Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Office of the Chief Clinical Officer
Dr Steevens' Hospital|Steevens' Lane|Dublin 8|D08 W2A8
email: cco@hse.ie

Oifig an Phríomhoifigigh Cliniciúil
Ospidéal Dr Steevens|Lána Steevens|Baile Átha Cliath 8|D08 W2A8

Patient Safety Impact Memo

Friday 25 June 2021

Office of the Chief Clinical Officer, HSE

Status Update

Our focus, as always, is on the safe delivery of patient care. However, I remain conscious of the impact of this incident on staff health and wellbeing. I acknowledge the impact this lengthy incident is having on all grades at all levels within the service. Once again, I want to express my gratitude to you as you continue to manage this crisis with the highest level of professionalism and commitment. The agility of your response in such a dynamic and high-risk environment is remarkable. I am grateful also to patients and service users for their continued patience and support through this difficulty period.

This is the seventh memo to provide updates on clinical risks and provide guidance for clinical services as we enter the seventh week of the HSE IT System Cyberattack. Recovery has been underway for several weeks with activity restored on most sites. The number of patients presenting to ED remains exceptionally high, both GP referrals and self-referrals and trolley numbers have risen. We remain concerned about the added strain and risk this generates.

Communication has re- issued to GPs and by public media to raise awareness of potential delays in unscheduled care and to avoid hospitals where possible. There has been further restoration of important ICT systems in areas such as CCSD this week and further progress is expected in areas such as the Endorad system over the weekend. However, colleagues in ICT have advised that operational capacity will remain constrained until all ICT systems, including the many smaller systems, are restored. We continue to apprise ICT of the clinical risks generated by this cyberattack and the cumulative nature of the risk.

This week, restoration of internet access has been prioritised and it is expected to function from Monday 28th June. As was the case with email, access will be intermittent for some time. Restoration of the internet will enable the use of web based applications used by many clinical and administrative systems in our service.

The onerous task of uploading backlogs and reconciling patient records continues on most sites and the level of stress and risk involved in this process is well recognised. As this work progresses

evidence of incidents and near misses emerge. It is critical therefore that we continue to manage these risks to mitigate them where possible, identify, report, and manage incidents and share lessons learned to prevent recurrence. The NIMIS has been activated so you are now asked to revert to the electronic reporting system. Your commitment and creativity in developing highly innovative ways to deliver the safest possible care in extraordinarily difficult circumstances has served patients well in recent weeks.

Over the first weeks of the incident, even with these contingencies in place and with limited ICT recovery, most providers curtailed services. Scheduled care has, of necessity, now resumed in hospitals. Recovery in community services has been slower and this represents a burden on elements of the care pathway. While the level and pace of recovery remains variable, and I am grateful for your collective patience and collaboration.

Principles

Advice on clinical management over the course of this incident has been underpinned by the need to prioritise patient safety and maintain critical clinical services with the lowest practical level of risk in a very difficult environment. The ICT focus has shifted to internet access, recovery of multiple smaller ICT systems, integration of major systems and community service restoration. In clinical services the focus is on management of recovery and the safe resumption of services as quickly as is practical while clearing administrative backlogs. It remains essential that this is closely monitored at service level to enable those services that can deliver scheduled care with an acceptable level of clinical risk to do so, without overburdening affiliated services. Radiology and laboratory services ability to resume activity remains limited until full internet access is restored and recovery is established. Thus, overall operational capacity will remain restricted until full connectivity is restored.

There may be some residual effects attributable to new Firewalls.

The principles are to:

1. Prioritise patient safety.
2. Protect unscheduled and urgent care.
3. Ensure continuation of time-critical care and treatment e.g., dialysis, surgical procedures, radiotherapy.
4. Ensure involuntary admissions in Mental Health Services are conducted as safely as possible.
5. Enable staff to work as safely as possible as we recover the usual digital support and enablement.
6. Reinstate services in a manner that does not threaten recovery or compromise the safe follow-up of patients seen during the cyberattack.
7. Provide meaningful communication to address patient's and other service users concerns and enable informed decision making.
8. Support staff and acknowledge the risks to them of operating in an environment where we begin to recover the usual information systems support.

Updated Risks

The integrated clinical and operational risk subgroup of the National Crisis Management Team now meets each Monday and Friday to continue to guide the operational response based on clinical priority. Earlier memos described how this incident impaired access to patient records, information management systems and timely accurate diagnostic tests. As such it creates a risk to patients and service users because of inadvertent clinical error, delayed diagnosis, and delayed treatment. The cumulative effect of risks is now evident and new risks are emerging as scheduled procedures become urgent etc. Risk accrues daily as does the adverse impact on recovery. Backlogs in clinical appointments and reconciliation of patient records and investigations with originals remain an independent risk that will prolong the recovery phase of this incident placing additional pressure on our system, staff and ultimately patients.

We identified overarching clinical risks which are shared by all services inherent in the absence of current IT and digital systems six weeks ago remain active until recovery is complete:

1. Risk of harm to patients because of clinical errors related to lack of access to clinical notes.
2. Risk of harm to patients because of reduced access, delayed diagnosis, and treatment due to widespread slowing of all internal processes.
3. Risk of harm to patients because of severe restriction in GP access to diagnostic laboratory and radiology tests.
4. Risk of harm to patients because of reliance on telephone and written ordering of tests and communication of results, with risk of lost results.
5. Risk of harm to patients because of manual reporting with transcription errors in handwritten results.
6. Risk of potential breaches of GDPR, which must be managed in the context of the immediate priority of managing clinical risk to the patient.
7. Patient and service user fear and frustration related to uncertainty and delays which will increase as the incident progresses; and
8. Risk to staff of working in a high stress environment in the absence of usually IT supports.

Likewise, the specific risks for foundational services and particular patient groups remain active, albeit mitigated by substantial recovery e.g., Laboratory, Radiology and Cancer. We continue to capture additional risks and mitigations for important clinical areas e.g., Endoscopy, High Tech Infusions

Clinical Guidance:

1. Information updates are provided on the HSE website and individual hospital websites. These are continually revised as the incident and recovery progresses and should be referred to for the most up-to-date information available.
2. The State Claims Agency has published guidance on their website with regards to indemnity https://stateclaims.ie/uploads/publications/State-Indemnity-Guidance_IT-cyberattack-on-the-health-and-social-care-sector-from-14-may-2021_21.5.21_2021-05-21-150239_tytw.pdf

3. A daily Cyber Security Incident update is posted on the HSE website and can also be followed @hselive on Twitter.
4. CCO advice on options for the management of accumulated laboratory samples issued on May 25 remains active.
5. Communication has issued to all sites outlining presumptive ICT recovery timelines for major systems including email
6. The differential pace and level of recovery is such that the ability to deliver clinical services will also vary. Active ongoing, communication with local management and GPs is essential to optimise care.
7. Advice to GPs has issued and is updated weekly. Outward HealthLink communication to GPs has been restored. Arrangements are in place to enable GPs to order a limited suite of laboratory tests from private laboratories. This is a temporary measure to while systems recover in the hospital laboratories that normally provide service to GPs.
8. Services to prioritise delivery of urgent, unscheduled, and time-critical care within the limitations of the impact of the incident.
9. Services should continue provide scheduled care subject to risk assessment in the recovery phase. The risk assessment should consider the impact on other services.
10. The need to safely manage volume of demand is once again reiterated. The efforts made across the community and hospital service to reduce requests for investigations have made an important contribution to managing this situation and it is essential that this continues as a very high level of demand will compromise overall safety and recovery.
11. As recovery progresses, clinicians should remain mindful of the differential pace of recovery in some diagnostic services when scheduling activity and ordering investigations.
12. Support for less experienced colleagues is essential as is peer to peer support under these, now prolonged, difficult circumstances.
13. It is important for all staff to comply with the National Incident Management Policy. The electronic National Incident Management System (NIMS).has now been reactivated.

Thank you all again for your response to this crisis and to assure you that, within the HSE and with Government departments, we are committed to support you as we work to resolve and restore IT systems to deliver clinical care. Please disseminate this memo to colleagues who do not have access to HSE email or mobile phones.