Zanti Confidentiality Policy – June 2022

Client Confidentiality

Purpose

The purpose of this policy is to ensure that that all client information is private and confidential. Zanti Consulting is responsible for maintaining client privacy in accordance with all federal and local / state regulations.

Policy

Under no circumstances will members of Zanti Consulting Pty Ltd discuss, or in any way reveal client information to unapproved employees, colleagues, other clients, family or friends, whether at the practice or outside of it, such as in the home or at social occasions. This includes client accounts, appointments, referral letters or any other clinical documentation.

Zanti Consulting Pty Ltd practitioners and other employees are aware of confidentiality requirements for all client encounters and understand that significant breaches of confidentiality may provide grounds for disciplinary action or dismissal.

Client Information Management

Purpose

The purpose of this policy is to clearly state the protocol for handling personal information, including health information.

Policy

Zanti Consulting Pty Ltd have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of this information is every client's right.

This policy outlines how the practice handles personal information collected (including health information) and how the security of this information is protected. A privacy statement is made available to clients and anyone who requests it.

There are no degrees of privacy. All client information must be considered private and confidential, even that which is seen or heard. Therefore, such information is not to be disclosed to family, friends, employees or others without the client's approval. Sometimes details about a client's medical history or other contextual information, such as details of an appointment, can identify them - even if no name is attached to that information. This is still considered health information and it must be protected. Client information may not be disclosed either verbally, in writing, in electronic form, or by copying either at the practice or outside it, during or outside work hours, except for strictly approved use within the client care context, or as legally directed.

Privacy Statement

This statement informs clients how their health information will be used. This includes the sharing of information to other organisations to which the practice usually discloses client health information, and any law that requires the particular information to be collected. Client consent to the handling and sharing of health information should be provided at an early stage in the process of client care. Clients should be made aware of the collection statement when giving consent to share health information.

In general, quality improvement or audit activities for the purpose of seeking to improve the delivery of a particular treatment or service is considered a directly related secondary purpose for information use or disclosure. Specific consent for this use of client health information is not required.

Staff Access

Zanti Consulting Pty Ltd client health records can be accessed by an appropriate team member when required. All client health records are electronic and accessible through Power Diary by appropriate employees.

Zanti Consulting Pty Ltd employees have different levels of digital access to client health information. To protect the security of health information, employees do not give their computer / Power Diary passwords to others in the team.

Personal health information should be kept where employee supervision is easily provided and kept out of public view and access.

Computer Security

Active and inactive client health records are kept and stored securely within Power Diary.

This practice is considered paperless and has systems in place to protect the privacy, security, quality and integrity of the personal health information held electronically. Appropriate employees are trained in computer security policies and procedures.

Zanti Consulting Pty Ltd computers and servers comply with computer security standards.

Administration Security

Reception and other practice employees should be aware that conversations in the main reception area can often be overheard in the waiting room. As such, employees should avoid discussing confidential and sensitive client information in this area.

Whenever sensitive documentation is discarded, the practice uses an appropriate method of destruction. Documents are placed in the confidential waste bin, and confidential waste is disposed of securely. All computers, memory sticks or CDs are disposed of properly by a designated employee.

Zanti Consulting Pty Ltd employees ensure that all forms of client information are not visible to the public.

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where client information is sent by mail, the use of secure postage or a courier service is used - determined on a case by case basis. Return address states the physical or post office address, but the practice name is not identified on the envelope.

Incoming client correspondence and diagnostic results are opened by a designated employee.

Items for collection or postage are left in a secure area out of public view.

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to practitioners and other approved staff. Faxing is point to point, and will therefore usually only be transmitted to one location.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver. Each fax is accompanied by a cover sheet, the cover sheet includes the words “confidential” and a fax disclaimer notice that affiliates with Zanti Consulting Pty Ltd.

Emails are sent via various nodes and are at risk of being intercepted. Client information may only be sent via email if it is securely encrypted according to industry and best practice standards.

Third-Party Requests

Purpose

The purpose of this policy is to define the procedures for timely, approved and secure transfer of client health information in relation to valid requests.

Policy

Requests for third-party access to client records should be initiated by either receipt of correspondence from a lawyer, government agency, another source including the examples listed below, or by the client with a written request. Where a client’s written request and / or signed approval is not obtained, the practice is not legally required to release information without a court order.

Requests for access may be received from various third parties including:

- Subpoena / court order / coroner / search warrant
- Relatives / friends / caregivers
- External practitioners & healthcare institutions
- Police / lawyers
- Health insurance companies / workers compensation / social welfare agencies
- Employers
- Government agencies
- Accounts / debt collection
- Research / quality assurance programs

- Media

Transfer of Client Records

Purpose

The purpose of this policy is to guide employees in the process of timely, approved and secure transfer of records.

Policy

Transfer of records from this practice can occur in the following instances:

- For legal reasons, when a record is subpoenaed to court
- When a client asks for their record to be transferred to another practice, due to moving residence or for other reason
- Where an individual record report is requested from another source
- Where the practitioner is retiring and the practice is closing

Client Access to Their Health Information

Purpose

The purpose of this policy is for Zanti Consulting Pty Ltd employees to understand and comply with client rights in regard to accessing a client's own health information.

Definitions

Person Responsible describes a parent of the individual, a child or sibling of the individual, who is at least 18 years old, a spouse or de-facto spouse, a relative (at least 18 years old), a member of the household, a guardian or a person exercising an enduring power of attorney granted by the individual that can be exercised for that person's health, a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency.

Policy

Clients have the right to access their personal health information. This principle obliges health practices and other parties that hold health information about a person to grant access to their information on request, subject to certain exceptions and payment of fees (if any).

Zanti Consulting Pty Ltd has a privacy policy in place that outlines the management of health information, and the steps a client must take to access their health information. This includes the different forms of access and the applicable time frames and fees.

Zanti Consulting Pty Ltd respects each client's privacy, and allows access to information via personal viewing in a secure private area. The client may take notes about the content of their record, or may be given a photocopy of the requested information. A practitioner may explain the contents of the record to the client if required. An administrative charge may be applied, at the practitioner's discretion.

Release of information is an issue between the client and the practitioner. Information will only be released according to privacy laws and at the practitioner's discretion. Requested records are reviewed by the practitioner prior to their release and written approval must be obtained.

Data Breach Notification

Purpose

The purpose of this policy is to advise Zanti Consulting Pty Ltd employees on actions required if a data breach occurs

Definitions

Data Breach describes circumstances when personal information that an entity holds is subject to unapproved access. This can be malicious action, human error, or a failure in handling or security.

Personal Information is information about an identified individual or an individual who is identifiable from the information.

Policy

A data breach occurs when personal information that Zanti Consulting Pty Ltd holds is subject to unapproved access or disclosure or is lost. Data breaches can happen to any practice.

Zanti Consulting Pty Ltd can reduce the reputational impact of a data breach by effectively reducing the risk of harm to affected individuals, and by demonstrating accountability in their data breach response.

Procedure

Zanti Consulting Pty Ltd employees understand the importance of being transparent when a data breach occurs - whether or not it is likely to cause serious harm to impacted individuals. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that Zanti Consulting Pty Ltd takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in the practice's personal information handling capability.

Examples of a Data Breach

- Loss or theft of a physical device (such as a laptop or paper records)
- Unapproved access by an employee or other person
- Inadvertent disclosure due to human error, such as a fax being sent to an incorrect number
- Disclosure to a third party due to an inadequate verification process

Consequences of a Data Breach

- Financial loss
- Potential damage to clients' reputations
- Damage to clients' physical or mental well being
- Responding to a Data Breach

As data breaches can be caused or exacerbated by many factors, there is no single way of responding to a data breach. Each breach should be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

- Contain the data breach to prevent any further compromise of personal information
- Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm
- Notify individuals, government bodies and medical indemnity if required
- Review the incident and consider what actions can be taken to prevent future breaches

Zanti Consulting Pty Ltd takes each data breach or suspected data breach seriously, and moves immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed.

Steps will be taken to contain, assess, and notify either simultaneously or in quick succession. In some cases, it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.

Zanti Consulting Pty Ltd determines how best to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, additional steps may be taken that are specific to the nature of the breach.