# STATE INDEMNITY GUIDANCE: 15
# IT CYBER-ATTACK - TUSLA (FROM 14 MAY 2021)

## Introduction

The State Claims Agency (SCA) recognises the enormous impact, and associated risks, of the IT cyber-attack on Tusla systems, which occurred on 14 May 2021. The purpose of this document is to provide State indemnity advices, and risk management guidance, in respect of the General Indemnity Scheme (GIS), to all Tusla servants and/or agents following the cyber-attack.

## Does State indemnity apply?

It is recognised that, in many situations, Tusla may be providing care and services without access to service users' electronic records. The SCA confirms that all approved business activities carried out by Tusla, including those relating to the safety of service users, staff and members of the public, are covered by the GIS. The GIS indemnifies Tusla its servants and/or agents in respect of any claims for personal injury and/or third-party property damage, arising from the negligence of Tusla, its servants and/or agents.

## Does State indemnity apply to claims alleging data breach?

Claims taken against Tusla by a party alleging personal injury associated with a data breach, resulting from the cyber-attack against Tusla, will be managed by the SCA. This includes claims for personal injury by persons, where such persons allege that a data breach caused the person trauma or psychological sequelae. Where a claimant alleges a data breach in the absence of any allegation of a personal injury, such a case will not fall within the SCA's remit.

## Incident reporting

The National Incident Management System (NIMS) has not been affected by the cyber-attack. As a precaution, it has been necessary to temporarily suspend NIMS access to Tusla to minimise any associated risk.

The statutory obligation to report incidents will be fulfilled by recording incidents on paper National Incident Report Forms (NIRFs). All completed NIRFs should be retained for inputting on NIMS at a later date. In order to report serious/sensitive incidents, please liaise with your designated Tusla contact:

- National Health & Safety Manager
- Risk and Incident Officer

## Risk management advice

- The SCA advises that Tusla's servants and/or agents, if and where possible, should document in the records, or temporary records, the limitations to the care and/or services being delivered, if applicable, as a consequence of the IT cyber-attack.

- Where relevant and appropriate, Tusla's servants and/or agents should communicate to those availing of its services that the ability to provide care/services is being limited by the circumstances described above, and such communications should be documented in the record.

- The SCA advises that formal risk assessments should be undertaken to include, but not limited to, provision of services and storage and management of temporary records.

- The use of alternative IT-based communication channels should be risk-assessed, ensuring that any alternative mechanisms are appropriately secure and GDPR compliant.

## How can I contact the SCA?

Should you have any queries please contact the National Health & Safety Manager or the Risk and Incident Officer who will liaise with the SCA regarding your query.