



Privacy and Personal Data: Navigating the Minefield

Sarah Auva'a

Head of Spark Compliance & Privacy

Today's workshop

- Introductions
- Privacy 101
- Why manage privacy?
- Good communications help ensure shared expectations
- Personal information mapping and privacy policies
 - Prepare an information map for your organisation
- Before you send your next comms
- You've had a privacy breach
- Recap
- Questions

Spark Volunteer Day

- Spark Foundation is the charitable branch of Spark New Zealand
- Launched in July 2011, the Foundation is a registered charitable trust
- A Volunteer Day is gifted to Spark people every year
- FY16 - 28% participation saw 1,390 days gifted - with a value of \$417,000



Spark^{nz}
Foundation

Introductions

- Who you are
- Your biggest privacy concern?





Privacy 101

What is personal information?

- Any information about an identifiable, living individual
- It may still be personal information even if it doesn't include someone's name
- If there's a reasonable chance that a person can be identified using the information, it is personal information
- Not ltd to “data base” type information – includes “unstructured information” and information volunteered by the individual e.g. could include what client has advised in an interview, or the contents of a letter of complaint
- e.g. name, phone number, income, bank account information, service usage information

Privacy principles

- Only collect personal information that you need for lawful purposes connected with the purpose of your organisation
- Try to collect personal information directly from the individual concerned
- Collect information fairly and legally
- When collecting personal information, tell the individual what you will use it for
- Only use / share personal information in ways consistent with what you have advised the individual
- Keep personal information safe and secure
- Allow individuals to access and correct their personal information
- Don't hold personal information for longer than you need it

Privacy principles

- There are some exceptions to some of these principles e.g. publicly available information
- The Office of the Privacy Commissioner has excellent resources that provide more detail
- www.privacy.org.nz



Why manage privacy?

Data is critical for organisations

High quality data supports
good decision making &
strategy execution

Personal Information is
increasingly valuable

Successful organisations use
personal information to meet
stakeholder needs and achieve
organisational objectives while
maintaining the trust and
confidence of individuals

Organisations are held accountable for the privacy of personal information

- Individuals expect it
- Public awareness about their privacy rights is increasing
- Privacy stories get big media coverage
- New Zealand has a strong privacy regulator, the Office of the Privacy Commissioner
- Stricter privacy legislation may happen soon

Personal information underpins key stakeholder relationships



- to organisations they **trust**
- sometimes out of **necessity**



Organisations **hold** personal information about their key stakeholders

- clients
- employees
- volunteers
- donors



When stakeholders entrust personal information they have **expectations**

- that their information will be kept **safe**
- about **how their information will be used and what for**

When
organisations and
individuals have
shared
expectations about
personal
information use,
it's win-win

- Shared expectations enable organisations to use personal information to serve stakeholders and achieve organisational objectives and
 - maintain stakeholder trust and confidence
 - support strong, ongoing stakeholder relationships
 - help provide continued access to sustainable, high quality data sources

Poor privacy management can hurt stakeholders

- Embarrassment & humiliation
- Anxiety
- Distress
- Reputational damage
- Financial loss
- Relationship problems
- Physical danger












HOME » NEWS » UK NEWS



Dementia charity warned to take action over data protection failings

An investigation found that Alzheimer's Society used their personal email addresses to share information about people who used the charity



     



The Alzheimer's Society describes itself as "the UK's leading dementia support and research charity".

 The Telegraph  Like Page 4M likes

Latest Video

-  Large rat climbs on sleeping commuter
-  Teen pepper-sprayed at Trump rally

Windows taskbar: 3:32 p.m. 29/03/2017



Privacy failures hurt organisations too...

- Damage to stakeholder relationships
- Stakeholders less likely to engage and share
- May discourage other potential stakeholders
- Office of the Privacy Commissioner investigations
- Settlement payments, damages
- Bad PR
- Clean up costs
- Lost opportunities

Good intentions may still create privacy concerns



- Automatically enrolling service users in a new / different programme
- Sharing details of clients with another organisation who may be able to offer support
- Collecting additional information from other sources to better support stakeholders

Good intentions may still create privacy concerns



- Sharing donor details with another organisation seeking donors
- Creating shared databases for efficiency
- Using volunteer's contact details to seek donations
- Publishing contact details of volunteers / employees so they can be reached outside of regular hours

Good intentions may still create privacy concerns



- Sensitive data
- Fund raising, wealth screening
- Lapsed donors, volunteers
- Data matching
- Direct marketing
- Using publicly available data



Good communications help ensure shared expectations

Shared purposes can be misaligned if...

- Organisation and stakeholder have different views of the shared purpose
- Organisation's view of shared purpose wider than stakeholder's
- Shared purpose out of date
- Personal information gathered from source other than the stakeholder
- Stakeholder's circumstances have changed e.g. data gathered in time of necessity / unusual circumstances
- Organisational change of direction
- Governance / compliance failure – information used for different purpose by mistake e.g. volunteers / new employees not aware of what information to be used for

Managing privacy with good communications

- Every stakeholder communication provides an opportunity to align expectations
- Most important time is when collecting personal information
 - e.g. phone call, form, online
 - Build privacy statements into these information collection points
- Use a privacy policy to pull it all together
 - Easier for your stakeholders
 - Provides clarity for organisation as well

You need to advise individuals

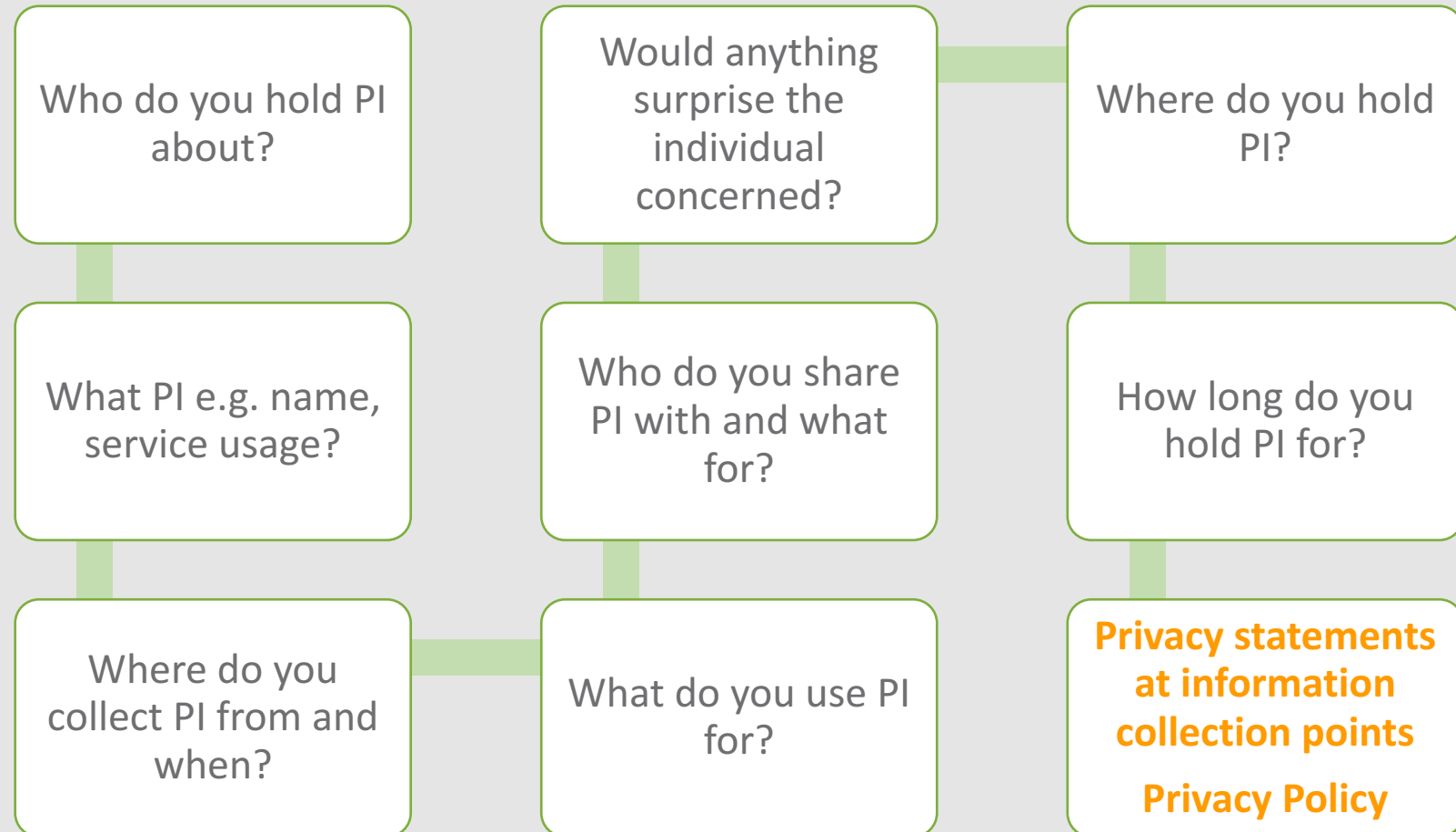
- What personal information you're collecting
- Why you're collecting the information i.e. what you will use the information for
- Whether the individual needs to provide the information – and what will happen if they don't
- Who you will share the information with, and why
- Where you will hold the information and how long you will hold it for
- That the individual can request access to their information, and request correction of any incorrect information (include contact details / process)



Personal information mapping and privacy policies

Mapping information collection and use makes it easy to build privacy into communications

“PI” is
personal
information



Who do you hold Personal information about? e.g. Employees, Volunteers, Board Members, Donors, Service Users / Clients, Website visitors	What Personal information do you hold e.g. name, address. Service usage	Where do you collect PI from, and when? e.g. from client when they sign up for service online, from client’s GP, from website when donor makes an online donation	What do you use Personal Information for?	Who do you share Personal Information with and what for?	Is there anything about the use / sharing of the Personal Information that might surprise the individual whom the information is about?	Where do you hold Personal Information	How long do you hold Personal Information for?	Is it addressed in privacy statements for information collection points?	Is it addressed in privacy policy?
Clients	Name	Client	Health mentoring services	Workouts Ltd - gym discounts	No	Held by Health Services Org	For 2 yrs after services provided		
	Phone number	Client	Health mentoring services	Workouts Ltd - gym discounts	No	Held by Health Services Org	For 2 yrs after services provided		
	Email	Client	Health mentoring services		No	Held by Health Services Org	For 2 yrs after services provided		
	Weight	Client	Health mentoring services		No	Held by Health Services Org	For 2 yrs after services provided		
	Blood pressure	Client’s GP	Health mentoring services		No	Held by Health Services Org	For 2 yrs after services provided		
	Medication	Client’s GP	Health mentoring services		No	Held by Health Services Org	For 2 yrs after services provided		
	Client’s health goals	Client	Health mentoring services		No	Held by Health Services Org	For 2 yrs after services provided		
Volunteers	Name	Volunteer	Organise volunteer roster		No	Held by Health Services Org	For 1 yr after volunteer finishes		
	Phone number	Volunteer	Organise volunteer roster		No	Held by Health Services Org	For 1 yr after volunteer finishes		
	Email	Volunteer	Organise volunteer roster		No	Held by Health Services Org	For 1 yr after volunteer finishes		
	Skills	Volunteer	Organise volunteer roster		No	Held by Health Services Org	For 1 yr after volunteer finishes		
	Availability & max hours per month	Volunteer	Organise volunteer roster		No	Held by Health Services Org	Deleted end of each month		

Creating privacy statements & policies

- Simple
- Transparent
- Plain English
- Align with organisational values, culture and communications style
- Can be informal and friendly in tone and style
- You may have several privacy policies e.g. a website privacy policy, and separate policies for clients and volunteers

Creating privacy statements & policies

- **Be specific**

- We collect information about you to provide you with our services.



- We collect your name and contact details, together with information about your weight and health goals to provide you with health mentoring services.



- With your consent we will collect information about your blood pressure and any medication you are on from your GP to assist with the provision of our health mentoring service. If you consent to this please provide the name and address of your GP below.

Creating privacy statements & policies

- **Don't share information unnecessarily**
- **Don't overstate data use / sharing**
 - Health Services Org collects client name, address, phone number, weight, blood pressure and medication details
 - With client consent, Health Services Org shares information with the local gym, WorkOuts Ltd who like to offer Health Services Org clients a discounted gym membership
- With your consent we share **all of your all personal information** with WorkOuts Ltd
- With your consent, we share **your name and phone number** with WorkOuts Ltd so that they can contact you to offer you a discounted gym membership



Implementing your privacy comms

- Make it accessible to individuals
- Socialise it with all staff, volunteers and agents
- Highlight why it's important, including impact for individuals and organisation if not followed
- Keep refreshing the message so it stays top of mind internally
- Keep it prominent
- Update for new data, new data collection points, uses etc
- Set up processes for complaints, and information & correction requests
- Complaints provide information to update processes / policies



Before you send your next comms

Comms checklist

- Does the communication include personal information about anyone?
 - If yes, have they given consent?
 - If yes – might they still be surprised or concerned?
 - Does the information need to be disclosed in an identifiable way?
- Comms audience / recipients
 - What's the intent of the comms – have the recipients consented for their information to be used to receive comms of this type?
 - Have they agreed for these particular contact details (e.g. email address) to be used for this purpose?

Comms checklist

- Are you requesting more information from recipient?
 - If yes, have you advised
 - What information will be used for
 - Who will be able to access the information
 - Where it will be stored and for how long
 - Of their right to request access and correction
- Are contact details and consents current – reasonable to assume accurate?
- Ability to opt-out of future comms?
- Emails -
 - use bc (blind copy), not cc (copy all)
 - Ensure correct attachments

Comms checklist

- Snail mail – are envelope and address window discrete enough given the nature of the communication?
- Outbound calling
 - phone line may be shared with others – verify who you are speaking to
 - do not call registers
 - take care to identify you are speaking with intended recipient before sharing personal information or providing message for recipient



You've had a privacy breach

Stem, assess, mitigate

1. Stem the breach as far as possible
2. Understand what data has been accessed / released and who is affected
3. Identify possible impact to those affected
 - None
 - Embarrassment
 - Reputational damage
 - Financial harm
 - Physical danger
4. What can be done to mitigate any impact?
 - Can they take steps to mitigate possible harm?
 - Would advising them cause unnecessary distress?

Significant breach

- e.g. large # of people impacted, or if the impact to individuals could be serious
- Consider seeking professional assistance.
- Tapping quickly into subject matter expertise can help reduce the harm to individuals, help your organisation recover more quickly and reduce chance of future breaches.
- While breach reporting is not mandatory in New Zealand currently, engagement with the Office of the Privacy Commissioner on a confidential basis can be extremely helpful in identifying best steps to remedy, and gaining from the benefits of expertise and experience.

Recap

- Aim to establish a shared purpose between your organisation and your stakeholders for use of personal information
- Consider whether stakeholders might be surprised / upset by the way their information is used
- Map out information that your organisation collects to enable informed communications to stakeholders about personal information use
- Ensure everyone in your organisation understands and applies your privacy policy



Questions

- Burning issues
- Any other questions

