3 September 2015

PRIVACY INCIDENT REPORT

INCIDENT

The Department of Immigration and Border Protection (the Department) contracts Bupa Australia Health Pty Ltd (Bupa) to provide immigration health assessment and medical services.

The Department's Bupa Contract Manager was advised on 8 August 2015 of a disclosure of personal and sensitive information contained in a Microsoft Excel spreadsheet by a Sonic HealthPlus (SHP) employee on 7 August 2015. SHP is a subcontractor of Bupa who deliver immigration medical services and health checks on behalf of the Department.

The information was disclosed in the course of a Microsoft Excel spreadsheet being emailed in error to an unknown email address.

BACKGROUND

Under the Contract between the Department and Bupa (the Bupa Contract) Key Performance Indicators (KPIs) are specified which determine the application of yearly price increases.

The purpose of one KPI measurement is to encourage prompt client services by measuring processing times at individual Bupa medical centres. This KPI measures the time from when a client attends a Bupa clinic to commence their health examination to when the results are finalised and submitted. In order for Bupa to meet this KPI threshold, Bupa must ensure timely delivery of services, including those delivered by Bupa's subcontractors.

SHP had been sending to Bupa regular Status Reports in the form of Excel spreadsheets with eMedical case details, to identify and ensure cases were completed in a timely manner, including notes around any delays. The Department was not aware of these Excel spreadsheets being created until the privacy breach

occurred, as the health processing portal and eMedical systems are the only protected systems authorised to be used by the Department's medical contractors.

DETAILS

The SHP employee usually charged with the preparation of the Status Report was due to commence planned Annual Leave on 6 August 2015. On the same day, an SHP temporary employee was provided training on the process, in order to undertake the work from 7 August 2015.

On 7 August 2015, the SHP temporary employee prepared a daily Status Report by extracting data from eMedical without the Department's authority or endorsement. The SHP temporary employee sent the Status Report to the SHP clinical staff member using a personal email address, as they had not been allocated an official SHP email address.

The SHP clinical staff member emailed the Status Report onwards to relevant SHP internal stakeholders and the Bupa Provider Liaison Manager. The SHP clinical staff member also intended to blind carbon copy the SHP temporary employee into the email, however mistyped the email address. As a result, the email was inadvertently sent to another email address.

A few hours later, the SHP clinical staff member drafted an unrelated email, noting that a previously unfamiliar email address appeared in the address line while typing. The SHP clinical staff member then realised the error and that the previous email was also sent to the same erroneous email address.

EXTENT OF BREACH

As an 'undeliverable mail' notification was not received from the erroneous email address, it was deduced that the Status Report was sent to a valid email address, the identity of the account owner being unknown.

The Status Report contained personal information relating to 317 immigration medical clients, including:

- full name;
- date of birth;
- passport number;
- visa type;
- visa subclass;
- clinic location;
- Health Assessment Portal (HAP) ID;
- scheduled medical examination date;

- medical examination code / type (eMedical); and
- brief notes, summaries and comments about the status of the medical tests being conducted.

No actual personal client medical records were sent.

RESPONSE TO INCIDENT

7 August 2015

- The SHP clinical staff member, upon realisation of the error, attempted to recall the email with no success. The SHP clinical staff member escalated the issue to the SHP Clinical Lead, with further attempts made to recall the email proving unsuccessful.
- The SHP Clinical Lead escalated the incident to:
    - SHP Operations Manager;
    - SHP General Manager (Clinical Governance);
    - SHP General Manager (Technology and Systems);
    - SHP Special Projects Manager; and
    - SHP General Manager (Business Development and Marketing).
- The SHP General Manager (Technology and Systems) made several additional attempts to recall the email from the SHP email server. These attempts were also unsuccessful.
- SHP referred the incident to the Bupa Commercial and Contracts Manager, also advising that SHP had exhausted all technological avenues to recall the email.

8 – 10 August 2015

- Bupa sent two additional emails to the mistyped email address requesting the recipient to contact Bupa to confirm deletion of the email. To date, no response has been received and deletion of the email has not been confirmed.
- The Bupa Commercial and Contracts Manager referred the incident via email to the Director, Immigration Health Services and the Department's Bupa Contract Manager,.

11 August 2015

- Following a request from the Department's Contract Manager, the Bupa Contracts Manager sent the following email to the erroneous email address:

> To whom it may concern,
>
> On Friday 7/8/15 an email was sent to this gmail account in error. We kindly request that you undertake the following actions;
>
> - If the email has not yet been read, please delete the email immediately
> - If the email has been read, please delete the email and any copies immediately
>
> Thank you in anticipation.

- The Immigration Health Services Section prepared Media Talking Points and a Hot Issues Brief for the Communications and Media Branch in anticipation of briefing the Minister for Immigration and Border Protection, and relevant Senior Executive Service Officers within the Department.

Internal Consultation

- The Immigration Health Services Section referred the incident to the following areas within the Department for advice and appropriate action:
    - Information Access Capability Section;
    - Information and Data Policy Section;
    - Integrity and Professional Standards Branch;
    - Commercial Legal Section;
    - External Accountability Section; and
    - Cyber Operations Section.

13 August 2015

- The Information Access Capability Section provided their advice, recommending various courses of remedial action, including notification of the incident to the Office of the Australian Information Commissioner (OAIC).
- Bupa provided the Department with copies of the formal incident report and the erroneously disseminated report

17 August 2015

- The Department's Cyber Security Section advised that after some investigative work, no further action, that had not already been explored could be taken to identify the unintended recipient of the email.

28 August 2015

- The Department's Chief Medical Officer issued a letter to the Managing Director of Bupa, advising that the Department considers that Bupa has failed to comply with its obligations under clause 28 of the Bupa Contract relating to Privacy.
- Bupa was also advised of its obligations under Part 6 of the *Australian Border Force Act 2015* which outlines information secrecy and disclosure provisions applicable to 'entrusted persons', defined to include contractors and service providers whose work relates to immigration, customs and border protection.
- Bupa have been given a 14 business day timeframe to provide further information to the regarding circumstances that led Bupa and SHP to create email reports outside of the authorised departmental health systems. Bupa were also advised that the Department required an immediate review of all security of information policies and procedures within Bupa and their subcontractors.

3 September 2015

- This report was prepared and cleared by the External Accountability Section and the Immmigration Health Services Section for the purposes of reporting the incident to the Office of the Australian Information Commissioner for their consideration.

ADDITIONAL REMEDIAL ACTION

- Bupa have undertaken to review SHP protocols and practices for allowing information to be disseminated using a non-official SHP email address.
- The Bupa Contract Manager and Bupa Quality Assurance Manager are currently managing the incident and have instructed SHP to cease future distribution of the Status Report.
- The Department's Bupa Contract Manager raised with Bupa the need for more timely escalation of issues with details, in line with agreed communication protocols between Bupa and the Department.
- The Department's Contract Manager is currently liaising with the Commercial Legal Section to manage to the implications of standing arrangements under the contract between Bupa and the Department.
- The Immigration Health Services Section and External Accountability Section are currently managing a strategy within which to notify the individuals affected by the incident. The External Accountability Section intends to keep the Office of the Australian Information Commissioner informed and updated in relation to the notification process.

- The Department's Bupa Contract Manager will be conducting a review into the transmission of client information outside of the Department's authorised IT systems, and the possible action under the terms of the Contract with Bupa.

INCIDENT REPORT CLEARED BY:

Name: s. 22(1)(a)(ii)
Position: Manager, External Accountability Section
Date: 3 September 2015

Name: s. 22(1)(a)(ii)
Position: Director, Immigration Health Services Section
Date: 3 September 2015

Name: s. 22(1)(a)(ii)
Position: A/g Assistant Director (Bupa Contract Manager)
Immigration Health Services Section
Date: 3 September 2015

Australian Government
Department of Immigration and Border Protection

6 October 2015

OAIC Reference: DBN15/00073
DIBP Reference: OHR-15-00343

Notification of Privacy Breach: Sonic HealthPlus
RESPONSE TO FURTHER QUESTIONS

1. **Whether DIBP has notified or intends to notify affected clients and if not, the factors it has considered in coming to that conclusion. I note that notification is most effective when it is timely and provides sufficient information to enable affected individuals to take mitigating action.**

It is the Department's intention to notify the individuals affected by the data breach. A notification letter template has been co-drafted by the Immigration Health Services Section and External Accountability Section which is to be signed off by the Department's Chief Medical Officer. This template has been cleared through the Civil Litigation and Compensation Section and Comcover, the Department's general insurer.

On 17 September 2015, the Head of Legal at Bupa contacted Google Australia's General Counsel in relation to the data breach. Google advised that:

- The email was temporarily removed from the recipient's inbox;
- The individual was notified that a request was made to remove access to the email;
- The recipient would have 20 days to object to the removal of the email; and
- In the event that no objection is received within 20 days, the email would be permanently deleted.

A response is expected from Google in the week commencing 12 October 2015.
Work has already progressed in collating the contact details of each affected individual so the notification process is expedited once this response has been received from Google.

2. **Information about Bupa's review of its and SHP's security policies and procedures including the transmission of client information outside of DIBP's authorised IT systems**

On 28 August 2015, the Assistant Secretary of the Department's Immigration Health Branch sent a formal notice to the Managing Director of Bupa Visa Medical Services (BVMS) in response to the Sonic HealthPlus Privacy Breach. The notice requested that Bupa provide the following information:

1. Provide further information to the Department regarding circumstances that led Bupa and Sonic HealthPlus to create email reports outside of the authorised departmental health systems.
2. Bupa to undertake an immediate review of all security of information policies and procedures within Bupa and their subcontractors
3. Bupa to demonstrate to the satisfaction of the Department that Bupa and its subcontractors have sufficient systems in place to prevent future breaches of clause 28, including ensuring the elimination of work practices that may lead to further unauthorised disclosures of personal information.

Bupa subsequently engaged an external party to undertake the review of the policies and procedures relating to security of personal information handled by BVMS and all of their subcontractors, including Sonic HealthPlus. Information was obtained from all but three of Bupa's subcontractors and a report detailing the investigation was provided to DIBP by Bupa on 16 September 2015.

As three of Bupa's independent providers did not provide Bupa with the requested information, the report submitted to DIBP by Bupa was deemed incomplete. DIBP provided Bupa with an extension of time to obtain the information from the three providers and Bupa was requested to submit an updated report by 9 October 2015. To date an updated report has not been submitted to DIBP.

3. Any further developments regarding DIBP and Bupa's contractual arrangements.

The department's contractual arrangements concerning Bupa will be reviewed following receipt of the updated report detailing the review of the policies and procedures relating to security of personal information handled by BVMS and all of their subcontractors, including Sonic HealthPlus.

From: External Scrutiny
To: s. 22(1)(a)
Cc: s. 22(1)(a)(ii) ; External Scrutiny
Subject: RE: DBN15/00073 - DIBP Notification of Privacy Breach (Sonic HealthPlus) [DLM=For-Official-Use-Only]
Date: Tuesday, 20 October 2015 2:49:35 PM

For-Official-Use-Only

Hi s. 22(1)(a)(ii)

Thanks for the phone conversation earlier today.

As discussed, please find below the webpage on the Migration Alliance website:

http://migrationalliance.com.au/immigration-daily-news/entry/2015-10-dibp-indadvertently-disclose-a-client-s-sensitive-personal-information.html

As advised, and contrary to their concerns, we can confirm that the PDF attached to the webpage was in fact the notification to affected individuals that the Department disseminated, and not a scam as they fear it to be. Furthermore, the Department is preparing a formal response to the five (5) questions posed by the concerned registered migration agent, through Migration Alliance.

This information is provided to you in the event that the affected individuals or their representatives contact the OAIC in relation to the information contained in the above webpage.

As always, if you have any further issues, please do not hesitate to contact us through this mailbox.

Kind regards

s. 22(1)(a)(ii)
Privacy Officer | External Accountability Section
Risk and Assurance Branch | Integrity, Security and Assurance Division
Corporate Group
Department of Immigration and Border Protection
P: (02) 6264 s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @border.gov.au
E: s. 22(1)(a)(ii) @border.gov.au

For-Official-Use-Only

From: s. 22(1)(a)(ii) [mailto s. 22(1)(a)(ii) @oaic.gov.au]
Sent: Tuesday, 6 October 2015 12:55 PM
To: External Accountability
Cc: s. 22(1)(a)(ii) ; Privacy
Subject: RE: DBN15/00073 - DIBP Notification of Privacy Breach (Sonic HealthPlus) [DLM=For-Official-Use-Only]

Thanks for the response s. 22(1)(a)(ii) I'll be in touch if we require any further information.

Regards,

s. 22(1)(a)(ii) I Adviser I Privacy Practice, Advice and Technology
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY NSW 2001 | www.oaic.gov.au
+61 2 s. 22(1)(a)(ii) | s. 22(1)(a)(ii) @oaic.gov.au

From: External Accountability [mailto:s. 22(1)(a)(ii) @border.gov.au]
Sent: Tuesday, 6 October 2015 12:50 PM
To: s. 22(1)(a)(ii)
Cc: s. 22(1)(a)(ii) ; Privacy
Subject: RE: DBN15/00073 - DIBP Notification of Privacy Breach (Sonic HealthPlus) [DLM=For-Official-Use-Only]

For-Official-Use-Only

Dear s. 22(1)(a)(ii)

Please find attached a copy of the Department's Response to the OAIC's request for further information in relation to the disclosure of personal information by Sonic HealthPlus, one of the Department's sub-contracted service providers.

Please do not hesitate to contact us should you have any further queries or concerns.

Kind regards

s. 22(1)(a)(ii)
Privacy Officer | External Accountability Section
Risk and Assurance Branch | Integrity, Security and Assurance Division
Corporate Group
Department of Immigration and Border Protection
P: (02) s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @border.gov.au

For-Official-Use-Only

From: s. 22(1)(a)(ii) [mailto:s. 22(1)(a)(ii) @oaic.gov.au]
Sent: Monday, 21 September 2015 1:44 PM
To: External Accountability
Cc: s. 22(1)(a)(ii) ; Privacy
Subject: RE: DBN15/00073 - DIBP Notification of Privacy Breach (Sonic HealthPlus) [DLM=For-Official-Use-Only]

Dear s. 22(1)(a)(ii)

Thank you for your email of 3 September 2015 advising the Office of the Australian Information Commissioner of a data breach incident in which the Department of Immigration and Border Protection (DIBP) and a sub-contracted service provider, Sonic Health Plus (SHP), disclosed clients' personal information by sending a spreadsheet containing their information to an incorrect email address in error (our reference: DBN15/00073).

The data breach

You advise that DIBP contracts Bupa Australia Health Pty Ltd (Bupa) to provide immigration health assessment and medical services, and Bupa sub-contracts to SHP to deliver these services. You advise that as a result of Bupa being required to meet key performance indicators, SHP had been sending Bupa regular status reports about the progress of the cases it was processing. You advise that DIBP had not been aware of this practice prior to the incident occurring.

You advise that on 7 August 2015, a temporary SHP employee used their personal email address

to send the daily status report to a SHP clinical employee. The SHP clinical employee subsequently mistyped the temporary SHP employee's email address in the blind carbon copy field when emailing the report to other SHP staff, which resulted in the report being sent to an unknown external email address. The report contained the personal information for 317 immigration clients including their identity details, visa information, health assessment portal ID, scheduled medical examination date and brief notes about the status of the medical tests being conducted. However, none of the clients' medical records were included.

Remedial steps

You advise that in response to this incident:

- SHP has attempted to recall the email without success
- Bupa has sent emails to the recipient email address requesting the owner contact it to confirm deletion of the email, however, to date no response has been received
- the matter has been referred to the appropriate areas within SHP, Bupa and DIBP for follow up
- DIBP has informed Bupa that it considers Bupa has not complied with its contractual obligations regarding privacy
- Bupa are reviewing SHP protocols and practices regarding the transmission of information using non-official SHP email addresses
- Bupa and SHP have stopped distributing the status report
- DIBP and Bupa are reviewing their current contractual arrangements and obligations.

I note that you also advise that DIBP was considering its notification strategy.

Relevant guidance

You may find the OAIC's *Data Breach Notification Guide: A Guide to Handling Personal Information Security* (DBN Guide) and *Guide to information security: 'reasonable steps' to protect personal information* (Information Security Guide) useful in responding and helping to prevent and manage future breaches.

These resources guide entities on how they may take reasonable steps, within the meaning of the Privacy Act, to protect the personal information they hold from misuse, interference, loss and from unauthorised access, use, modification or disclosure.

Further information required by the OAIC

In order to inform our response to this matter, I would appreciate if you could provide a detailed update on DIBP, Bupa and SHP's response to this incident. In particular, I would appreciate it if you would provide:

1. whether DIBP has notified or intends to notify affected clients and if not, the factors it has considered in coming to that conclusion. I note that notification is most effective when it is timely and provides sufficient information to enable affected individuals to take mitigating action
2. information about Bupa's review of its and SHP's security policies and procedures including the transmission of client information outside of DIBP's authorised IT systems
3. any further developments regarding DIBP and Bupa's contractual arrangements.

Next steps

I look forward to receiving your response. I would appreciate your reply by **Tuesday 6 October 2015**.

If we receive a complaint from individuals affected by this incident, we will deal with the complaint on its merits. If this occurs, we will refer to the information you provided in your notification, as well as any other information relevant to this matter.

Generally, the OAIC asks that complainants refer their complaint directly to the relevant APP entity in the first instance. If the complainant is not satisfied with the handling of their complaint by the entity, they may then complain to the OAIC.

If you have any questions or wish to discuss this email, please feel free to call me.

Regards,

s. 22(1)(a)(ii) I Adviser I Privacy Practice, Advice and Technology
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY NSW 2001 | www.oaic.gov.au
+61 2 8231 s. 22(1)(a)(ii) | s. 22(1)(a)(ii) @oaic.gov.au

From: External Accountability [mailto:s. 22(1)(a)(ii) @border.gov.au]
Sent: Thursday, 3 September 2015 5:29 PM
To: Enquiries
Cc: s. 22(1)(a)(ii) ; External Accountability; Privacy
Subject: DBN15/00073 - DIBP Notification of Privacy Breach (Sonic HealthPlus) [DLM=For-Official-Use-Only]

For-Official-Use-Only

Dear OAIC Enquiries

I am writing to report that the Department of Immigration and Border Protection was advised of a possible data breach that occurred on 7 August 2015. A Privacy Incident Report outlining the circumstances of the incident is attached for your consideration.

We would be grateful if you could please forward this notification to a relevant contact officer at the OAIC's Regulation and Strategy Branch for their appropriate action.

Please do not hesitate to contact us should you have any further queries or concerns.

Kind regards

s. 22(1)(a)(ii)
Privacy Officer | External Accountability Section
Risk and Assurance Branch | Integrity, Security and Assurance Division
Corporate Group
Department of Immigration and Border Protection
P: (02) 6264 s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @border.gov.au

For-Official-Use-Only

****
WARNING: The information contained in this email may be confidential.
If you are not the intended recipient, any use or copying of any part
of this information is unauthorised. If you have received this email
in error, we apologise for any inconvenience and request that you
notify the sender immediately and delete all copies of this email,
together with any attachments.
****

Australian Government

Department of Immigration and Border Protection

23 October 2015

To: Hisham El-Ansary
Managing Director, Bupa Health Services
Bupa
33 Exhibition Street
Melbourne, VIC 3000

Copy to:
Brett Comer
General Manager, Bupa Medical Visa Services
Bupa
33 Exhibition Street
Melbourne, VIC 3000

Peta Dunn
First Assistant Commissioner,
Community Protection Division
Department of Immigration and Border Protection
s. 22(1)(a)(ii)@border.gov.au

Notice of Privacy Breach of Patient Medical Records by Bupa and its Subcontractor, Sonic HealthPlus

Dear Hisham,

I refer to the privacy breach reported by Bupa Australia Health Pty Ltd (Bupa) on Saturday 8 August 2015, involving the disclosure of personal information of 317 immigration clients to an unknown Gmail address by Bupa's subcontractor, Sonic HealthPlus (Sonic).

Reports received
Thank you for your letter dated 12 October 2015 which included the updated version of the Herbert Smith Freehills report on 'Visa and migration services – review of personal information security policies and procedures'. The Department acknowledges Bupa's attempts to obtain information from security information policies and procedures from all Bupa subcontractors, noting that all subcontractors have submitted the requested information with the exception of Geraldton Panaceus.

The Department has reviewed the Bupa report on the privacy breach dated 16 September 2015 (Bupa Report) and the updated Herbert Smith Freehills report summarising the review of all security information policies and procedures within Bupa and their subcontractors.

Issues
The Department has particular concerns regarding the circumstances leading to the privacy breach. In December 2014 a secure automated feed was introduced to enable Bupa to monitor

processing times and the Department acknowledges that up until 31 March 2015, this automated feed was only available to Bupa on a weekly basis. However, the Department does not accept that the absence of a daily data feed necessitated Bupa and Sonic to establish a process of transmitting personal client identifiers (specifically name, date of birth, passport number and summary of medical condition) via email. If the intent of the spreadsheet was to monitor performance against KPI two, the client identifiers (other than the HAP ID and date of examination) could have been removed from this spreadsheet to achieve this purpose.

The Department notes that the privacy breach occurred on 7 August 2015, approximately four months after the report became available daily. Despite the provision of the daily data feed to Bupa from 31 March 2015 onward, the practice of sending personal client information between Bupa and Sonic HealthPlus via email continued until the privacy breach occurred.

However, the Department notes that Bupa has identified work practices that may lead to unauthorised disclosure of personal information and has confirmed elimination of such work practices.

Breach

After considering the initial incident reports provided by both Bupa and Sonic, the Bupa Report dated 16 September 2015 and the review undertaken by Herbert Smith Freehills, the Department considers that Bupa has taken sufficient steps to remedy its breach of clause 28 of the Contract. Although the Department does not currently intend to pursue contractual remedies for this breach, the Department will continue to monitor Bupa's implementation of the recommendations from the independent review, as articulated and agreed by Bupa in paragraph 3.2.1 of the Bupa Report dated 16 September 2015.

The Department does not intend, at present, pursue any action against Bupa or its subcontractors in respect of any potential breach of the Australian Border Force Act.

Next Steps

As previously advised, the privacy breach was reported to the Office of the Australian Information Commissioner (OAIC) on 3 September 2015. On 6 October 2015 the Department submitted further information to the OAIC upon their request. The Department continues to engage with the OAIC in relation to this matter and will notify Bupa regarding any co-operation required.

On 16 October 2015 the Department notified the affected clients of the breach via email. The Department anticipates the notification will generate client complaints and requests Bupa's co-operation in managing these complaints.The Department confirms the current notification provisions in place under the Communication and Issues Management Protocols will remain in effect until further amendment by agreement between the parties.

Please contact s. 22(1)(a)(ii), Director Health Services at s. 22(1)(a)(ii)@border.gov.au if you have any questions.

Yours sincerely

s. 22(1)(a)(ii)

Paul Douglas
Assistant Secretary Immigration Health
Department of Immigration and Border Protection
s. 22(1)(a)(ii)@border.gov.au
GPO Box 9984 Sydney NSW 2000

From: s. 22(1)(a)(ii)
To: s. 22(1)(a)(ii)
Cc: External Scrutiny; s. 22(1)(a)(ii)
Subject: FW: TRIM: DIBP data breach notification about Bupa and Sonic Health Plus [SEC=UNCLASSIFIED]
Date: Monday, 30 November 2015 3:32:45 PM

UNCLASSIFIED

Hi s. 22(1)(a)(ii)

Referring to the email below, the OAIC has proposed not to take any further action on the incident at this time. From a Departmental perspective, we consider this matter closed.

Thank you for your proactive work in escalating this to us as appropriate, and as always, more than happy to discuss any issues or concerns you may have moving forward.

Kind regards

s. 22(1)(a)(ii)
Privacy Officer | External Accountability Section
Risk and Assurance Branch | Integrity, Security and Assurance Division
Corporate Group
Department of Immigration and Border Protection
P: (02) 6264 s. 22(1)(a)(ii)
E: s. 22(1)(a)(ii) @border.gov.au

UNCLASSIFIED

From: s. 22(1)(a)(ii) [mailto:Js. 22(1)(a)(ii)@oaic.gov.au]
Sent: Monday, 30 November 2015 2:11 PM
To: External Accountability
Cc: s. 22(1)(a)(ii)
Subject: TRIM: DIBP data breach notification about Bupa and Sonic Health Plus [SEC=UNCLASSIFIED]

Dear s. 22(1)(a)(ii)

Thank you for providing further information on 6 October 2015 to the Office of the Australian Information Commissioner (OAIC) about the data breach involving the Department of Immigration and Border Protection (DIBP), DIBP's contracted service provider Bupa Australia Health Pty Ltd (Bupa) and Bupa's sub-contracted service provider, Sonic Health Plus (SHP) (our reference: DBN15/00073).

The breach involved an SHP employee disclosing clients' personal information by sending a spreadsheet containing clients' information to an incorrect email address in error.

In your response of 6 October 2015 you advise that in addition to the steps DIBP set out in its notification of 3 September 2015:

- DIBP intends to notify the affected individuals about the breach
- Bupa has contacted the email service provider of the receiving email address, Google, about this matter and Google has temporarily removed the email containing clients' information from that email's inbox and commenced the process of permanently deleting the email.

You also advise that:

- Bupa is continuing to review its subcontracted service providers' policies and procedures relating to the security of personal information and is expected to provide DIBP with an updated report by 9 October 2015
- DIBP intends to review its contractual arrangements with Bupa after it receives the aforementioned report from Bupa.

I note that in your email of 20 October 2015, you confirmed that DIBP had notified all of the affected individuals about this incident.

Next steps

It appears DIBP is taking appropriate steps to contain and respond to the data breach incident. Therefore, we do not propose to take any further action on this matter at this time.

If we receive a complaint from individuals affected by this incident, we will deal with the complaint on its merits. If this occurs, we will refer to the information you provided in your notification, as well as any other information relevant to this matter.

Generally, the OAIC asks that complainants refer their complaint directly to the relevant APP entity in the first instance. If the complainant is not satisfied with the handling of their complaint by the entity, they may then complain to the OAIC.

If you have any questions or wish to discuss this email, please feel free to call me.

Regards,

s. 22(1)(a)(ii) I Adviser I Privacy Practice, Advice and Technology
Regulation and Strategy Branch
Office of the Australian Information Commissioner
GPO Box 5218 SYDNEY NSW 2001 | www.oaic.gov.au
+61 2 8231 s. 22(1)(a)(ii) | s. 22(1)(a)(ii) @oaic.gov.au

For Official Use Only

9 December 2016

Privacy Report – ASPEN Medical

This incident is being reported to the Office of the Australian Information Commissioner for the purposes of transparency only.

INCIDENT

Three laptops used by Aspen Medical for the purpose of keeping notes about clinics were stolen from Aspen Medical's office at the Republic of Nauru Hospital sometime during the evening of 28 November and early morning Tuesday 29 November 2016. The laptops were configured so that staff from Aspen Medical did not need passwords to log in, as they were used by multiple clinicians for various day to day tasks.

BACKGROUND

Aspen Medical is currently contracted to provide emergency medical and light surgical support in Nauru for the Department of Immigration and Border Protection (DIBP). Aspen Medical has also been contracted to conduct specialist medical clinics such as Orthopaedic, Ear, Nose and Throat and podiatry to refugees, asylum seekers and Nauruan nationals on a frequent basis. s. 47G(1)(a)

s. 47G(1)(a)

RESPONSE

A representative from the RoNH advised Aspen Medical that the RoNH Outpatient department, Radiology unit and Dressing clinics had also been the subject of unlawful entry and theft including theft of computers and hard drives. Aspen Medical's representative was asked to complete an internal incident form and spoke with the Supervisor of the security team. Later in the morning the representative went to the Nauruan Police Force (NPF) and provided a written statement. The NPF advised Aspen Medical's representative the matter was under investigation and that they are following up on a suspect.

THE LAPTOPS

s. 47G(1)(a)

s. 47G(1)(a)

FOLLOW UP ACTIVITY

As a result of the theft of the laptops Aspen Medical is undertaking an audit to confirm that all computers used by Aspen Medical for the services are password protected and stored securely.

INCIDENT REPORT CLEARED BY:

s. 22(1)(a)(ii)
Position: A/g Assistant Secretary, Information Management Branch
Date: 9 December 2016