Data Breach Notification

Last updated 2nd April 2026

The purpose of this policy is to advise AVA Orthopaedics 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 AVA Orthopaedics holds is subject to unapproved access or disclosure or is lost. Data breaches can happen to any practice.

AVA Orthopaedics 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

AVA Orthopaedics 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 AVA Orthopaedics 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:

1. Contain the data breach to prevent any further compromise of personal information
2. 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
3. Notify individuals, government bodies and medical indemnity if required
4. Review the incident and consider what actions can be taken to prevent future breaches

AVA Orthopaedics 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.

AVA Orthopaedics 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.

Reporting Data Breaches

What to include in a data breach report:

- Your practice or agency's name and contact details
- Description of the data breach
- Description of the types of information involved
- Recommendations about the steps individuals should take in response to the data breach