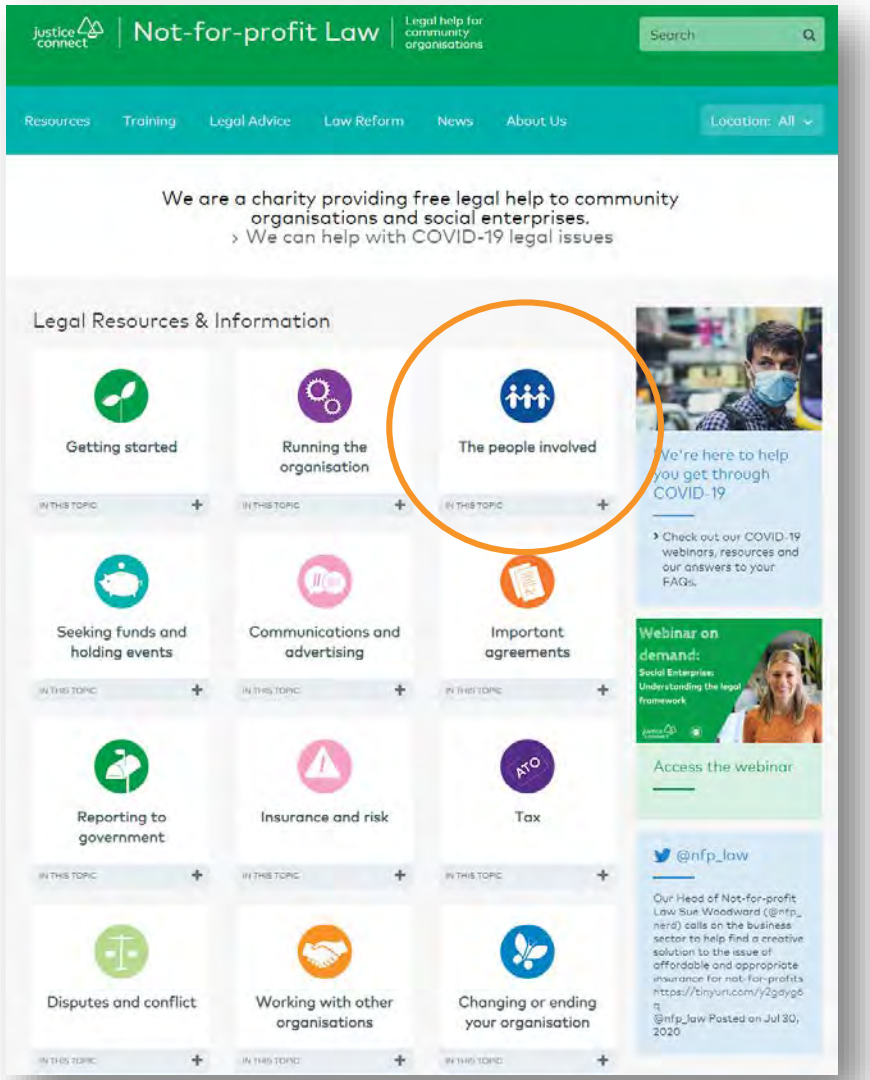
APPs and the personal information lifecycle

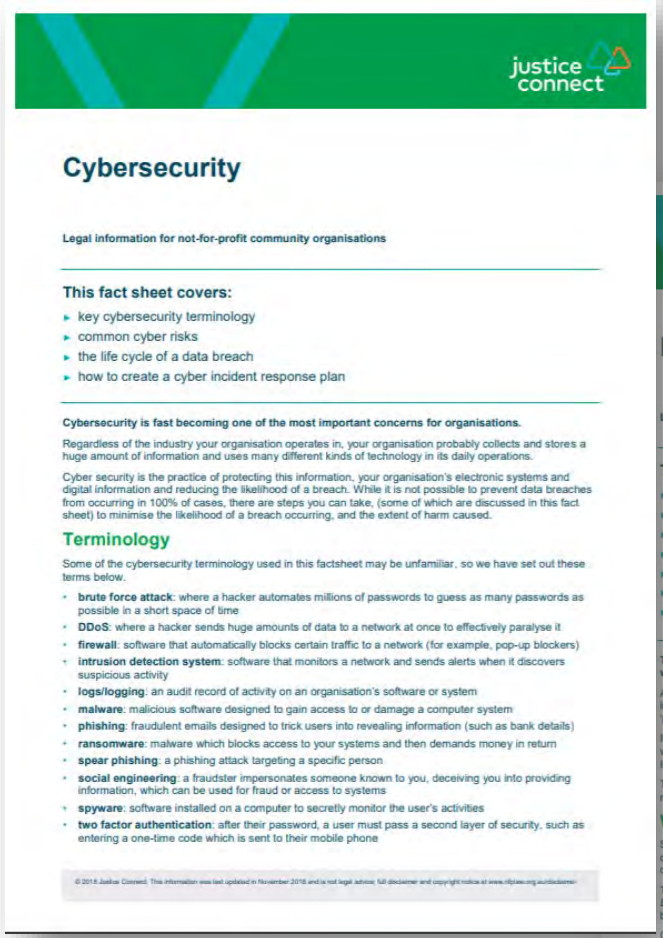


APPs and the personal information lifecycle



www.nfplaw.org.au





Thank you for listening.

Tag us @justiceconnect

Mention #justiceconnect

Tweet @nfp_law

Follow us @justiceconnect

STRIDE For better mental health

Governance, Information Management and Privacy

Embracing Change

Catherine Scott-Richardson, December 2020

About Stride

Australia's longest-established mental health charity providing specialist mental health services to people with mental illness & complex needs since 1907.

Our Services

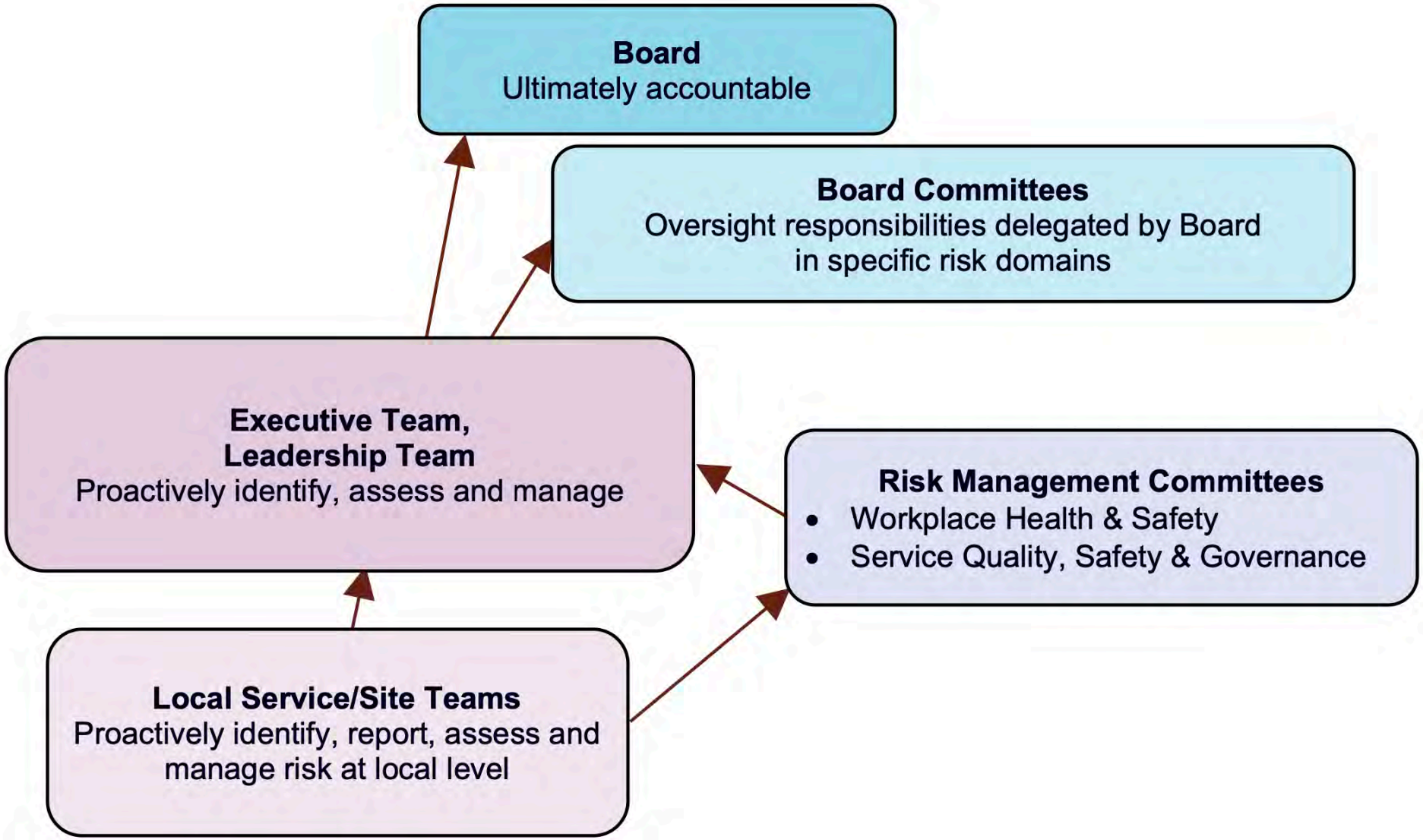
Stride provides a full range of mental health services designed to support those with a lived experience of mental distress. The care and support we provide ranges from assistance with developing the skills to manage day-to-day tasks through to fully-supported accommodation for those with complex needs.

Our services work with a range of demographics across:

- Kids
- Young People
- Adults
- Families and Carers

Take the first step towards better mental health

Governance


Board
Ultimately accountable
Board Committees
Oversight responsibilities delegated by Board in specific risk domains
Executive Team, Leadership Team
Proactively identify, assess and manage
Risk Management Committees
• Workplace Health & Safety
• Service Quality, Safety & Governance
Local Service/Site Teams
Proactively identify, report, assess and manage risk at local level

Governance

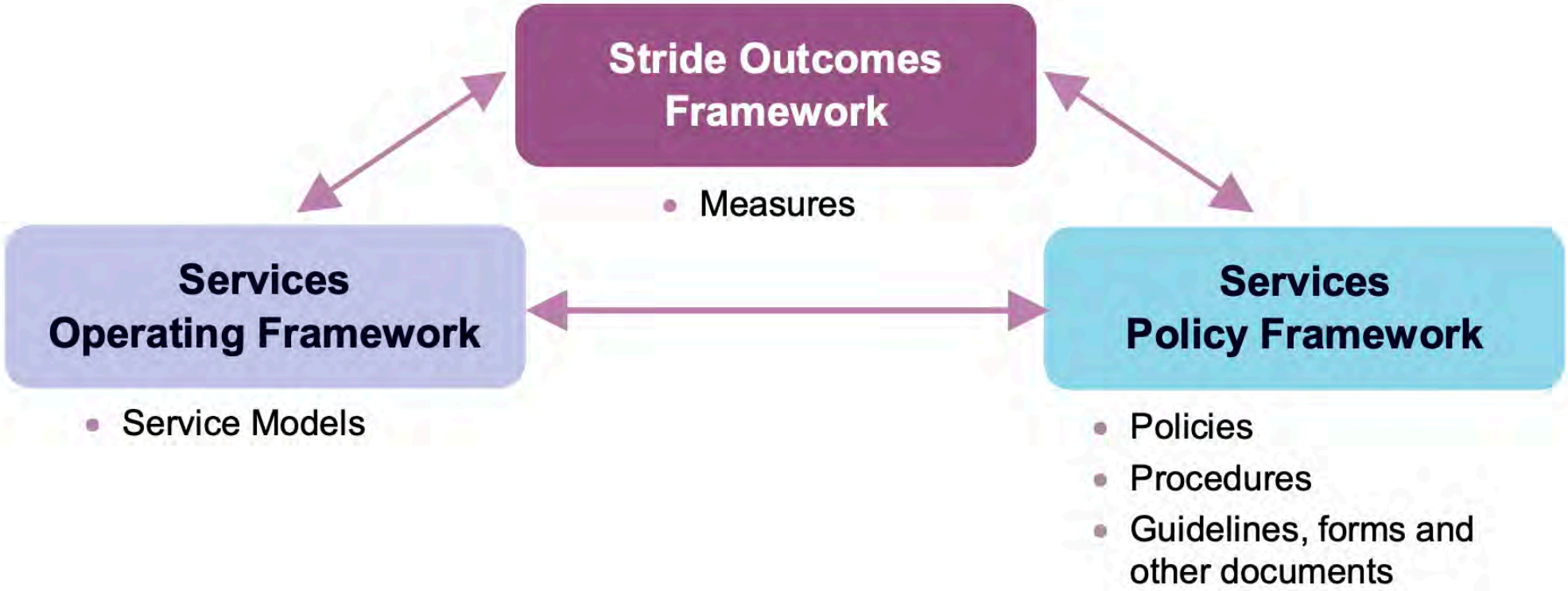
Corporate Governance

- Financial, enterprise risk, and legal compliance
- Strategic direction

Service / Clinical Governance

- Service quality and participant safety
- Participant and carer engagement
- Participant and service outcomes
- Staff education and training

Governance


Stride Outcomes Framework
Measures
Services Operating Framework
Service Models
Services Policy Framework
Policies
Procedures
Guidelines, forms and other documents

Using information

- Stride requires participant confidentiality to be maintained to the highest standards and to comply with legislative requirements.
- Participants must be informed about consent, confidentiality and how their information will be recorded and used.
- All information collected must be recorded in the relevant database or electronic medical or participant record system approved for use in each program delivery area in line with funding body and legislative requirements.

Using information

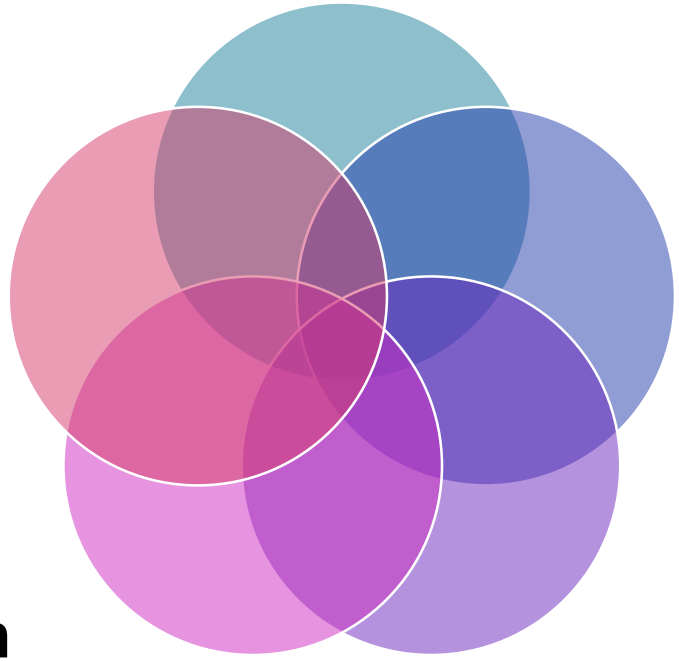
- Data collected is used to report on consumer / participant type, access and program activities and performance and must be de-identified when used for funding body reporting purposes or used within Stride for service review and planning purposes.
- Participant information can only be collected, shared or transferred and reported upon with consumer / participant consent.
- Appropriate security mechanisms for both electronic records and hard copy records must be maintained to the highest standards (ISO 27001) and in compliance with State and Federal legislation (Privacy Act 1988).
- On commencement of employment, staff and volunteers are orientated to and advised of their obligations to comply with Federal Privacy legislation and Stride procedures and guidelines on Confidentiality and acceptable use of the Information Technology.

Information technology

- Stride ensures that there are comprehensive authorisation systems in place to manage access to information in order to support decision-making and facilitate the highest quality of care and participant services.
- Electronic records are backed up regularly to ensure information is not lost. Archived participant files are kept securely and in accordance with State and Federal legislation on information retention requirements.

General duty

Third party disclosures



Professional ethics

Legislation

Common law

Conclusion and Key Messages

- There is a delicate tension between corporate and clinical governance as it stands within mental health organisations, irrespective of whether they are public, private or not for profit.

- Considering the above point, information management comprises both the architecture and administration of the systems and how we best use those systems to shape and enhance quality service delivery.

- Within mental health organisations like Stride, obligations around participant privacy is determined by professional ethics, common law and legislation.

Q&A Panel Discussion

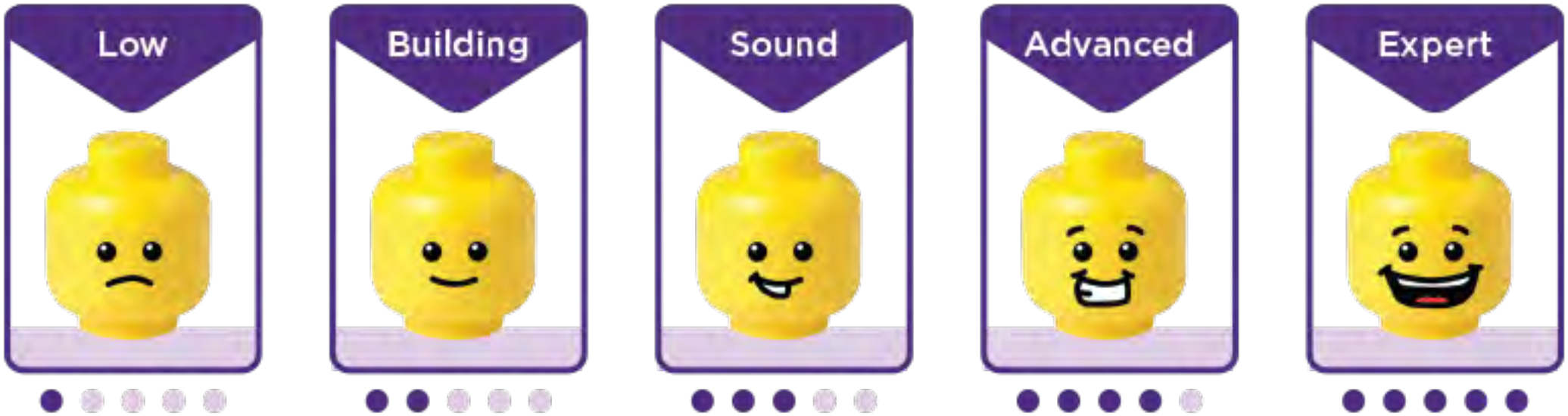
Katrina Broadbent, Assurance Manager, PricewaterhouseCoopers

Mae Tanner, Manager - Training, Justice Connect

Catherine Scott-Richardson, National Manager - Governance, Safety & Quality, Stride Mental Health (formerly Aftercare)

LIVE POLL

How would you rate your knowledge of
the NDIS Practice Standards and registration requirements?



1 2 3 4 5

THANK YOU FOR JOINING US TODAY

NEXT WEBINAR

25 February 2021: Quality Management and Continuous Quality Improvement

ACCESS RESOURCES

Find out more about the Embracing Change project

- View past webinars
- Find resources

www.mhcc.org.au/project/embracing-change

LET'S CHAT

Project Manager: **enis@mhcc.org.au**