

**Cloud Questionnaire**

|  |  |  |
| --- | --- | --- |
| **Service / Project** | **Completed By** | **Date** |
|  |  |  |
| **Approver\*** | **Role** | **Date** |
|  |  |  |

\* Clinical Director or Service Manager

|  |
| --- |
| **Briefly describe the cloud service you propose to use and the data that will be stored** |
|  |

**Please tick the statements that are correct**

(Do not tick statements that you are uncertain about)

|  |  |
| --- | --- |
| **Information Disclosure Risk** |  |
| The information is publicly available or it can be de-identified so that its release into the public domain would not compromise our obligations to a person or an organization. |  |

|  |  |
| --- | --- |
| **Information Alteration Risk** |  |
| No person or organisation will be harmed if the information is altered by mistake or intentionally by a wrongdoer. |  |

|  |  |
| --- | --- |
| **Information Loss Risk** |  |
| No person or organisation will be harmed if the information is lost by the cloud provider; OR we can easily maintain a local copy of the information. |  |

|  |  |
| --- | --- |
| **Business Continuity Risk** |  |
| We will be able to carry on our activities if the service is disrupted or is unavailable for an extended period. |  |

If you did not tick every statement, your project has risk which should be investigated before proceeding further.

Please return the completed form to:

[IT.ServiceDesk@ccdhb.org.nz](mailto:IT.ServiceDesk@ccdhb.org.nz)

How to complete this form

The 3DHB ICT Cloud Questionnaire is designed to enable you to determine if your proposed cloud service is likely to introduce any risks that need to be managed or investigated further.

The reality is that no system is perfect - hacking is commonplace, cables get cut, equipment fails and backups get lost from to time.

When answering these questions, focus on the question and think about it as if the undesired behaviour **has happened**. Then ask yourself, “what would this mean for me, my staff, my patients and my service or business unit?” The vendor may have assured you that their cloud service is “secure” and that you can use it without having to worry about anything. ***These questions are not asking you how good the vendor thinks their system is.*** ***They are asking you to think about what would happen if something goes wrong.***

***Question 1*** **“The information is publicly available or it can be de-identified so that its release into the public domain would not compromise our obligations to a person or an organization.”**

This question is about ***privacy***. As a government entity, a DHB must be seen to be protecting the privacy of patients and staff. We also have to be seen to be taking good care of the DHBs business information such as financial records. There are clear guidelines on what is acceptable and what is not.

Staff information is ANYTHING that enables a staff member to be identified. Some people don't even like their name being put in the phone book. That is your starting point.

Patient information is EVERYTHING that the DHB holds about that person if it is identifiable in any way.

Business information is ANYTHING concerning the DHB that we would not make public unless it could be obtained by an official information request.

De-identified information is data that has had the personal identifiers removed such as name, address, NHI, date of birth and address etc.

If properly de-identified information is stolen by a hacker, it is unlikely to affect a person’s privacy because the hacker can’t tell who it is.

If you are unsure about the status of your information, contact the DHB Privacy Officer.

***Question 2*** **“No person or organisation will be harmed if the information is altered by mistake or intentionally by a wrongdoer.”**

This question is about ***safety***. The key here is to think about what could happen if someone was to alter the information in some way. This could be by accident or it could be intentional. With clinical records, it can be critical for the information to be accurate. Would you be able to tell if the information was altered? What would be the effect? Would someone’s life be endangered or would it just cause inconvenience that you could live with? Would it be different if was just a single record that was changed or a large group of records?

***Question 3*** **“No person or organisation will be harmed if the information is lost by the cloud provider; OR we can easily maintain a local copy of the information.”**

This question is about ***information loss***. The key here is to think about what could happen if the vendor was to lose your information and be unable to recover from backups. This could happen due to human error or an event such as a fire or ransom ware attack. Would you be able to recreate the information if you needed to? Would it just be an inconvenience which you could live with or would you have a serious problem? Does the vendor provide a means for you to take a copy of your information from time to time?

***Question 4*** **“We will be able to carry on our activities if the service is disrupted or is unavailable for an extended period.”**

This question is about **business continuity**. The key here is to think about what would happen if you suddenly couldn’t reach the service anymore. This could be temporary due to a cable failure or permanent if, for example, the vendor goes out of business. It could also happen if you forget to pay the vendor’s bill. Would you still be able to carry on your activities by using some other means? Would it just be an inconvenience which you could live with? Is there another supplier of a similar service which you could easily switch to?

Any reputable vendor should publish their **terms and conditions** and **privacy policy** on their website.

Read these. They tell you what you the vendor agrees to do. For example they may limit their liability, in the event of something going wrong, to the last payment you gave them. Is this good enough? They might reserve the right to use the information you are storing on their service for their own purposes. They might even claim ownership of the information. Is this acceptable to you?

***Contact the 3DHB ICT Service Desk if you need additional assistance with this form.***