How to Report a Serious Incident

Serious incidents include death; severe self harming; suicide attempt; overdose; harm to or from others; acts or omissions in care that result in moderate or severe harm, including incidents that prevent (or threaten to prevent) an organisation's ability to continue to deliver an acceptable quality of safe care. Some data breaches are classed as a serious incident. Serious incidents in healthcare are events where the potential for learning is so great, or the consequences to members, families and carers, staff or organisations are so significant that they warrant our particular attention to ensure these incidents are identified correctly, investigated thoroughly and, most importantly, trigger actions that will prevent them from happening again. We will ensure that in managing complaints and serious incidents it complies with confidentiality and data protection policies.

All serious incidents must be reported verbally on the same day that the incident has come to your attention to the lead clinician who is on safeguarding duty and offering safeguarding consultations via the clinical panel for that day. Our safeguarding team can be contacted via the clinical panel on your Experts Platform Dashboard. Please see our Senior Clinician Availability Rota for guidance on who to contact for assistance with managing serious incidents. There is dedicated support on duty everyday working day. Do not delay making referrals or contacting safeguarding agencies in an emergency.

You will be required to complete a Serious Incident Notification Form. This must be completed and forwarded to the lead clinician who is on safeguarding duty and offering safeguarding consultations via the clinical panel for that day within 24 hours of becoming aware of the incident.

There is a dual reporting/escalation procedure for data breaches which also need to be escalated/reported to the Director of IT Security and Infrastructure (wanja-eric.naef@helloself.com) on the same day that the incident has come to your attention. Please read this policy in conjunction with our Associate Data and Data and Technology Handbook.

If Wanja-Eric Naef is unavailable please report to our Chief Technology Officer (mike.unwin@helloself.com). Following a data breach you will need to complete an ICO self assessment, forward the results to the Caldicott Guardians in the Information Governance Team (Wanja-eric.naef@helloself.com or pelumi.olawale@helloself.com) to take appropriate action.

A rapid review and immediate action will take place to establish the facts; ensure security of data; ensure the safety of the member(s), other service users, members of the public and staff; and to secure all relevant information to support further investigation. Given the serious nature of the incident you will be expected to meet with the a member of the Clinical Excellence Team within three days of the serious incident coming to your attention.

We promote a non blaming approach to serious incidents and wish to establish an environment where it feels safe to share, learn and develop. We are here to support our therapists and ensure our members receive safe and effective care. A senior clinician will continue to check in with you and your wellbeing given the emotional impact of caring for others. We have helpful resources shared on the associate drive too. We appreciate your feedback on the services we provide and your experience of working with us.

Our serious incidents procedure is as follows: