Privacy Impact Assessment

for

Contact: Hayley Samuel
General Manager
hayley@medsac.org.nz
Version: 1.3
Issued: 16 February 2023

Purpose

The purpose of this document is to articulate the impact on patient privacy and subsequent mitigations created by the introduction of SAATSdata.

Version History

Date	Document Version	History	Author / Reviser
27/08/2019	0.1	Created based on template	Peter Gilbert
15/09/2019	0.2	Completed first draft based on information provided	Peter Gilbert
26/09/2019	0.3	Updates from MEDSAC	Peter Gilbert
16/10/2019	0.4	Updates based on feedback from Privacy Commission	Peter Gilbert
27/07/2020	0.5	Updates from MEDSAC	Hayley Samuel
22/10/2020	1.0	Updates based on feedback from Privacy Commission	Hayley Samuel
28/10/2021	1.1	Updates to reflect data collection field changes and updated ACC service codes	Hayley Samuel
12/04/2022	1.2	Updates to incorporate Privacy Act 2020 – addition of *Principle 12 – Disclosure outside New Zealand* and renumbering of *Principle 13 – Unique Identifiers*	Hayley Samuel
16/02/2023	1.3	Additional data fields added	Hayley Samuel

Approvals

Date	Document Version	Approver name and title	Signature
22/10/2020	1.0	Kim Lund – SAATSdata Project Lead	
28/10/2021	1.1	Kim Lund – SAATSdata Project Lead	
12/04/2022	1.2	Kim Lund – SAATSdata Project Lead	
16/02/2023	1.3	Hayley Samuel – General Manager	

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.

1.1. Who we are

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 and forensic services in New Zealand in the area of sexual assault/abuse. Its membership includes doctors and nurses with skills and experience from many disciplines working in the field of sexual assault/abuse care and forensic medicine.

MEDSAC's raison d'etre is 'improving the wellbeing of people affected by sexual assault/abuse', a purpose that it shares with other organisations operating within the sexual harm sector. MEDSAC's ambition is that 'people in New Zealand who are affected by sexual assault/abuse

have equitable and timely access to appropriate and high-quality health care and medico-legal services'.

The organisation provides nationally accessible education, training and support of clinicians to ensure maintenance of internationally recognised standards of best practice in the medical and forensic management of sexual assault and child sexual abuse or assault, including the medico-legal process. MEDSAC provides this training for doctors and nurses from all regions of the country.

MEDSAC was formed in 1988 by a group of doctors who recognised the need for a specialised medical service to address the complex and varied needs of people who disclose a history of recent or historic sexual assault or abuse. Prior to this date, medical professionals, including Police Medical Officers (PMOs) did not have any training, protocols or guidelines in the management of these affected people. People who reported acute sexual assault/abuse to Police were often examined in police stations by unsupported PMOs, a far from optimal situation.

MEDSAC has become the acknowledged NZ expert body in sexual assault/abuse medicine and is recognised as such by the Ministry of Health (MoH), Accident Compensation Corporation (ACC) and New Zealand Police (NZ Police), as well as by the Health and Disability Commissioner and also by international bodies such as the World Health Organisation.

MEDSAC is the only professional medical body that provides training and an accreditation system for the medical forensic response to sexual assault/abuse in New Zealand. MEDSAC-trained and accredited clinicians are the primary providers of acute forensic sexual assault/abuse medical care and follow-up throughout the country.

MEDSAC has successfully developed and maintained medical forensic training programmes, peer review processes and national update programmes, which reflect internationally recognised standards of best practice. These training courses form the basis for MEDSAC's education and accreditation of clinicians engaged in the provision of SAATS.

MEDSAC has developed an accreditation process for child, adolescent and adult medical forensic examiners for sexual assault/abuse, which ensures standards of best practice and knowledge. This process is recognised and supported financially in part by the funders of SAATS in addition to being acknowledged by the NZ justice system.

The MEDSAC Manual "The Medical Management of Sexual Assault" is a key resource for practitioners, NZ Police and the legal fraternity.

In 2016, MEDSAC was engaged as a valued (steering group) participant in the independent Sapere review of SAATS, which resulted in 26 recommendations for service improvement, nine of which have been, or are currently being, implemented by MEDSAC. This review resulted in the development of a new SAATS contract which was launched in 2018, which included many of the critical MEDSAC-informed Sapere recommendations.

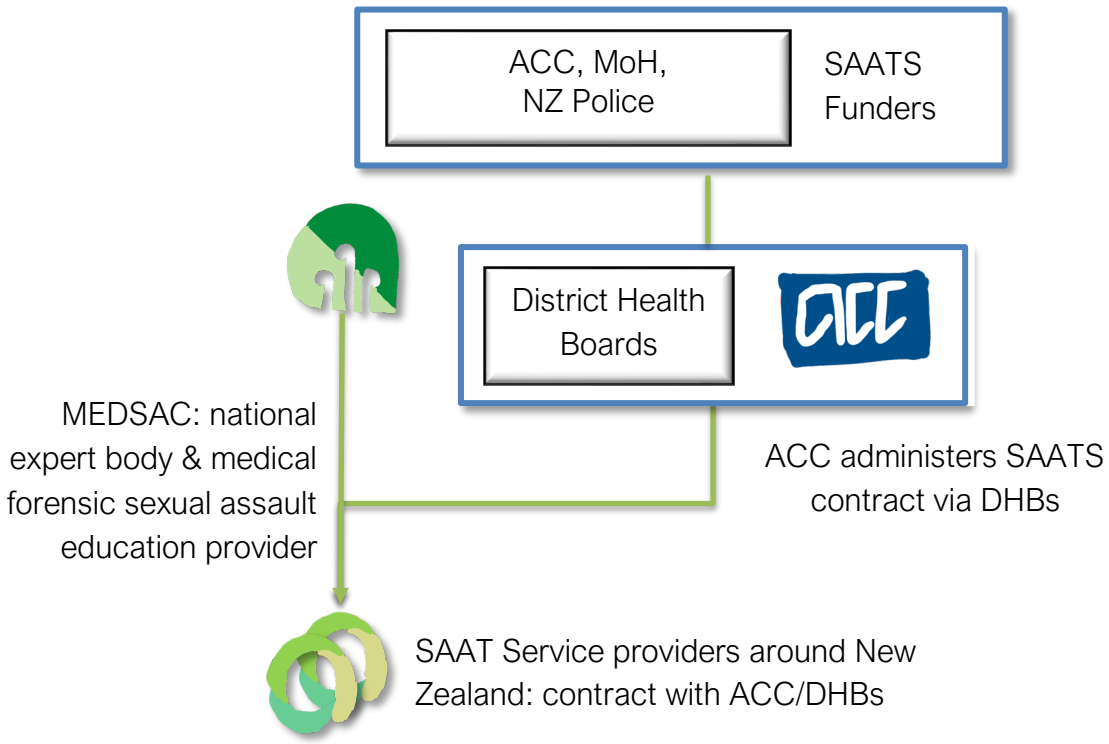
1.2. SAATS

In November 2006, MEDSAC alerted agencies including ACC, NZ Police and the MoH to the fragility of existing medical sexual assault/abuse services around the country and provided the clinical expertise for the development of a new Sexual Abuse Assessment and Treatment Service (SAATS).

SAATS is now a national service (17 regions), funded by ACC, NZ Police and the MoH, which provides medical care and forensic examinations for people who may have experienced sexual assault/abuse. MEDSAC remains the expert medical forensic advisor on matters relating to the provision of SAATS.

The SAATS contract is made between ACC (on behalf of the funders) and District Health Boards (DHBs). However, some DHBs have subcontracted the service out to a PHO, dedicated Trust etc.

SAAT Services vary widely throughout the country due to the challenges of geographic spread and, in some cases, under-resourcing; particularly in regards to administrative support. Not all services have dedicated facilities, dedicated administrative support or employed daytime staff.



1.3. SAATS-Link

In 2017 MEDSAC established SAATS-Link, which fulfilled a long-term strategy to form an effective clinical network to support clinicians engaged in the delivery of SAATS. The establishment of SAATS-Link, which was a significant MEDSAC initiated outcome of the Sapere review, was jointly funded by MEDSAC and the Government funding agencies. The network is now fully operational, including a clinical data management facility which went live in September 2020.

SAATS-Link provides:

- National Network – connecting the people who provide SAAT Services throughout Aotearoa New Zealand.
- SAATS-Link Manual – operating guidelines for SAATS clinicians and administrators
- Expert Advice - an online forum of medical forensic experts who provide advice and support to the SAATS-Link community
- Online Forums – community forums for sharing information and facilitating discussions on clinical and administrative matters
- Membership and Services Directory – online access to all SAAT Service providers and members of the SAATS-Link community

It is intended that SAATS-Link will be consolidated with the MEDSAC website in late 2020 for enhanced user-access.

Update: The consolidated SAATS-Link and MEDSAC websites went live in July 2021.

1.4. Terms of Reference

This assessment serves to:

- Identify the potential effects that SAATSdata may have on individual's privacy
- Identify areas of risk where there may be potential for breach of privacy
- Identify strategies that will be put in place to mitigate the risks identified
- Illustrate to the governance groups, steering groups, stakeholders, future users of the solutions, and the public that due diligence has been carried out to assess and minimise potential areas of risk to comply with the Information Privacy Principles
- Ensure that SAATSdata includes the functionality and capability to support the mitigation strategies

1.5. Assessment Process

Resolution8 Limited was contracted to:

- Review the processes used to identify SAATSdata solution needs
- Review the way the system has been constructed

- Capture how data collection processes are completed
- Review the agreements used for the collection, storage and retention of the information
- Understand how the solution will continue to be maintained
- Identify solution and process risks and their mitigation

With this information collected, Resolution8 then reviewed this against each of the Privacy principles to complete an assessment of how well each has been addressed by MEDSAC.

2. Solution Overview

This section describes the solution as a whole, that is, computer systems and people systems that enable the computer solutions.

2.1. Why the solution has been created

"The aim of this project is to set up a secure national database that will hold de-identified case information collected in New Zealand SAAT Services. The database will allow for consistent and accurate national data collection pertaining to the scope, nature and management of sexual assault in New Zealand."

Rationale for developing the database: SAAT Services are embedded in other agencies around the country, such as DHBs and PHOs. Therefore, patient information is currently collected in multiple formats depending on the resources of the services. There is no central repository of information at present, which impacts on the ability to provide feedback to services around the country by MEDSAC. Many SAAT Services are under-resourced, particularly those in rural areas and capturing information is labour intensive and subsequently not done in a consistent manner throughout New Zealand. Few services currently store electronic patient information (Auckland and Wellington services currently hold some information electronically).

This project aims to provide secure storage of SAATS information and make it readily available to individual services for purposes of informing practice, required reporting and service development. This will benefit staff within the services, the agencies supporting them and ultimately will benefit the patients by having a well-informed team of clinicians that are responsive to the needs of those accessing the services by basing care on evidence based and objective information.

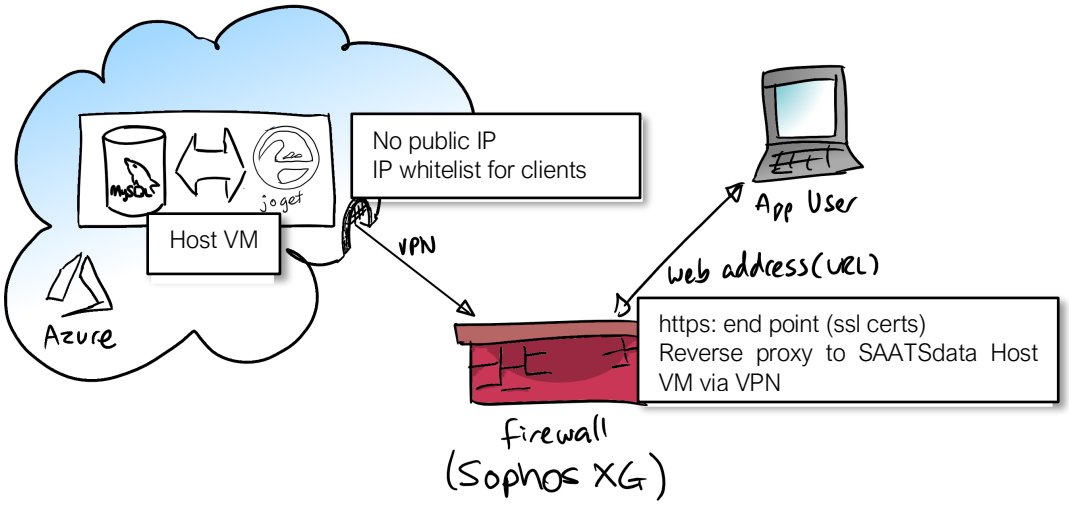
2.2. Technical Overview

The SAATS-Link Database is built on the following components:

- External web access via the internet
- Secured access to only authorised users
- Protected by Environmental Science and Research (ESR) firewall
- Located in the Microsoft Azure platform under ESR account and connected by ESR Virtual Private Network (VPN)
- One simple Patient Event Record search and delete screen (where appropriate rights are granted)
- One simple Patient Event Record entry and edit form
- A User Profile form for self-management, including:
    - Name change
    - Password change
    - 2 factor authentication activation

- A Manage Users form:
    - Accessible by a System Manager only
    - Force a change password for a user
    - Select the 'User Service Location(s)' they can access
    - Set whether an Admin User or not
    - Disable a user
- Core solution functions including (managed by roles applied to user accounts):
    - Other static data maintenance tables
    - Reports
    - Data Export functions
    - Data Import functions
- Audit trail against all actions (CRUD) via database triggers

The diagram below shows a high-level architecture for the solution.



The Azure cloud (based in Sydney, Australia) hosts SAATSdata. This is built using a MySQL database and the Joget framework. MySQL holds the data and tracks changes to records and the Joget solution provides the website forms that SAATSdata users enter patient, clinical and other event data into.

This is locked down and not visible to the internet and can only be reach by the VPN – virtual private network. The VPN essentially creates a tunnel that only those with the authorised access can reach the solution. All information that travels across the VPN is encrypted and can only be accessed by those with access to the VPN – further protecting the information as it travels to the Azure cloud.

The firewall – hosted in New Zealand in the Revera Data Centre, on behalf of ESR – ensures only data to and from specific web addresses can reach SAATSdata. It also controls ESR staff access to the solution.

The application user uses a specific web address (URL) to reach the solution which is directed to the ESR firewall. The website address uses the https encryption technology to ensure any data to or from the solution is not visible to anyone as it travels across the internet. Access to

the solution is controlled by username and password plus 2 factor authentication activation for that account.

The reverse proxy approach further hides SAATSdata solution by presenting the solution as if it were actually located at the firewall.

2.3. Stakeholders

There are multiple stakeholders in this project:

- MEDSAC/SAATS-Link: this agency will hold the data in secure storage The proposed national data collection system will enable a better understanding of, and potentially contribute to, improved SAAT Service delivery by enabling audit at the service- and national-level.
- Institute of Environmental Science and Research (ESR): ESR has been contracted to develop a secure software system which meets government standard for the highest level of security.
- NZ SAAT Services: Individual services are comprised of the SAATS clinicians and the organisations that they are contracted under. These services capture the patient data and record it. This is currently being done by the SAATS clinicians manually and entered into the Medical Examination Record (MER), medical notes and clinical proformas. The MER is a handwritten document that records all aspects of the forensic history and examination. No new data is being captured, the project proposes to assist service providers with a consistent and central process for collecting national data.
- SAATS Contract Holders (DHBs and PHOs): Contract holders will need to ensure that they have systems in place to assist the services with the ability to capture clinical data. For those services where resources are not available, MEDSAC will provide central assistance to the service to achieve this.
- Individuals who have experienced sexual violence that present to SAAT Services: Individuals presenting to the service will see no change to the service due to the proposed project. Privacy statements will be available at all sites to ensure patients are aware of the data practices.
- SAATS Funders: (ACC, Ministry of Health and NZ Police) have no direct role in the project. They are supporting MEDSAC with funding. Required reporting by SAATS already occurs but will be made easier for services through this clinical information collection process. National data will provide funders with better evidence-based information for which to make funding decisions and contract enhancements.

2.4. Affected Business Process

The introduction of SAATSdata will affect the following workflows:

- Individuals who present to a SAAT Service for a sexual assault medical/forensic examination: this group will be made aware of the data collection processes via a secure privacy statement.
- NZ SAAT Services: Each service will need to ensure patients they are working with are aware of the new data collection system, complete new agreement processes, potentially understand and collect data they haven't had to in the past and input that information into the solution or in paper form.
- SAATS Contract Holders (DHBs and PHOs): Contract holders will need to ensure that they have systems in place to assist the services with the ability to capture clinical data. For those services where resources are not available, MEDSAC will provide central assistance to the service to achieve this.

2.5. Governance

SAATSdata and access to the information held within it is governed at a national level by the MEDSAC board, however the individual SAAT Service providers are tasked with management and oversight of their own datasets within SAATSdata.

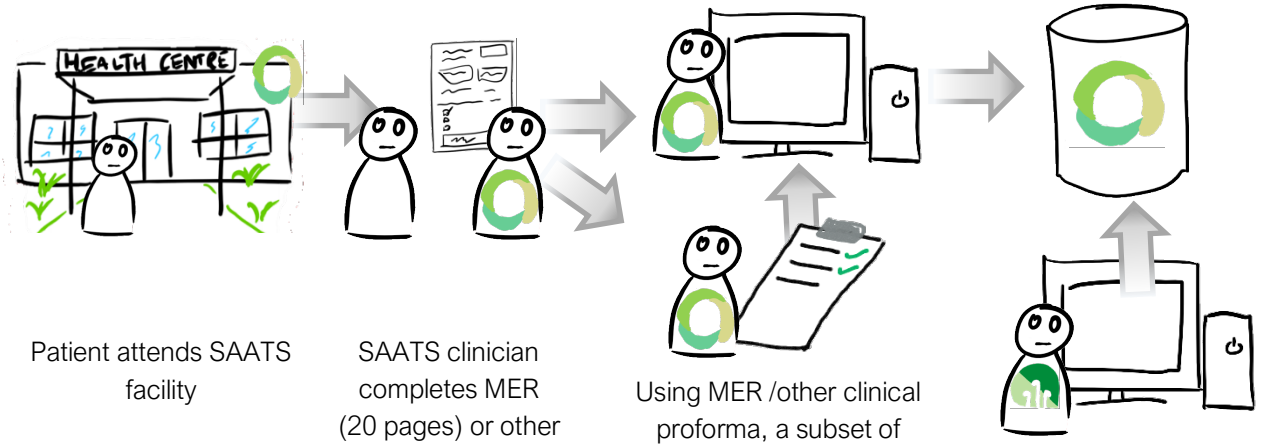
Any requests for information from the database at a national level will be addressed and governed by the MEDSAC board, more local information is managed by the relevant contracted SAAT Service providers.

Information use by each group is described in the following section.

3. Information Workflows

The following workflows result in information being added to or drawn from SAATSdata.

3.1. Patient presents to SAATS



Patient attends SAATS facility

SAATS clinician completes MER (20 pages) or other clinical proforma

Using MER /other clinical proforma, a subset of information is entered into SAATSdata electronic form, paper form or online. Clinician may do this and/or SAATS administrative staff

If no admin support at SAAT Service paper or electronic form is entered by authorised MEDSAC staff (SAATSdata System Manager)

MEDSAC will require that SAATS providers display this notice in their waiting and examination rooms.

PATIENT DATA

We want to improve sexual assault care in Aotearoa, New Zealand.

To help achieve this, we will record information about your visit here today in a secure national database. The database is called SAATSdata. It is owned by Medical Sexual Assault Clinicians Aotearoa (MEDSAC).

We will never record your name or address in this database.

SAATSdata will help us understand who we are and who we are not seeing. It will show us where more funding is needed for medical sexual assault services.

We will store and use your information in accordance with New Zealand privacy laws. The SAATSdata database is managed by the Institute of Environmental Science and Research (ESR).

For a copy of the SAATSdata Privacy Impact Assessment, please scan the QR code or visit https://medsac.org.nz/saatsdata

SAATS providers will be encouraged to notify patients of where and what will happen with their data.

Any paper files provided to MEDSAC are destroyed every week. PDF files are to be stored by SAAT Service providers who remain responsible for their safe and secure storage.

3.2. SAAT Service Provider use of data

The SAAT Service can only see information entered into SAATSdata where they were the provider for that patient event. They can extract this data as they require and use it for their own reporting and planning. Typical uses will be:

- Quarterly report to ACC and contract holders that includes; exam, gender, type of exam, whether it was a Just In Case, historic – this is a built-in report in SAATSdata
- Billing for ACC integrated with ACC system – unique identifier, service item code, number of service items delivered and includes ACC number if there is one (where ACC45 capable) – to be sent to ACC for payment
- Can extract all data to spreadsheet – adhoc analysis – only see their own data

Collated regional and national data will be presented in graph format for SAAT Services to view as a national picture e.g. exam time of day, exam type, cases by ethnicity.

3.3. MEDSAC data use

The MEDSAC team utilise the data for analysis and national reporting. Data is examined at regional and national levels to support activities such as:

- Help refine services and service expectations
- Direct training
- Input to the forensic kit development
- Inform SAATS contract review and development

3.4. Access to data by other stakeholders

No other stakeholders have access to the data captured. Any requests for data will be considered by the MEDSAC board according to their terms of reference. If permission is granted, provision of information is managed by the MEDSAC staff (SAATSdata System Manager).

3.5. Data Collected

The information collected in the system is a mix of administrative (for contract and billing purposes), and clinical details. The table below details the information that the system collects for each event. Every entry is assigned an automatically generated SAATSdata ID and the date it was entered is captured. * = required

	Question	Response options	Comments
Administrative/Reporting	**Patient demographics**		
	MER ID	Unique ID from MER	
	NHI	Patient National Health Index number	Optional entry for SAATS but required by Auckland SAAT Service
	Patient Management System ID	Unique ID from SAAT Service	
	ACC45	Unique ID from ACC45 form	If an ACC45 claim – required for billing purposes
	Age at visit*	Age (years)	DOB is 'identifiable' data, whereas age is not. Important to enable basic demographic description of service users to inform service delivery and monitoring of SA trends over time
	Gender*	• Female • Male • Non-binary • Transgender female • Transgender male • Gender diverse other • Unknown	Important to enable basic demographic description of service users to inform service delivery and monitoring of SA trends over time
	Ethnicity	• Ethnic_1* • Ethnic_2 • Ethnic_3 • Ethnic_4 • Ethnic_5 • Ethnic_6	Record 6 ethnicity options as per 2017 MoH ethnicity data collection protocols
	Service details		
	SAAT Clinic name*	Drop down list with a brief 4-5 letter code to denote clinic	Able to organise data by clinic, will provide means to ensure clinics can only access their own data
	Off-site exam location	• ED • Hospital (other) • Sexual Health • Prison • Other (specify)	
	Initial forensic/non-forensic examination (if not performed by the service - skip to referral section)		
	Crisis Support staff present	• Yes • No	If Crisis Support present
	Referral Source	• Police • Sexual Health • Self-referred • Primary care • ED • Youth service • Crisis service	Provides information about pathways into SAAT Services

	Question	Response options	Comments
		• Oranga Tamariki • Prostitutes collective • Other (state)	
	Historic exam > 1 month	• Yes • No	
	Just in Case exam_1	• Yes • No	
	Just in Case exam_2	[If Yes] – Date of consent to release to Police	
	Date of initial examination	Date	
	Time of examination	Time	Time taken from MER
	Referral (for follow up)		
	Referred from other SAAT Service?	• Yes • No	
	Referring SAAT Service	Drop down list	A drop down list of SAAT Service locations
	Non SAATS referral	• Yes • No	
	Non SAATS referral description	Specify	
Clinical history and examination	**Patient history**		
	GP to be notified	• Yes • No • Unknown	Record of permission given or request to send letter to GP. Assists in continuity of care.
	Mental Health history	• Past • Present • Both • No history • Unknown (i.e. not asked)	
	Disability History	• Physical • Intellectual • Both • No disability • Unknown	Response options taken from Australian SARC database
	History of assault		
	Date of alleged event	Date if known (drop down calendar)	Most recent alleged assault

	Question	Response options	Comments
	Time of alleged event	Time (approx.)	Most recent alleged assault
	If date unknown	• <24hrs • 25-48hrs • 49-71hrs • 3 – 7 days • >7 days – 1mth • >1mth – 12mths • >12mths • Unknown	
	Recollection of assault (full or partial)	• Full • Partial • None	
	Reports pressure applied to neck (strangulation) and/or hand/object over mouth/nose (suffocation)	• Strangulation • Suffocation • None • Both • Unknown	
	Alcohol consumption (in 6hrs prior to alleged event)	• Yes • No • Unknown	
	Suspected DASA (drug assisted sexual assault)	• Yes • No • Unknown	
	Alleged contact type		
	Penetration of vagina/genitalia	• No • Yes • Attempted • Unsure • No Memory • N/A	
	Penetration of anus/rectum	• No • Yes • Attempted • Unsure • No Memory	
	Digital-genital contact	• No • Yes • Attempted • Unsure • No Memory	
	Oral-genital contact	• No • Yes • Attempted • Unsure • No Memory	
	Object penetration of vagina/genitalia	• No • Yes • Attempted • Unsure	Added February 2023 to reflect legal definition of rape

	Question	Response options	Comments
		• No Memory • N/A	
	Object penetration of anus/rectum	• No • Yes • Attempted • Unsure • No Memory	Added February 2023 to reflect legal definition of rape
	Offender history		
	Relationship of offender to complainant	• Partner/ex-partner • Family member • Known < 24 hours • Known >24 hours • Stranger • CSW/client • Unknown • Other	
	Gender of alleged offender (AO)	• Female • Male • Gender diverse • Multiple • Unknown	NOTE: Ongoing discussion in NZ about recording information about gender. Recommend that gender of AO be recorded in the same way as gender of the complainant using StatsNZ categories until 'official' decisions made.
	Number of offenders	• Single • Multiple • Unknown	
	Clinical exam and management		
	Genital exam performed	• Yes • No	
	Genital exam recorded on male/female proforma	• Female • Male • N/A	
	Anogenital findings	• No findings • Acute genital findings • Non-specific finding • Not examined	
	HIV PEP started	• Yes • No	
	Clinician information		
	Examiner name	• Name from dropdown list	Added February 2023

	Question	Response options	Comments
	Hours spent	• Hours: Minutes	Added February 2023
	Nurse/other assistant name	• Name from dropdown list	Added February 2023
	Hours spent	• Hours: Minutes	Added February 2023
	Trainee name	• Name from dropdown list	Added February 2023
	Hours spent	• Hours: Minutes	Added February 2023
Billing	**Initial service type**		
	Initial Service Type	Drop down of ACC billing codes	Required for billing purposes
	Service Billing Period	Date	Required for billing purposes
	Initial visit non-attendance		
	Initial visit non-attendance 1 (SADN3)	Date, Service Type, Billing Period	
	Follow-up activity		
	1st follow-up (SA13/SA13T/SA40/SA40T)	Date, Service Type, Billing Period	
	Subsequent follow-up_1 (SA14/SA14T/SA41/SA41T)	Date, Service Type, Billing Period	
	Subsequent follow-up_2 (SA14/SA14T/SA41/SA41T)	Date, Service Type, Billing Period	
	Follow-up non-attendance		
	Non-attendance follow-up 1 (SADN1)	Date, Service Type, Billing Period	
	Non-attendance follow-up 2 (SADN2)	Date, Service Type, Billing Period	
	Other Charges		
	Paediatrician out of hours callout fee	Date, Service Type, Billing Period	Added February 2023 to reflect SAATS contract

3.6. Common Controls

For any computer system there are certain access controls that need to be in place to secure the information as it is collected, retrieved, updated or deleted. This reviews those controls and how they are addressed by SAATSdata.

3.6.1. De-identified Record

As demonstrated by the data fields section, there is not enough required identifiable information included in SAATSdata records to enable identification of an individual. The only information that goes along with a record being entered into the system is a unique identifier for the record, the unique MER number, the unique SAAT Service identifier from their Patient Management System (PMS), age, gender and ethnicity. Age is captured rather than data of birth to further support de-identification of the record.

The exception to complete de-identification is when an NHI and/or ACC45 is entered for a patient event.

- The NHI number is optional and has been included in the system for SAAT Services that require this information for their internal reporting.
- The ACC45 number (if utilised) is required for invoicing purposes where applicable.

The risk of patient re-identification via the NHI or ACC45 is managed via the following governance controls:

- 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.
- All access and use of data is tracked through an audit trail in to order to ensure data access has been appropriate by all system users.

3.6.2. Identification and Authentication

Only people with user accounts can access SAATSdata. Those user accounts are managed from within the system itself – ESR is not involved in user provisioning.

User accounts have a user name and a password. The passwords are assessed against the rules below. Each login event requires the user to complete a two factor authentication process[1].

- Not be a dictionary word or based on a dictionary word. E.g. P@ssword
- Not be a word found in user's personal information
- Not be telephone number, calendar date, licence plate or other common number

[1] Two factor authentication process: single factor authentication is where you only use one means to identify yourself to a system, such as a username. Two factor utilises a second means to further authenticate you should be able to access the system.

- Not be the username or based on the username e.g. J0hnd0e
- Not be the company name or based on company name. e.g. AcmeCo1
- Not be a keyboard pattern e.g. 1qazxsw2
- Use a upper/lower case as well as digit and symbols
- Consist of a minimum of 10 characters in length
- Consist of a minimum of 16 characters for administrative accounts
- Passwords expire after 6 months and must be reset

3.6.3. Access Control

Once in an IT system your access should be controlled, limiting the actions you can take and information you can see. In SAATSdata the following roles and access are enabled:

Role	Access	Who holds this role
Service Provider	• Can add new cases • Can update their own cases • Can review cases for their service only • Can delete cases entered by their service • Generate required service reports i.e. for ACC and billing • Can reset their password	• SAATS Clinicians • SAATS Administrative staff
Billing	• Can generate billing reports • Can reset their password	• SAATS Administrative staff
System Manager	• Can create, delete or update user accounts • Can set up new providers • Associated users to providers • Can complete all actions other roles can	• Authorised MEDSAC staff – SAATSdata System Manager
Technical System Support	• Can create, delete or update user accounts • Can set up new providers • Associated users to providers • Can complete all actions other roles can	• Authorised ESR technician provided with temporary access as required (not continued open access)

It is a system requirement, as is required for any computer software system, to have trusted staff to install and manage the software; a technical custodian who will have super-user access. This role will be performed by the SAATSdata System Manager (MEDSAC staff member). The SAATSdata System Manager will be responsible for providing user management, analytical

reporting and 'help desk' duties to support the authorised SAATSdata users. The SAATSdata System Manager is bound by strict confidentiality and non-disclosure requirements specified in the employment contract whilst they are employed by MEDSAC, and following the end of their employment. This requirement is no different from any other patient management system and does not indicate a departure from standard data integrity practice. An additional governance control placed on the super-user, and other users, is that all access and use of data is tracked through an audit trail. Regular audits are required to be conducted by all SAAT services utilising the system to monitor appropriate SAATSdata access pertaining to their service data.

An authorised ESR technician will have temporary access provided to the production solution[2] as required for high level system support. The ESR privacy and confidentiality policies address strict confidentiality and non-disclosure requirements in order to protect data integrity. Changes and fixes to the system can be made by ESR without interacting with the production solution.

3.6.4. Backup and retention

All information stored in SAATSdata is backed up nightly, these are stored in the ESR data centre – hosted by Revera. That means should an issue occur, any lost data in the production system can be reinstated with the data from the backup taken the previous night. Any data entered since the last back up will have to be re-entered by SAATS staff.

The whole SAATSdata production system can be re-established within 2 hours.

3.6.5. Audit and Traceability

SAATSdata tracks all changes made to records in the database, those changes include:

- Creation of records
- Retrieval of records
- Updating records
- Deleting records

For each of these the following information is captured:

- Username
- What was done (creation, retrieval, update, deletion)
- When it was done

A record is logged capturing the time and date that a user accesses the system.

SAATS Services are required to conduct regular access audits of SAATSdata use, pertaining to their service data, in order to ensure data access has been appropriate by all system users. Audit reports are a system feature for governance control purposes.

[2] Production Solution: Refer to Glossary of Terms

4. Securing Patient Information

Several steps have been taken by MEDSAC to ensure information is captured and stored securely.

4.1. Firewalls, limited ports and limitation on where traffic can come in from

Going through the Firewall is the only way to reach SAATSdata. Only limited IP addresses can reach the solution, this is managed by the Firewall. Only port 443 is open for those addresses that can access the solution.

The Azure VM host can only be reached via the VPN, all other internet access is disabled for the host.

4.2. Encrypted communication between SAATSdata and users

All traffic to the solution is encrypted using the TLS 1.2 protocol. This is compliant with the NZISM 17.2, Approved Cryptographic Algorithms. A review proxy is used to ensure the end point location of SAATSdata cannot be discovered.

4.3. Use of exclusive networks to communicate with other key integration points

Once traffic reaches the Firewall it is then directed across an encrypted VPN between the ESR equipment and the Azure host virtual machine.

4.4. Terms of use agreed to by all users before they are given access

As a user access the SAATSdata system for the first time they will be prompted with a terms of use, they must accept these terms of use before being able proceed into the system. These terms require that users:

- Will not access data for any other purpose beyond what it was collected for
- If they download data they will not use it for a purpose other than what it was collected for
- They will keep their password and username private and not share it with any other person
- If they believe their account has been compromised they will report it immediately to MEDSAC
- Breach of any of these terms will result in their account being disabled

4.5. Controlled user account allocation

User access is managed by MEDSAC. If a SAAT Service staff member leaves, the SAAT Service notifies the MEDSAC team so that their account can be disabled – meaning it can no longer be used to access SAATSdata.

A regular audit of user accounts will be performed by all SAAT Services to ensure no accounts remain for departed staff members.

The controls around IP address restrictions further ensures that those that have departed a SAAT Service cannot access the solution unless they are on the SAAT Service network.

4.6. Penetration testing

An independent audit has been completed of SAATSdata solution by Aura Information Security. This report concluded there were some minor issues that have since been addressed and verified as addressed by ESR.

The assessment was conducted from a black box perspective. A black box test is conducted without knowledge of internal application structure, logic, or processes. This type of testing reveals security vulnerabilities purely via interaction with the application and examination of output dependant on controllable inputs. A black box approach is limited regarding the types of vulnerabilities it can discover unless a full compromise of a system takes place.

The scope of this assessment was SAATSdata web application. Testing was carried out remotely from Aura's Auckland office.

This security assessment was based on industry standards for testing web and mobile applications as outlined by the Open Web Application Security Project (www.owasp.org).

4.7. Data migration testing

Historic data already captured by the Wellington SAAT Service has been uploaded into SAATSdata. This was transferred via encrypted file to the ESR team who uploaded it directly in to the database. Accuracy was assessed by the SAAT Service themselves.

It is intended that the same process will also occur for the historic data captured by the Auckland SAAT Service.

5. 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.

5.1. 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

5.2. 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:	-

5.3. 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.

5.4. 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:	-

5.5. 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

5.6. 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:	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.

5.7. 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:	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.

5.8. 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:	-

5.9. 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:	-

5.10. 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.

5.11. 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 – (a) the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to 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.

5.12. Principle 12: Disclosure Outside New Zealand

Principle:	Principle 12 sets rules around sending personal information to organisations or people outside New Zealand. A business or organisation may only disclose personal information to another organisation outside New Zealand if they check that the receiving

	organisation is subject to the Privacy Act, or privacy laws that provide comparable safeguards to the Privacy Act, or will adequately protect the information.
Current:	Data is only reported at national, district and regional levels and will not be shared outside of New Zealand.
Change:	There are no changes from the current methods of data reporting restricted to New Zealand only.
Risk:	No new risks
Mitigation:	-

5.13. Principle 13: Unique Identifiers

Principle:	Rule 13 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. SAAT 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.

6. Glossary of Terms

Term	Description
Access Audits	Regular access audits generated by SAAT 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

Term	Description
	organisation of doctors and nurses formed to develop and maintain standards of best practice in the delivery of medical 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.