Notifiable Data Breaches Scheme

Joanne O'Brien
CRH Law
Level 7, 193 North Quay
Brisbane Qld 4000

P: 07 3236 2900
E:jobrien@crhlaw.com.au

Key Points

- Amendment to the *Privacy Act 1988 (Cth)*
- Applies to *entities* that have obligations under the *Privacy Act*
  - Turnover greater than $3M
  - Health Service Provider that holds health information about individuals
- Commences 22 February 2018
- Mandatory notification of *Eligible Data Breaches*
- There are exceptions

Context

- Strengthen protection of personal information
- Increasing activity by cyber criminals
  - hackers and scammers
  - Ransom demands
- Community concerns about identity theft and privacy
- Transparency & confidence

What is the NDB Scheme

- Obligations for notifying affected individuals & Australian Information Commissioner about data breaches likely to result in serious harm

Eligible Data Breach

- Occurs when:
  1. Unauthorised access to, or unauthorised disclosure of personal information or a loss of personal information;
  2. Likely to result in serious harm to 1 or more individuals; and
  3. Not been able to prevent the likely serious risk with remedial action

What is Serious Harm?

- Can be psychological, emotional, physical, reputational, or other forms of harm
- Requires an objective assessment from perspective of a reasonable person in the entity's position
- Relevant matters listed in s.26WG

Serious Harm – Relevant Matters

What would the reasonable person think taking into account:

- Sensitivity of the information;
- Number of security measures protecting the information;
- Person or kinds of persons who have obtained the information;
- Whether those persons could circumvent security technology;
- Nature of the harm; and
- Other relevant matters

Serious Harm Checklist

1. Type/s information accessed or lost
2. Circumstances of the breach
3. Nature of the harm that could result

Exception – Remedial Action

- If there has been a breach and action is taken before access to, or disclosure of information causes serious harm; &
- As result reasonable person not likely to think there would be serious harm

Example

- You operate a Home Care service
- Carers are issued with mobile devices that enable them to access client information - care plans, budgets
- Carer leaves a device at a coffee shop during lunch break
- Realises when she gets back to her car but it is taken from the coffee shop
- She immediately reports the device as lost
- IT remotely delete all information on the device within 1 hour of report

Suspected Data Breach

- Suspect a data breach that may result in serious harm
- Max 30 days to conduct assessment
- Must be ‘reasonable’ & ‘expeditious’
- For the entity to decide what process to use for assessment

CHECK IT
DON’T CHANCE IT

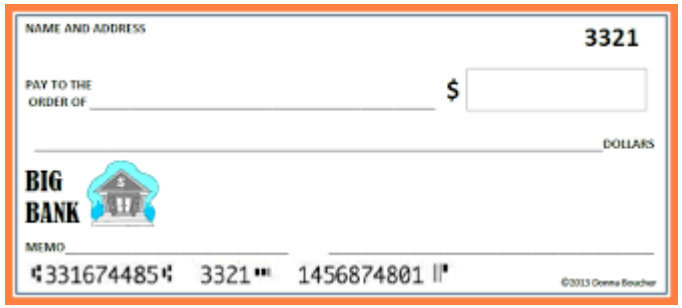
Assessment

OAIC suggests 3 steps

1. Initiate – decide whether assessment is necessary
2. Investigate
   - Quickly;
   - Who may have had access;
   - What information is affected; and
   - Likely impact
3. Evaluate – is it an eligible data breach

Example

- Residential care facility
- IT manager reports unusual access to system after running daily checks
- Receptionist logged into accounts system at 3.00am
- You speak to the receptionist who confirms it wasn't her but mentions her password is her surname



Exception – Other Entities

- Cloud provider suspects breach & conducts assessment
- The breach relates to information you collected
- No requirement for you to conduct assessment

Who to Notify

1. Australian Information Commissioner; and
2. Any individuals at likely risk of serious harm

Notification to Commissioner

- In the form of a statement that includes:
  - Your organisation's identity and contact details
  - Description of the eligible date breach
  - Type of information involved
  - What steps you recommend that individuals take in response to the breach
- There will be an electronic form
  - Notifiable Data Breach Form

Notification to Individuals

As soon as practicable after completion of the statement to the AIC

Contents of the statement to be:

a. Given to all individuals whose information involved;
b. Given to only individuals at likely risk of serous harm; or
c. Published on entity's website & publicised

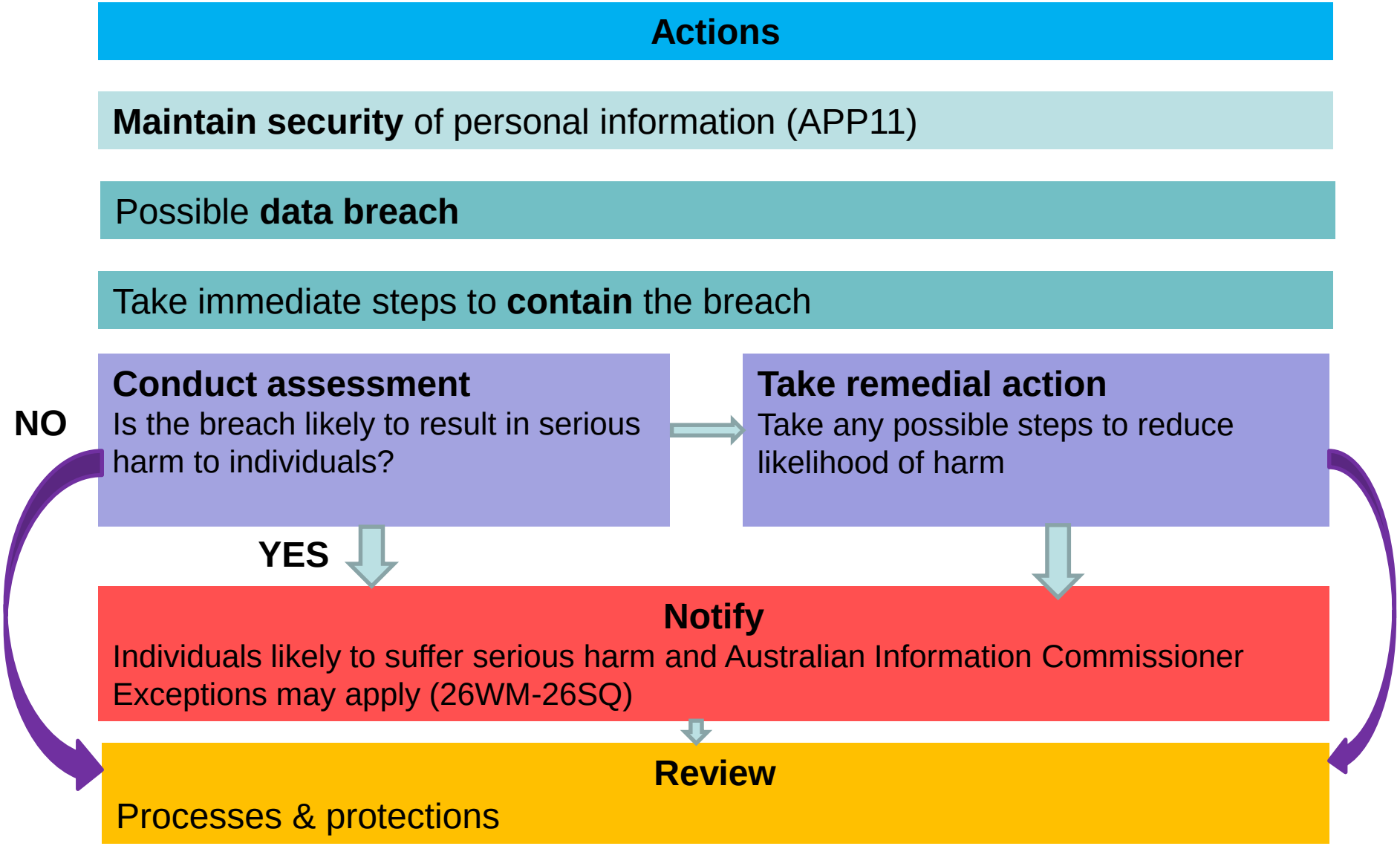
Timing

The Commissioner

- As soon as practicable after becoming aware of reasonable grounds to believe has been a breach

Individuals

- As soon as practicable after completion of the statement for the Commissioner


Actions
Maintain security of personal information (APP11)
Possible data breach
Take immediate steps to contain the breach
Conduct assessment
Is the breach likely to result in serious harm to individuals?
NO
YES
Take remedial action
Take any possible steps to reduce likelihood of harm
Notify
Individuals likely to suffer serious harm and Australian Information Commissioner
Exceptions may apply (26WM-26SQ)
Review
Processes & protections

To Do List

- Review protections in place for personal & health care information
- Review Privacy Policy
- Check arrangements with suppliers, contractors, consultants, community partners
- Prepare a plan for dealing with a data breach
- Cyber security training

QUESTIONS?

CRH Law

JOANNE O'BRIEN
CRH Law
Level 7, 193 North Quay
Brisbane Qld 4000

P: 07 3236 2900
E:jobrien@crhlaw.com.au