Maintaining infectious disease surveillance during a national IT outage: lessons from the Republic of Korea's 2025 data centre fire

Seunghyun Lewis Kwon,[a] Seul-Ki Kang,[a] Jihee Lee,[a] Gyehee Lee[a] and Hyungmin Lee[a]

Correspondence to Hyungmin Lee (email: sea2sky@korea.kr)

Problem: On 26 September 2025, a fire at the National Information Resources Service Data Centre disabled the Infectious Disease Information System and halted automated surveillance in the Republic of Korea.

Context: The information system is the backbone of the country's infectious disease surveillance network, integrating clinical, laboratory and epidemiological data via an automated electronic notification interface. Diseases are categorized into Classes 1–4, based on their potential impact and level of urgency. This supports decision-making on outbreak preparedness and response.

Action: The Korea Disease Control and Prevention Agency immediately designated its 1339 call centre as the reporting channel for urgent Class 1 infectious diseases. Within 24 hours, it had developed temporary cloud-based reporting tools enabling local health centres to report Class 2 and 3 diseases. Using Naver Forms, health centres reported only essential infectious disease variables based on notifications received from medical institutions via fax or phone. Sentinel surveillance data for Class 4 diseases were collected using standardized Excel templates via Google Forms. Interagency meetings were routinely held to ensure transparent coordination.

Outcome: Class 1 notifications continued through the 1339 hotline during the outage, which lasted until 28 October 2025. Following system restoration, disease-specific totals from the temporary cloud-based reporting tools and the restored datasets showed high overall consistency (Pearson correlation coefficient = 0.99, $P < 0.001$).

Discussion: Essential surveillance functions can be maintained during a nationwide IT outage through adaptive reporting mechanisms and strong institutional coordination. Infrastructure redundancy, disaster recovery capacity and regular simulation exercises are also critical for maintaining surveillance continuity.

PROBLEM

On 26 September 2025, the Infectious Disease Information System (IDIS) in the Republic of Korea shut down, paralysing nationwide automated disease reporting and laboratory notifications. The source of the disruption was a fire at the National Information Resources Service (NIRS) Daejeon Data Centre. A lithium battery exploded during a replacement operation on the uninterruptible power supply in the NIRS server room.[1] Though there were no significant casualties, the large-scale fire burned for nearly 22 hours, disabling hundreds of government information systems.[2]

Heavy reliance on a centralized information system exposed the vulnerability of national infectious disease surveillance systems. Although a disaster recovery system with multiregion redundancy was under development, it was not yet fully operational, making the damage catastrophic.[3] Without online access to its core surveillance platform, the Korea Disease Control and Prevention Agency (KDCA) risked being disrupted for the foreseeable future. Consequently, alternative reporting channels to maintain essential surveillance functions and ensure the continuity of infectious disease monitoring were crucial.

CONTEXT

IDIS underpins the Republic of Korea's infectious disease surveillance network. It integrates clinical, laboratory and epidemiological data from public and

[a] Division of Infectious Disease Control, Korea Disease Control and Prevention Agency, Cheongju, Republic of Korea.
Published: 15 June 2026
doi: 10.5365/wpsar.2025.16.5.1368

private health-care facilities, supporting real-time outbreak detection and prompt response.[4] The reporting system categorizes diseases into Classes 1–4, based on impact and urgency. The details of each disease class are described elsewhere.[5] **Fig. 1** illustrates the comprehensive flow of surveillance data. The process begins with physicians at medical institutions reporting infectious disease cases to public health centres, which then transmit the information to local governments and KDCA. Class 1 diseases must be reported immediately, and Class 2 and 3 diseases must be reported within 24 hours. Separately, sentinel institutions report Class 4 diseases within 7 days directly to KDCA, which analyses the incoming data and provides feedback to each reporting level to support timely response.

IDIS receives real-time reports from health-care facilities and clinical laboratories through an integrated electronic notification interface. These reports include essential surveillance variables such as patient demographics, disease names, symptoms and laboratory results. Data are continuously aggregated at KDCA's central surveillance unit. Once verified, the reported data are simultaneously shared with relevant bodies such as the Ministry of Health and Welfare, the Ministry of the Interior and Safety, and local governments. This enables outbreak alerts, emergency communication with the public and a unified government response.[4]

ACTION

Within the first few hours of the outage, KDCA activated its Emergency Operations Centre (EOC), which manages a nationwide hotline network, specifically the 1339 call centre and a 24-hour public health hotline.[6] This hotline connects residents, health-care providers and local health authorities to optimize disease reporting and risk communication. During the crisis, the call centre's primary function was reoriented from a general public information channel to an emergency reporting channel for urgent case notifications and the immediate reporting of critical events. The EOC received time-sensitive reports and maintained direct communication channels for Class 1 diseases such as avian influenza, Middle East respiratory syndrome and viral haemorrhagic fevers. When clusters of Class 2 and 3 diseases occurred, health-care providers were instructed to immediately contact the EOC by phone to ensure outbreak containment.

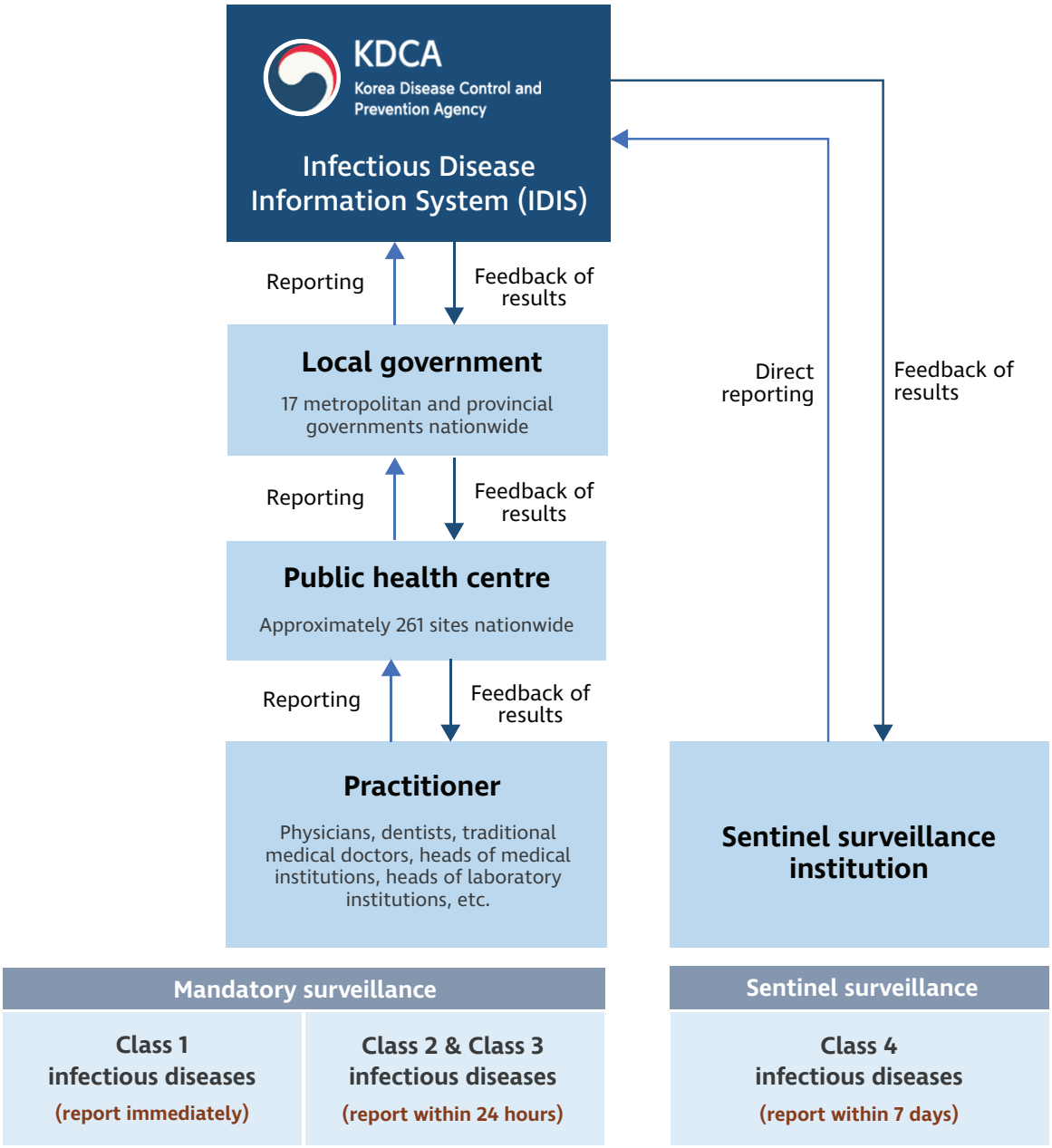
Subsequently, KDCA introduced temporary reporting channels to maintain uninterrupted mandatory infectious disease surveillance of Class 2 and 3 diseases, as collecting this volume of data via phone or fax was not feasible. KDCA selected Naver Forms, a commercial cloud-based reporting tool, for this stream because reporting of both these classes of diseases required rapid, case-based entry of essential surveillance variables by local public health centres. Field officers at local public health centres submitted case notifications through a cloud-based interface accessible by both computers and mobile devices. Each form captured essential surveillance variables such as disease name, age range, reporting date, number of reported cases and case classification, mirroring the key fields of IDIS. Submitted entries were automatically logged into a central spreadsheet to prevent duplication and maintain data quality, reviewed by KDCA's surveillance analysts, and verified by the four Regional Centers for Disease Control and Prevention through telephone follow-up when necessary.

In parallel, KDCA distributed standardized Excel spreadsheet templates for Class 4 sentinel surveillance of diseases, such as COVID-19 and influenza, to designated hospitals and local clinics. Google Forms was selected for this stream specifically for its direct file upload functionality. Unlike Naver Forms, Google Forms enabled these medical institutions to directly upload their weekly reports using standardized Excel templates to maintain routine monitoring.

Both platforms collected only essential, non-identifiable surveillance variables. No direct personal identifiers were collected, such as name, personal identification number or date of birth. Also, access to submitted data was restricted to authorized personnel to ensure data privacy. Compliance with the temporary reporting scheme was supported through existing reporting obligations, instructions delivered through established emergency communication channels, and KDCA's centralized review of submitted reports.

The Central Disaster and Safety Countermeasure Headquarters was established following the outage to serve as the secretariat for intergovernmental communication and decision-making.[7] It supported KDCA primarily through intergovernmental coordination during

Fig. 1. **Flowchart of infectious disease surveillance reporting, Republic of Korea**



the outage by convening meetings regularly with relevant government agencies. Through this process, information on the situation was shared transparently, risks were assessed and recovery plans were disseminated. Within the disease control sector, KDCA held regular internal meetings where updates on data restoration, emergency reporting and field-level challenges were circulated. The Agency disseminated announcements and operational guidance on the temporary reporting scheme through its existing emergency communication network, including the 1339 call centre, direct phone communication with local public health centres and reporting institutions, and regular coordination meetings. These same channels were used to respond to queries, clarify reporting procedures and share updates on emergency reporting and system restoration. Through these communication channels,

KDCA maintained the information flow between central and local levels and facilitated the sharing of critical alerts and public health decisions despite the system outage.

OUTCOME

IDIS functionality was restored on 28 October 2025. KDCA requested that local public health centres upload all official disease notification data reported from medical institutions during the outage to IDIS by 18 November.[8] A data reconciliation process was then conducted to assess the consistency of the temporary reporting data against the official IDIS records. **Fig. 2** summarizes the chronology of the key surveillance continuity interventions and recovery milestones during the outage.

Using Pearson's correlation analysis, disease-specific total case counts reported through the temporary cloud-based reporting tools were compared with the corresponding totals in the restored IDIS dataset covering the same reporting period. This analysis was not intended to assess epidemiological relationships among diseases; rather, each disease was treated as a paired unit of comparison between the two data sources. The comparison focused on Class 2 and 3 infectious diseases – specifically vaccine-preventable diseases, waterborne and foodborne infections and viral hepatitis, as these categories accounted for the majority of emergency notifications during the outage. As shown in **Table 1**, the Pearson correlation coefficient was 0.99 ($P < 0.001$). Some disease-specific differences were observed, including for varicella and viral hepatitis C, for which IDIS counts were higher than the temporary reporting counts. These differences likely reflect the subsequent inclusion in IDIS of additional cases validated via laboratory confirmation through routine reporting pathways following system restoration.

This high correlation suggests that the emergency reporting methods preserved the overall consistency of surveillance information during system disruption. The combination of web-based survey form submissions, hotline communication and regional centre verification ensured the continuity of mandatory surveillance. Data comparison also confirmed that the essential variables were sufficient to sustain daily monitoring and timely response. Furthermore, weekly sentinel surveillance reports were published without interruption during the outage. These easy-to-build and highly accessible solutions enabled the continuation of regular nationwide case-reporting. This experience vividly demonstrates that flexible data collection tools that are independent of the official system can preserve critical reporting capacity during large-scale IT disruptions.

DISCUSSION

The 2025 fire at the NIRS Daejeon Data Centre highlighted several lessons to strengthen surveillance resilience in the Republic of Korea. First, the outage exposed the inherent vulnerability of concentrating critical health information infrastructure in a single facility, underscoring the importance of geographically distributed backup infrastructure. Second, it demonstrated the need for a fully operational and routinely tested disaster recovery system, including backup IT infrastructure and predefined recovery procedures for restoring essential surveillance functions if the primary system were to become unavailable.[9] Third, the experience underscored the importance of regular simulation drills and business continuity exercises. The World Health Organization (WHO) Regional Office for the Western Pacific, through its *Asia Pacific Health Security Action Framework*, has consistently urged Member States to support prevention and preparedness for public health emergencies and strengthen the resilience of health security systems to respond.[10] Finally, strong institutional coordination can help maintain essential surveillance functions when technology fails, as demonstrated by KDCA's rapid activation of communication networks and robust interagency collaboration.

This report has several limitations. The comparison between the temporary and restored surveillance datasets was based on aggregated disease-specific counts for the same reporting period and Pearson's correlation analysis, without daily or regional analyses or formal measures of agreement. Furthermore, no formal indicators of response times or measures of broader public health impact were available during the outage. Therefore, the findings should be interpreted as evidence of overall surveillance continuity rather than exact agreement between the systems or a comprehensive assessment of public health impact.

In August 2025, before the outage, the Government of the Republic of Korea underwent its second WHO

Fig. 2. **Timeline of key surveillance continuity interventions during the national IT outage, Republic of Korea, September–November 2025**

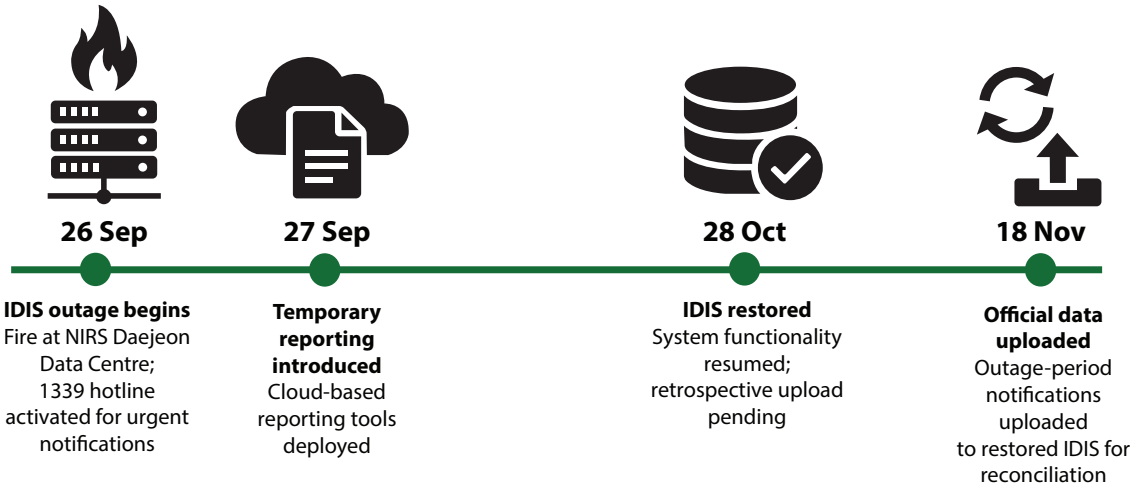


Table 1. **Comparison of IDIS dataset with temporary cloud-based reporting data, 2025**

Infectious disease	IDIS[a] (*n* = 4098)	Cloud-based reporting[b] (*n* = 3913)	Pearson's *r*	*P*
Cholera	1	1	0.99	<0.001
Enterohemorrhagic *Escherichia coli*	105	111		
Haemophilus influenzae type B	1	1		
Legionellosis	67	61		
Measles	35	34		
Meningococcal disease	4	3		
Mumps	503	506		
Paratyphoid fever	54	53		
Pertussis	98	84		
Pneumococcal disease	20	22		
Rubella (acquired)	1	0		
Scarlet fever	810	809		
Shigellosis	8	9		
Tetanus	4	3		
Typhoid fever	39	36		
Varicella	1772	1663		
Vibrio vulnificus sepsis	21	21		
Viral hepatitis A	82	78		
Viral hepatitis B	12	13		
Viral hepatitis C	401	350		
Viral hepatitis E	60	55		

IDIS: Infectious Disease Information System.

[a] Official disease notification data were uploaded after the system was restored; these were used as the reference dataset for comparison. Higher IDIS counts for some diseases, including varicella and viral hepatitis C, may reflect additional notifications entered after laboratory confirmation through routine reporting pathways following system restoration.

[b] Case notifications submitted during the IT outage through the temporary cloud-based reporting form.

Joint External Evaluation. Through this assessment, the country was recognized for its strong International Health Regulations (2005) core capacities across every sector.[11] Although the IT outage was not part of the evaluation criteria, this case epitomizes the operational resilience of the government's core capacities.

In conclusion, this report suggests that essential infectious disease surveillance and interagency coordination can be maintained during a nationwide IT disruption through adaptive reporting mechanisms and strong institutional coordination. It also highlights the need to strengthen infrastructure redundancy and disaster recovery capacity, and to conduct regular simulation exercises to maintain surveillance continuity.

Acknowledgements

The authors sincerely appreciate all members of KDCA, local health authorities and medical institutions for their contributions to and support for the successful maintenance of infectious disease surveillance during the IT disruption.

Google Gemini was used solely for grammatical polishing and English language refinement. The authors confirmed all changes and take full responsibility for the content of the final manuscript.

Conflicts of interest

The authors have no conflicts of interest to declare.

Ethics statement

This work describes an emergency response and did not require ethics approval from the Institutional Review Board of KDCA.

Funding

None.

References

1. Sharman L. Explosive battery blaze in South Korea 'paralyzes' vital government services [news release]. CNN World; 27 September 2025. Available from: https://edition.cnn.com/2025/09/27/asia/south-korea-fire-data-center-daejeon-intl-hnk, accessed 6 December 2025.
2. Yoon J, Ahn A. Fire at South Korean data center causes government service outages [news release]. The New York Times; 27 September 2025. Available from: https://www.nytimes.com/2025/09/27/world/asia/south-korea-fire-government-data-center.html, accessed 6 December 2025.
3. Kim H. South Korea's Lee calls for improving security at national data centre after fire [news release]. Reuters; 29 September 2025. Available from: https://www.reuters.com/world/asia-pacific/south-korea-restart-551-647-administrative-systems-after-data-centre-fire-newsis-2025-09-28/, accessed 6 December 2025.
4. Park J, Ha S, Kim S. Overview of infectious disease information system and big data platform. Public Health Wkly Report. 2025;18(34):1277–91. doi:10.56786/PHWR.2025.18.34.2 pmid:41334209
5. Jang Y, Lee H, Park H. Surveillance system for infectious disease prevention and management: direction of Korea's infectious disease surveillance system. J Korean Med Sci. 2025;40(8):e108. doi:10.3346/jkms.2025.40.e108 pmid:40034093
6. Park S, Kim E. 질병관리본부 긴급상황실 소개 [Emergency operations center at the Korea Centers for Disease Control and Prevention]. Public Health Wkly Report. 2020;13(31):2279–88 (in Korean).
7. Yonhap. Gov't to focus on restoring crippled state online services after data center fire [news release]. The Korea Times; 27 September 2025. Available from: https://www.koreatimes.co.kr/southkorea/society/20250927/govt-to-focus-on-restoring-crippled-state-online-services-after-data-center-fire, accessed 6 December 2025.
8. 질병관리청, 방역통합정보시스템 및 대표누리집 운영 재개(10.28.화) [KDCA resumes operation of the Infectious Disease Information System and the main website (Tuesday, October 28)] [news release]. Cheongju: Korea Disease Control and Prevention Agency; 28 October 2025 (in Korean). Available from: https://www.kdca.go.kr/kdca/2847/subview.do?enc=Zm5jdDF8QEB8JTJGYmJzJTJGa2RjYSUyRjQxJTJGMjE1NDQ3JTJGYXJ0Y2xWaWV3LmRvJTNGcGFzc3dvcmQlM0QlMjZyZ3NCZ25kZVN0ciUzRCUyNmZpbmRPcG53cmQlM0QlMjZmaW5kV29yZCUzRCUyNnJnc0VuZGRlU3RyJTNEJTI2ZmluZFR5cGUlM0QlMjZmaW5kQ2xTZXElM0QlMjZwYWdlJTNEMTglMjY%3D, accessed 6 December 2025.
9. Abualkishik AZ, Alwan AA, Gulzar Y. Disaster recovery in cloud computing systems: an overview. Int J Adv Comput Sci Appl. 2020;11(9):702–10. doi:10.14569/IJACSA.2020.0110984
10. Asia Pacific health security action framework. Manila: WHO Regional Office for the Western Pacific; 2024. Available from: https://iris.who.int/handle/10665/377083, accessed 6 December 2025.
11. Joint external evaluation of the International Health Regulations (2005) core capacities of Republic of Korea: mission report, 25–29 August 2025. Geneva: World Health Organization; 2025. Available from: https://iris.who.int/handle/10665/385104, accessed 28 April 2026.