Australian Government

Office of the Australian Information Commissioner

7 August 2017

DonateBlood.com.au data breach (Australian Red Cross Blood Service)

Investigation Report

www.oaic.gov.au

Contents

Executive Summary

The Australian Red Cross Blood Service (**Blood Service**) website www.donateblood.com.au allows individuals to book appointments to donate blood.

On 5 September 2016, a database file containing information relating to approximately 550,000 prospective blood donors who had entered their details into the website was saved to a public-facing web server (the **data breach**). The file was inadvertently placed on the web server by an employee of a third-party provider, Precedent Communications Pty Ltd (**Precedent**). The data file was discovered and accessed by an unknown individual on 25 October 2016. On the same day, the individual notified the Blood Service via a number of intermediaries. The Blood Service immediately took steps to contain the breach.

The Blood Service responded on 26 October 2016 and in the following days. It took a number of steps to immediately contain the data breach, including temporarily closing the website. It notified individuals whose personal information was involved and provided assistance to those individuals.

On 27 October 2016, the Australian Information Commissioner (the **Commissioner**) opened a Commissioner initiated investigation into the incident under the *Privacy Act 1988* (Cth) (**Privacy Act**). The Commissioner's decision to open an investigation was made in light of the large number of Australians whose personal information was involved, and the sensitivity of the data. The Commissioner's investigation considered whether the Blood Service had met the requirements of the Privacy Act and whether the Blood Service's information handling practices, procedures and systems may have affected the likelihood and extent of the data breach. The investigation also considered the steps taken by the Blood Service following the incident to mitigate its impact and minimise the chance of reoccurrence. The Commissioner opened a separate investigation into the information handling practices of Precedent.

The root cause of the incident was a one-off human error on the part of a Precedent employee. The data breach occurred without the authorisation or direct involvement of the Blood Service, and was outside the scope of Precedent's contractual obligations to the Blood Service. As such, the Blood Service did not disclose the information in question within the meaning of Australian Privacy Principle (**APP**) 6.

Furthermore, the Blood Service had in place policies and practices to protect personal information as required by APP 11.1, including documented information security policies and regular staff training. Nevertheless, there were two matters within the Blood Service's control that were a contributing factor to the data breach and which constituted breaches of the Privacy Act. In particular, it appears that the incident would not have occurred but for:

- the absence of contractual measures or other reasonable steps on the part of the Blood Service to ensure adequate security measures for personal information held for it by the relevant third party contractor, in breach of APP 11.1
- the retention of data on the Donate Blood website for a longer period than was required, in breach of APP 11.2.

Although the Blood Service had not met all the requirements of the Privacy Act in relation to the data breach, the Commissioner commends the Blood Service for its quick response and handling of the breach. Overall, the Blood Service acted appropriately and in a timely manner to rectify the data breach, and its response to the data breach provides a model of good practice for other organisations.

The circumstances of this incident and the Blood Service's response mean that it is unlikely that there will be adverse consequences for affected individuals. All copies of the database backup have now been

destroyed. The Blood Service has enhanced its information handling practices since the incident. The Commissioner believes the community can have confidence in the Blood Service's commitment to the security of their personal information.

To assure the Commissioner and the Australian community that the Blood Service would continue to address the issues identified in the investigation, the Blood Service offered, and the Commissioner accepted, an enforceable undertaking on 28 July 2017.

Background

The Donate Blood website

The purpose of the Donate Blood website is to:

a. provide information relating to blood donation, types of blood, types of donation, uses of blood and answers to any questions the public may have relating to blood donation

b. provide a way for people to request an appointment to make a donation (individuals can also call the National Contact Centre or make an appointment in person at a Donor Centre).

The website's primary audience is donors and potential donors, with a second layer audience of researchers, media and career seekers. Personal information was entered onto the website by individuals wishing to make appointments and persons acting as co-ordinators for corporate donation groups.[1]

When a person makes an appointment using the website, the website transmits the personal information to Blood Service personnel. Once the Blood Service receives the information, it creates an entry in the Blood Service's internal National Blood Management System (**NBMS**), which records all donations and details of donors. At the time of the incident, information entered by potential donors on the website when making an appointment was also retained on the 'backend' of the Donate Blood website. No procedure was in place to destroy or de-identify this information.

A third party provider, Precedent, managed the Donate Blood website at the time of the data breach. Amazon Web Services hosted the production environment of the website (the live, user-facing version of the website). Non-production environments, including the website's User Acceptance Testing (**UAT**) environment (which was used for testing and seeking approval of changes to the website) were hosted and managed by Precedent directly. The UAT environment included a copy of the live website, including a copy of customer data entered by individuals on the website.

The data breach

The UAT environment contained a copy of all data entered into the production version of the website. The UAT version of the website was protected by Precedent through a number of mechanisms (including password protection). However, portions of the web server on which the UAT environment was located were publicly accessible to any internet user who knew where and how to look.

On 5 September 2016, a Precedent employee created a backup of the UAT database file (the **data file**) on the UAT environment for the Donate Blood website and saved the data file to a publicly accessible portion of the UAT server, instead of the intended secure location.

The data file contained registration information for the 550,000 prospective donors who had made an appointment to donate blood via the website between 2010 and 5 September 2016.

On 25 October 2016, an individual scanning the internet for security vulnerabilities located, accessed, and made a backup of the data file.

[1] The Blood Service's submission to the Office of the Australian Information Commissioner, 5 December 2016, page 3.

The data file contained personal information about approximately 550,000 individuals who had expressed an interest in donating blood on the Donate Blood website. The personal information consisted of all information collected about these individuals via the website, and included contact information and answers to questions about their eligibility to donate blood. Some of the information collected was sensitive and health information.

The categories of personal information collected via the Donate Blood website included:

- identifying particulars: first and last name, gender, date of birth and donor ID (optional)
- contact details: physical address, email address and phone number
- appointment preferences: postcode or suburb for donation, preferred date range request for donation and preferred time of day
- yes or no responses to donor eligibility questions: for example whether or not the prospective donor is taking antibiotics; had engaged in risky sexual behaviour; or if they are or have been pregnant in the last nine months.

Post-incident response

On 25 October 2016, the individual who discovered the vulnerability contacted Troy Hunt, a cybersecurity expert who operates the blog www.troyhunt.com and data breach notification service www.haveibeenpwned.com. Mr Hunt subsequently informed the Australian Cyber Emergency Response Team (**AusCERT**). AusCERT notified the Blood Service on 25 October 2016, and took steps to contain the breach.

After becoming aware of the compromise of the data, AusCERT attempted to contact the Blood Service. As AusCERT did not receive an immediate response from the Blood Service, AusCERT took steps to contain the data breach and undertook to identify and contact the Internet Service Provider (**ISP**) responsible for hosting the UAT environment. The ISP removed access to the UAT environment at approximately 22:45 on 25 October 2016. At that point the data file was no longer accessible.

The Blood Service became aware of the incident on 26 October 2016 and took the following steps to respond to the incident:

- Continued to engage with the Incident Management Service of AusCERT by telephone and in person to assist its response to the incident.
- Confirmed (via AusCERT) that a copy of the data file held by the unknown individual and Mr Hunt were deleted.
- Engaged IDcare, an identity and cyber support service, to undertake an independent risk assessment of the personal information compromised. IDcare assessed the personal information as being of low risk of future direct misuse.
- Notified the public and affected individuals on 28 October 2016 by:
    - issuing press releases confirming that a data breach had occurred, publishing statements on its website and social media sites (Facebook, Twitter and LinkedIn) and establishing a dedicated website, telephone hotline and an email inquiry facility to respond to public enquiries

- sending notice to affected individuals via text message (547,000) and all donors who had donated blood in the previous 3 years via email (630,000). A statement of IDCare's assessment was included in communication to donors.

- Engaged specialist organisations to conduct forensic analysis on the exposed Precedent server, monitor the Donate Blood website for any vulnerabilities or unusual activity and to monitor the dark web for any indication that the data was available or was being traded.

The Blood Service accepted full responsibility for the incident and provided support to affected individuals.

The forensic analysis commissioned by the Blood Service concluded that there were four requests to download the data file on 25 October 2016 from three different IP addresses, but that only one person actually downloaded the relevant file. No other download requests were identified prior to 25 October 2016. The individual has stated that they did not distribute the data file to any person aside from Mr Hunt and that all copies of the data file were subsequently deleted. There is no information to suggest that the data file is in the possession of any unauthorised parties.

Overall, the Blood Service acted appropriately and in a timely manner in response to the data breach. The circumstances of this incident and the Blood Service's response means that it is unlikely that there will be adverse consequences for affected individuals.

Commissioner's investigation

Under s 40(2) of the Privacy Act, the Commissioner may, on the Commissioner's own initiative, investigate an act or practice that may be an interference with privacy.

On 27 October 2016, the Commissioner commenced an investigation into the data breach and surrounding circumstances. The Commissioner considered the Blood Service's information handling practices, procedures and systems that may have affected the likelihood and extent of the data breach and focused on whether the Blood Service took reasonable steps to protect the personal information that it held from misuse and loss and from unauthorised access, modification or disclosure. The investigation also considered the steps taken by the Blood Service following the incident to mitigate the impact of the data breach and minimise the chance of reoccurrence.

Relevant provisions of the Privacy Act

Organisations covered by the Privacy Act must comply with the APPs contained in Schedule 1 of the Privacy Act. The APPs apply to the handling of 'personal information', which the Privacy Act defines as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[2]

APP 6 states that an APP entity must only use or disclose personal information for the primary purpose of its collection, unless it can rely on exceptions described under APP 6.1(a) – (b).

[2] The Privacy Act, s 6.

APP 11.1 states that an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

APP 11.2 states that an organisation must take reasonable steps to destroy or de-identify information it no longer needs for any purpose for which the information may be used or disclosed under the APPs.

Disclosure of personal information (APP 6)

APP 6 regulates the use and disclosure of personal information and states that organisations may only use or disclose personal information for the primary purpose of collection, unless an exception applies.

In general terms, an organisation 'discloses' personal information when it makes the information accessible to others outside the organisation and releases the subsequent handling of the personal information from its effective control. This may include an accidental release or an unauthorised release by an employee.

Findings

The data breach was caused by human error on the part of a Precedent employee. This occurred without the authorisation or direct involvement of the Blood Service, and was outside the scope of Precedent's contractual obligations to the Blood Service. The Blood Service did not disclose the data file, within the meaning of APP 6.

Protection of personal information (APP 11.1)

APP 11.1 in the Privacy Act requires organisations to take such steps as are reasonable in the circumstances to protect personal information its holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

APP 11.1 applies to personal information 'held' by an organisation. Information is held by an organisation where it has physical possession of the data, or the right or power to deal with the information even if it does not physically possess or own the medium on which the information is stored.[3]

A data breach occurring does not necessarily point to a contravention of APP 11. When deciding what steps to take to protect the personal information it holds, the Office of the Australian Information Commissioner (**OAIC**) would expect an organisation to review the nature of the information it holds, and the possible impact on individuals who the information relates to should it be compromised. It is therefore necessary to consider, having regard to the nature of the information and what steps were reasonable in the circumstances, whether the safeguards in place were sufficient.

Similarly, where an organisation outsources its personal information handling, relevant factors in deciding the steps that are reasonable in those circumstances include whether the organisation has:

- conducted appropriate due diligence on the services to be provided
- considered the scope of the personal information handling services to be provided
- considered what security controls and personal information handling measures the third party provider is expected to use
- included terms in the contract to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements.[4]

Protection of personal information by the Blood Service

The Blood Service provided the OAIC with an outline of the physical, technological and organisational measures it had in place at the time of the data breach. These included:

- **Physical safeguards:** controls on entry to its premises and restricted areas inside the premises. Hardcopy Donor Questionnaire forms and donor legal declarations (filled out at the Donor Centre) are held in sealed bags at a processing centre and after 6 months, are transferred to an off-site secure storage facility in boxes sealed by the Blood Service.
- **Technological safeguards:** network protections included firewalls, anti-virus and anti-malware installed on servers, web and email monitoring on internet and email gateways, use of data loss

[3] See APP Guidelines, paragraphs [11.4]-[11.6].

[4] OAIC *Guide to securing personal information*, January 2015, page 33. Available online at https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

prevention and vulnerability scanning tools. Biennial penetration and intrusion tests were also conducted, the most recent being completed in April 2016.

- **Organisational safeguards:** all staff must complete online privacy training every two years. Staff who mail and receive calls from existing and potential blood donors undertake specific privacy training, and information security awareness training is completed by all employees during employment. The Blood Service also has an *Information Security Policy* and various supporting policies and procedures including a password policy and a secure file sending policy.

Under its Deed of Agreement with the National Blood Authority, the Blood Service had recently completed an *Information Asset Classification Policy*, which provides that where data contains sensitive information (as defined in the Privacy Act), the information is classified as 'restricted', which requires strict control over access and management. However this policy was not in place at the time of the data breach.

The Blood Service has also advised that it has a documented risk management framework developed to identify risks in projects at the initiation stage. The framework provides for the Blood Service to identify risks: as an aspect of the sourcing strategy; for subsequent inclusion in the business requirements for a project; and to form appropriate contract terms. The Blood Service advised that sign off for sourcing strategy is the responsibility of the Executive Director of the relevant division.

The Blood Service has submitted that part of its risk management framework requires responsible staff members to complete a Privacy Impact Assessment (**PIA**) and consult with the Chief Privacy Officer and the Information and Communications Technology division if the project involves the handling of personal information. However, the Blood Service advises that it launched the Donate Blood website prior to the introduction of this PIA process in 2012.

While some of these measures did not apply in the specific circumstances of the data breach, it appears that the Blood Service has a security framework in place that includes documented information security policies, regular staff training and a consideration of risk management regarding the handling of personal and sensitive information about individuals.

Management of the Donate Blood website

The marketing team within the Blood Service was responsible for the management of the Precedent contract and services provided. The 2014 Agreements in place between the Blood Service and Precedent contained some provisions requiring Precedent to have security arrangements in place to handle Blood Service information.

The *Service Agreement* between the Blood Service and Precedent signed 18 September 2014 included the requirement that:

> The Supplier will comply with, and will ensure that its Personnel comply with, any policies or procedures notified by the Blood Service to the Supplier from time to time, including without limitation any policies relating to privacy, security, computer resources, Occupational Health & Safety and code of Good Manufacturing Practice (GMP) Awareness Training, where applicable.

The *Confidentiality Agreement* between the Blood Service and Precedent signed 18 September 2014 included the requirement that:

> The Recipient must protect all Confidential Information from unauthorised access or use, and must take and enforce proper and adequate precautions at all times to preserve the secrecy and the confidentiality of all Confidential Information.

> If the Recipient… breaches or is likely to breach any obligation or confidentiality arising under this Agreement, the Recipient must take reasonable steps to limit the consequences of that breach and to prevent any further breach.

'Confidential Information' included information relating to each of the parties' computer systems, clients, suppliers, business and affairs and information that is developed or gained through providing the services.

Findings

The Blood Service did not physically hold the personal information in the data file, as it was stored on systems operated by Precedent. However, the nature of the contractual relationship between the Blood Service and Precedent was such that the Blood Service retained effective ownership of the data. Given this, the data was held by both the Blood Service and Precedent, and both organisations have obligations under APP 11.1 to protect the information.

The personal information held by the Blood Service concerned donors' and prospective donors' health information. Some of the questions and answers contained in the compromised data included information of a sensitive nature, such as whether individuals had engaged in high-risk sexual activity. There was a foreseeable risk of adverse consequences to individuals if this information was subject to unauthorised disclosure. This is relevant in considering the degree to which the Blood Service should secure the personal information it holds.

While the Blood Service's personal information protections were strong in general, there were some issues with the manner in which it protected personal information held by third party providers.

It does not appear that the Blood Service assessed the adequacy of Precedent's security measures and practices when it made the decision to award Precedent the contract for the development and application support, ongoing management, consulting and testing, maintenance and upgrade of the Donate Blood website in 2015.

The contractual arrangements between the Blood Service and Precedent focused on service level agreements and were absent control measures to mitigate the corresponding risks of a third party provider. The Blood Service's requirements of Precedent in relation to information security were not clearly articulated or proportional to the scale and sensitivity of the information held by the Blood Service and Precedent. A reasonable step in the circumstances may have been to include specific contractual requirements for how Precedent would handle and store the personal information of blood donors on the Donate Blood website, and a reporting mechanism for the Blood Service to ensure these contractual requirements were being met.

The Blood Service failed to implement the appropriate contractual requirements or control measures in order to protect personal information that is handled by a third party provider.

Although its personal information handling practices were for the most part effective, the Blood Service did not take reasonable steps to protect the personal information held on the Donate Blood website, in contravention of APP 11.1.

Retention of personal information (APP 11.2)

APP 11.2 states that an organisation must take reasonable steps to destroy or de-identify information it no longer needs for any purpose for which the information may be used or disclosed under the APPs.

To meet its obligations under APP 11.2, an organisation should develop systems or procedures to identify information the organisation no longer needs and destroy or de-identify this information. It will generally not be appropriate for personal information to be retained indefinitely.

Practices at the time of the data breach

At the time of the incident, when an appointment was created by a prospective donor on the Donate Blood website, an email containing the information was immediately sent to Blood Service staff. The Blood Service staff used the information to create a profile in the NBMS, and to contact potential donors if there was an issue with the donor's ability to donate blood. Once the information was entered into the NBMS by the Blood Service staff, information entered by potential donors remained on the 'backend' of the website as a backup.

Donor and prospective donor information held in the NBMS is collected from the information provided by individuals via the Donate Blood website and in centre, when donors fill out the Donor Questionnaire. The Blood Service's *Records Retention and Disposal Authority and Records Management Policy* outlines the data retention framework at the Blood Service and also refers to specific minimum retention requirements and retention schedules for different record types, noting that the retention period may be extended if there is a business requirement to do so.

The Blood Service advised that the retention periods specified in the policy documents are to:

- fulfil safety requirements including tracing donors and recipients in the event of a blood borne disease, and
- ensure that the quality of the blood supply where donor responses to eligibility questions change.

However, the data retention policy did not extend to the information stored on the Donate Blood website. The Blood Service states that '[t]here was no process in place at the time of the incident for reviewing the information maintained on the backend of the website and how long it should be held'.[5]

Findings

The information collected via the Donate Blood website was gathered for the primary purpose of providing information to the public and to allow existing and potential donors to book an appointment. After a period of time, following the transmission of this information to the Blood Service Marketing and National Call Centre and its input into the NBMS, the personal information is no longer needed for that purpose, or any other function or activity of the Blood Service. As there appears to be no reason for historical data to be retained on the Donate Blood website database indefinitely, the information should be destroyed or de-identified after a defined period. The retention of the data on the Donate Blood website back end was a contributing factor to the data breach.

[5] The Blood Service's submission to the Office of the Australian Information Commissioner, 5 December 2016, page 4.

The Blood Service failed to take reasonable steps to destroy or permanently de-identify personal information it held that was no longer in use or needed, in contravention of APP 11.2.

Changes to information handling practices

After the data breach, the Blood Service conducted a review of its information handling practices and put in place changes to enhance those practices. These steps included:

- destroying all historical data from the Donate Blood website database
- deleting the personal information collected through the website every fortnight
- developing and implementing a *Third Party Management Policy* and *Third Party Management Standard Operating Procedure* to monitor third party providers' compliance with appropriate privacy and data security practices and procedures
- updating its template contractual terms for the acquisition of products and services to include comprehensive data security and privacy requirements
- amending its procurement process so that a PIA is completed prior to negotiation of any significant contract to ensure that privacy and data sharing are considered and appropriate protections are in place
- accelerating and expanding a review of its information and technology services
- engaging external consultants to review its incident management response and data security governance, processes and systems, with a view to identifying areas of improvement and strategies to implement these improvements
- limiting the personal information collected via the Donate Blood website as all eligibility questions are now grouped at the end of the questionnaire and there is a statement that an individual will be referred to the contact centre should they respond 'yes' to any of the grouped questions. The maximum information collected via the website is name, donor ID number, date of birth, address, phone number, email address, and gender.

Conclusion

The data breach occurred without the authorisation or direct involvement of the Blood Service, and was outside the scope of Precedent's contractual obligations to the Blood Service. There was no 'disclosure' by the Blood Service of the data file within the meaning of APP 6.

The steps the Blood Service had in place to protect personal information at the time of the breach were, for the most part, adequate. However, the Blood Service breached APP 11 in respect of the information on the Donate Blood website by retaining the information indefinitely, and by not having appropriate measures in place to protect information concurrently held by third party contractors.

Nonetheless, the Commissioner commends the Blood Service for its response following the incident. The Blood Service responded quickly and effectively when it was notified of the data breach, and worked swiftly to implement steps to mitigate against future data breaches of this nature. The Commissioner acknowledges the substantial work done by the Blood Service to communicate with the community in a transparent manner, assist individuals concerned about the incident, and to further protect donor information since this incident. The Commissioner believes the community can have confidence in the Blood Service's commitment to the security of their personal information.

The Commissioner is satisfied that the steps taken by the Blood Service are appropriate to rectify the data breach. The Commissioner has accepted an enforceable undertaking from the Blood Service formalising its commitment to review certain measures within a specific timeframe. The Commissioner considers this an appropriate conclusion to the investigation.