Summary

Privacy Impact Assessment

for

Contact: Hayley Samuel
Manager Information & Communication
Hayley@medsac.org.nz
Version: 1.0
Issued: 22 October 2020

Contents

1. Introduction

Some SAATS (Sexual Abuse Assessment and Treatment Services) in New Zealand are capturing information related to service provision and clinical management. A variety of methods are currently being used to collect data including electronic patient management systems (e.g. MedTech), MS Excel spreadsheets and other customised paper forms used within the clinic. For ACC reporting, each SAAT Service currently collects data that relate to numbers (and type) of cases seen for first and follow-up appointments that are required for monthly invoicing. KPIs were introduced in January 2018. All SAAT Services are required to report to ACC quarterly on case numbers by age and gender, and the nature of the case (whether forensic, non-forensic, just in case or historical). Annual narrative reports require details on service staff numbers, clinician accreditation, MEDSAC training status, and peer review attendance. In summary, some information is captured by all services using a range of methods but there is currently no national, standardised data collection process in place relating to SAAT Service provision.

To resolve this, Medical Sexual Assault Clinicians Aotearoa (MEDSAC), has designed the SAATSdata system which has been developed along with new processes for capture of this information into the SAATSdata database. The key mechanism of this database is the Medical Examination Record (MER) which captures key information collected at the time of a forensic, or just in case, medical examination. The MER is also currently being trialled as an electronic form.

MEDSAC provides the SAATSdata system for all SAAT Services to manage their own service data, and to generate their own respective service reporting for SAATS contract administration, analytics and in-house audit and evaluation of their service. National collated data, pertaining to the scope, nature and management of sexual assault in New Zealand, will be able to be generated by MEDSAC for the SAATS funders (Ministry of Health (MoH), Accident Compensation Corporation (ACC) and New Zealand Police (NZ Police)) to inform the development of evidence-based medical and forensic practices and monitor for provision of equitable access to services across New Zealand.

This document reviews each of the privacy rules and how they have been addressed by the SAATSdata system and its implementation by SAAT Services around the country.

2. Privacy Impact Analysis

This section considers each privacy principle and how it is upheld in the new system and mitigations for any risks introduced by the new solutions.

The key change to current workflows is that a subset of the information currently collected by SAAT Service providers will be shared with MEDSAC.

2.1. Principle 1: Purpose of Collection of Health Information

Principle:	Principle 1 of the Health Information Privacy code (HIPC) requires that information be collected only for the lawful purpose that is related to the function or activity of the health agency.
Current:	SAAT Services already complete the MER/other clinical proforma. Clinical proformas (other than the MER) may vary slightly from service provider to service provider. This information is stored in their own solutions and only billing information is shared with ACC and District Health Boards.
Change:	A subset of data captured in the MER/other clinical proforma, will be either entered directly into SAATSdata or into an electronic or paper form and then entered into SAATSdata. MEDSAC will have access to this information for reporting and analysis purposes. This is a new purpose for the data. No new information is being collected by services, it is however, being stored in a new location.
Risk:	The new purpose for collected information isn't clearly communicated with patients Information provided to SAATSdata may be accessed by someone outside of the SAATS provider and MEDSAC
Mitigation:	New purpose for data: • Patients attending the SAAT Services will be made aware of the data collection process and privacy assurances through, at a minimum, posted signage within the Service patient areas. Access to the new location for SAATS information: • SAATSdata can only be accessed by those granted access by MEDSAC • The user interface utilises encryption technologies to ensure information entered cannot be accessed by non-users • SAATSdata is behind a firewall and the Hosted VMs can only be reached via a VPN

2.2. Principle 2: Source of Health Information

Principle:	Principle 2 subrule (1) of the HIPC (2008) stipulates "where a health agency collects health information, the health agency must collect the information directly from the individual concerned" (p15).
Current:	Information has been collected under existing arrangements and directly from patients.
Change:	No change
Risk:	No new risks
Mitigation:	-

2.3. Principle 3: Collection of Health Information from Individuals

Principle:	Principle 3 addresses the need for those collecting the information to ensure that the individual is aware of the information flows and the purpose of those flows. Its intention is to provide autonomy to the individual in the control of their health information. Principle 3 ensures awareness by the individual of what is happening with them or their dependent's health information: a) The fact that the information is being collected b) The purpose for which the information is being collected c) The intended recipients of the information d) The name and address of - the health agency that is collecting the information, and the agency that will hold the information e) whether or not the supply of information is voluntary or mandatory f) the consequences for that individual if all or any part of the requested information is not provided g) the rights to access to, and correction of health information provided by principles 6 and 7 The HIPC indicates that although sharing information with other pertinent health agencies involved with the patient's care is good practice, it should only be done with the individual's knowledge. This rule is intended to assist the

	awareness of patients to what is happening with their health information, not to require consent from them for it to happen.
Current:	Information is captured as part of completing the MER/other clinical proforma.
Change:	Information captured in the MER/other clinical proforma, is entered into SAATSdata. Information stored in SAATSdata is used for service analysis and billing functions. The SAAT Service needs to provide ACC with administrative data for purposes of billing against the SAATS contract. SAATSdata provides a new forum to enter this data in order to receive payment for services provided.
Risk:	The new purpose for collected information isn't clearly communicated with patients Patients whose data is migrated were not made aware of the new use of that information
Mitigation:	New purpose: • Patients attending the SAAT Services will be made aware of the data collection process and privacy assurances through, at a minimum, posted signage within the Service patient areas. Migrated data: • Data being migrated is de-identified to the extent possible. Only the system super-user and the SAATS service that managed the patient event will have access to the unique identifiers (NHI and ACC45 if recorded). With the exception of the NHI (optional entry in SAATSdata) and the ACC45 number (if recorded), the data being migrated is already provided in such a form to the funders. The NHI will only be utilised for internal reporting requirements within the respective SAAT service that managed the patient event and will not be shared with the funders and the ACC45 number is provided to ACC only for billing requirements.

2.4. Principle 4: Manner of Collection

Principle:	Principle 4 addresses the need to ensure that information is collected in a fair and lawful manner.
Current:	Information is collected as part of the examination process and under the consent provided to SAATS providers.

Change:	There are no changes from the current methods of data collection.
Risk:	No new risk
Mitigation:	-

2.5. Principle 5: Storage and Security

Principle:	Principle 5 addresses the need for agencies holding the health information to secure it appropriately. No absolute measures are outlined, as the appropriate level of security depends on the sensitivity of the information.
Current:	The information captured in the MER/other clinical proforma is stored by the SAATS providers. Some non-identifiable information is provided to ACC and DHBs for billing purposes.
Change:	A new storage location is being established, SAATSdata. A subset of non-identifiable MER/other clinical proforma data will be captured on it.
Risk:	SAATSdata is accessed via the internet and may be open to unauthorised access
Mitigation:	The following are in place to address this: • Only those with a user account can access the system • Only internet traffic from SAAT Service provider networks can access the system • User accounts require two factor authentication • All ports to the solution are blocked except for the one assigned • All traffic to the solution and the ESR network is via https • The VM host is only accessible via a VPN, that is inside the ESR network • Users can only access data for the service they are part of • All users must sign a user agreement before access to the system • All data is backed up and stored off-site • All access and use of data is tracked through an audit trail

2.6. Principle 6: Access to Personal Health Information

Principle:	Principle 6 states: (1) That when health information is collected, individuals have a right to know whether an agency holds such health information and to have access to that health information. (2) Sets out the requirements that the individual be informed that they may request correction of that information.

	(3) Also sets out the right for the health providers to refuse a request for access to an individual or representative's child health information.
Current:	The rights of the patient posters (digital and print) are displayed in the SAAT Service provider clinic room/s informing the patients of their rights to their information.
Change:	Information stored in SAATSdata is de-identified to the extent possible but it may not be anonymised if the optional NHI and ACC45 fields are completed.
Risk:	Risk of re-identification of an individual from NHI (optional use) and ACC45 (if utilised).
Mitigation:	Only the super-user and the SAAT Service that managed the patient event will have access to the unique identifiers (NHI and ACC45). As a governance control, all access and use of data is tracked through an audit trail. SAATS Services are required to conduct regular access audits of SAATSdata use, pertaining to their service data, in to order to ensure data access has been appropriate by all system users. Audit reports are a system feature for this purpose. In the case of other users, it will be impossible for them to either view or identify a record as belonging to an individual. Service data is managed by the respective service and not by MEDSAC (other than MEDSAC providing technical support as required). To this end, any requests to MEDSAC for health information held in SAATSdata under Principle 6 of the HIPC, would be transferred to the respective service in accordance with section 39 of the Privacy Act.

2.7. Principle 7: Correction of Health Information

Principle:	Principle 7 outlines the representative's entitlement to request the correction of information held about them. It also outlines the health provider's obligation to correct information when it is wrong. When a health provider receives a request to correct information, but they do not wish to correct the information, the health provider is obliged under this rule to attach a note to a patient's record outlining the request and subsequent refusal.
Current:	The rights of the patient posters (digital and print) are displayed in the SAAT Service provider clinic room/s informing the patients of their rights to their information.
Change:	Information stored in SAATSdata is de-identified to the extent possible but it may not be anonymised if the optional NHI and ACC45 fields are completed.

Risk:	Risk of re-identification of an individual from NHI (optional use) and ACC45 (if utilised).
Mitigation:	Service data is managed by the respective service and not by MEDSAC (other than MEDSAC providing technical support as required). To this end, any requests to MEDSAC for correction of health information held in SAATSdata under Principle 7 of the HIPC, would be transferred to the respective service in accordance with section 39 of the Privacy Act.

2.8. Principle 8: Accuracy of Health Information to be checked before use

Principle:	Principle 8 requires information that is collected and stored by a health provider or agency, to be accurate, up to date, complete and relevant.
Current:	Data captured by the clinician is done so with the patient and subject to guidelines and practices.
Change:	No change
Risk:	No new risks
Mitigation:	-

2.9. Principle 9: Retention of Health Information

Principle:	Principle 9 states that health providers must not hold health information longer than necessary for the purposes for which it may be used.
Current:	Data is held by SAAT Service providers indefinitely due to the medicolegal, or potential medicolegal nature.
Change:	The new SAATSdata will hold patient data indefinitely to support trend and service analysis.
Risk:	No new risk
Mitigation:	-

2.10. Principle 10: Limits on the Use of Health Information

Principle:	Principle 10 limits a health agency's ability to use health information for purposes other than what it was collected for. A health agency that holds health information obtained in connection with one purpose must not use the information for any other purpose unless the health agency believes, on reasonable grounds — that the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained.
Current:	Data is only reported at SAAT Service level, not nationally.
Change:	The data collected in SAATSdata is specifically for analysis, billing and reporting purposes.
Risk:	The data is utilised for some other as-yet-to-be-defined purpose
Mitigation:	The MEDSAC board is charged with ensuring the data is only used for those purposes. Any new uses will require approval from the respective SAAT Service that the data belongs to. In addition, all necessary approval processes will be followed e.g. Health and Disability Ethics Committee approval.

2.11. Principle 11: Limits on Disclosure of Health Information

Principle:	Principle 11 limits the disclosure of personal information held by an agency. An agency that holds personal information is obliged not to disclose this information to a third party unless the agency believes disclosure is allowable under the stated reasonable grounds of principle 11. A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds, that – (c) the disclosure of the information is one of the purposes in connection with which the information was obtained;
Current:	Different parts of the MER/other clinical proforma data is currently shared with DHBs, ACC, ESR and NZ Police.
Change:	The information will be shared with MEDSAC.
Risk:	Information will be shared with other parties
Mitigation:	No other party will have access to the data in SAATSdata. Only reporting at national, district and regional levels will be shared outside of the MEDSAC body.

2.12. Principle 12: Unique Identifiers

Principle:	Rule 12 limits the abilities of health agencies to assign unique identifiers to patients.
Current:	An internal ID is used for patients, in addition to the MER number (if used), the NHI number (optional) and the ACC45 number (if completed).
Change:	These unique identifiers will be recorded in SAATSdata as they (with the exception of the NHI) are requirements for billing purposes. The NHI number is required in SAATSdata by some SAAT Services to align with their PMS/record management system and will not be utilised for any external reporting.
Risk:	A patient will be able to be identified by the unique identifiers.
Mitigation:	No agency utilising these unique identifiers external to the SAAT Service will have access to SAATSdata to be able to identify a patient i.e. the NHI (optional) and ACC45 (if completed) will only be visible to the SAAT Service that managed the patient event and the system super-user. As a governance control, all access and use of data is tracked through an audit trail. SAATS Services are required to conduct regular access audits of SAATSdata use, pertaining to their service data, in to order to ensure data access has been appropriate by all system users. Audit reports are a system feature for this purpose.

3. Glossary of Terms

Term	Description
Access Audits	Regular access audits generated by SAATS Services to ensure data access has been appropriate by all system users with access to their respective data.
ACC45	A 'New Injury Claim Form' utilised by ACC.
Azure	A solution provided by Microsoft, where virtual computers are provided as required by clients. Azure is Microsoft's version of cloud computing.
Clinical Proforma	A clinical proforma is a detailed record of an alleged assault taken by a SAATS clinician when the examination is being performed without an MER (a non-forensic examination).
Cloud Computing	Essentially this is a set of computer physically in other locations to where the user of those systems is. Cloud computing make a lot of use of Virtual Machines and allows people to quickly turn on, speed up, slow down and turn off capabilities of those Virtual Machines.
CRUD	Create, Retrieve, Update and Delete. Typical actions that can be performed on a data record.
Database Triggers	When an action is taken on a data record it can trigger other actions. In this system it results in the tracking of CRUD actions taken on that record.
Firewall	Equipment that controls access to computer networks, blanket blocking access or only allowing access if certain rules are met – e.g. only allow access from certain computers.
Joget	A software tool that makes creating new computer systems easier.
Host VM	A "virtual machine" is a computer that exists as software only – that is there isn't a tin box and specific parts that belong only to it. It lives on a "Host" computer and shares all the computer parts with other virtual machines.
https	Hypertext Transfer Protocol is a standard for how information should be sent from one computer to another on the internet. The S is for secure. This is provide by SSL Certificates.
MEDSAC	Medical Sexual Assault Clinicians Aotearoa (MEDSAC), formerly Doctors for Sexual Abuse Care [DSAC], is a national organisation of doctors and nurses formed to develop and maintain standards of best practice in the delivery of medical

Term	Description
	and forensic services in New Zealand in the area of sexual assault/abuse.
MER	Medical Examination Record, the detailed record of an alleged assault taken by a SAATS clinician.
MySql	Database software.
NHI	National Health Index number is a unique identifier assigned to every person who uses health and disability support in NZ.
Production Solution	Most published software has at least three versions of itself running: Production Solution – the one used for real patients, clinicians and data UAT Solution – not widely available Development Solution – used by the software developers to make changes When a change is needed to the software, it is usually completed in the Development Solution, subjected to a set of tests. Once those tests have been passed the change can be pushed to production.
SAATS-Link	SAATS-Link is an online resource, provided by MEDSAC, for people providing medical care in SAAT Services to people affected by sexual assault/abuse.
SAAT Services	A service that provides SAATS .
SSL certificates	Is the S in "https". Encrypts information traveling across it to ensure the data cannot be read by an unintended party.
Super-User	The system technical custodian (SAATSdata System Manager) who provides user management, analytical reporting and 'help desk' duties to support authorised SAATSdata users.
User Acceptance Testing (UAT) Solution	This is a copy of the computer system that is used by software developers and a select group of users to ensure any changes or additions to the software are working correctly before they are added to the Production Solution .
VPN	Virtual Private Network. Like creating a private, secure tunnel that you can only entered from one end or the other. Only those with the right "keys" can enter the tunnel.