digicert®

HealthLink

Uncompromising Trust
and Identity at Scale

Uncompromising Trust and Identity at Scale

New Zealand's healthcare system is built on a secure network of trust, developed and managed by Clanwilliam Health's HealthLink

Treating privacy with care

A patient in Auckland sits down with her oncologist to discuss options. There's good news, in the end. The cancer can be treated. But she will need to see a specialist in Tauranga. The oncologist has every confidence that the referral will be seamless. This is a guarantee, because both the oncologist and the specialty cancer treatment center use HealthLink to protect sensitive information. The patient needn't worry about lost or stolen records. Everything the specialist needs to know will arrive, secure and complete. With all the important information in hand, the specialist can work with the patient to create a treatment and recovery plan.

Protecting Australasia's patients

In 1993, New Zealand enacted health reforms, calling for a new system that would protect clinical information transmitted between providers, laboratories, medical services and patients. Now going into its third decade, HealthLink has enabled health information security for New Zealand and Australia at a massive scale, with unfaltering trust. Today, HealthLink connects over 15,000 medical clinics, securing and authenticating more than 100 million clinical messages annually.

**2000+ connected points
70+ software partners
10,000 Health Secure Digital Certificates**

The last thing a patient should have to worry about is their information privacy.
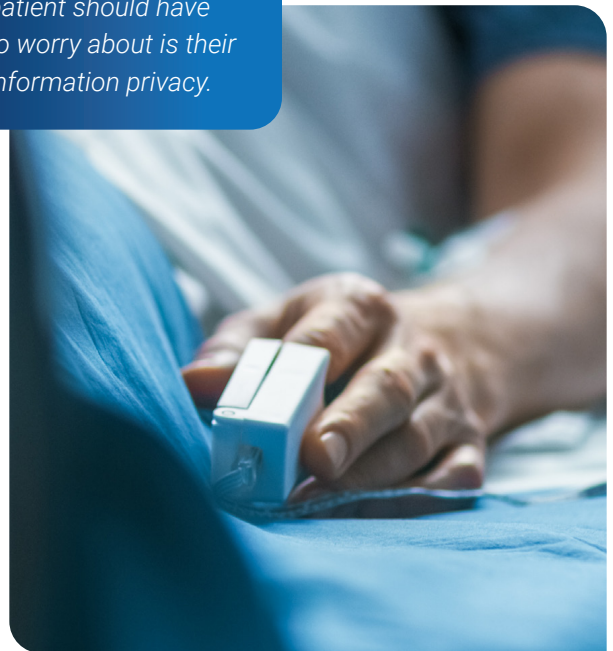
More than a signature

At the heart of HealthLink's services stands Public Key Infrastructure. PKI has been trusted for decades to secure communication in transit. But there's an additional feature of PKI that's especially valuable to medical professionals on the HealthLink network—authentication. When a key is generated, a unique signature is attached to that communication, proving the identity of the owner. This allows a care provider to digitally sign the document, lab report or eReferral, so the recipient knows the communication came from that provider, and it has arrived untampered.

> *"The model, from a use perspective, is peace of mind. It will just work."*
>
> *- Ivan Nola, HealthLink*

Innovation, alongside trust and certainty

Like most countries, New Zealand's healthcare landscape is complex. Whereas many organizations have greater control over their security environment, HealthLink deals with the monumental challenge of playing a secure intermediary role. There are a lot of moving pieces to contend with. From the lab to the insurer, hospital to patient, and from public clinics to private providers, HealthLink's solutions must be nimble and trustworthy at the same time.

With third party software and great variation in expertise and use, providing uncompromising trust and certainty requires flexibility and innovation. And, as new patients join the healthcare network, new clinics open, and new software and tools come online, the security solutions must scale and adapt. By combining ingenuity with trusted security, HealthLink has established a working solution that continues to provide integrity and peace of mind to Australasia's healthcare system and millions of patients.
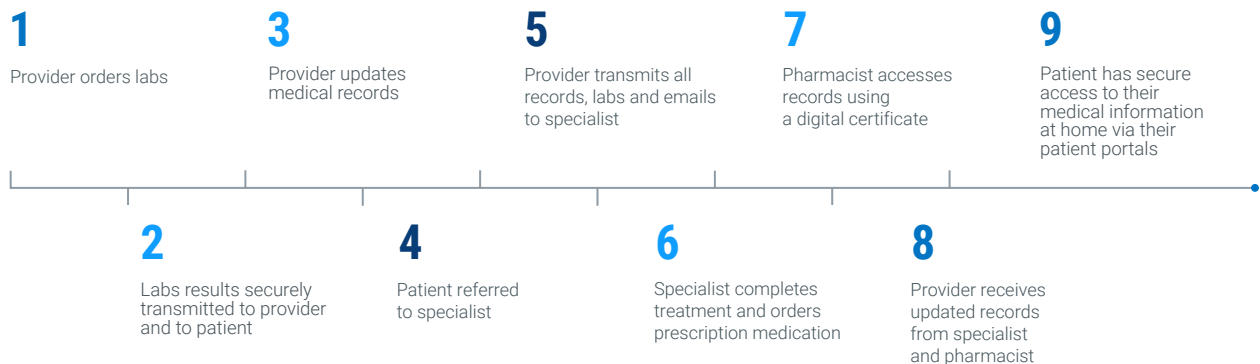
Refocusing on the patient

As trailblazers in secure health data delivery, HealthLink has built an infrastructure of forms and tools that help doctors quickly, easily and securely share patient information. In addition to increased efficiency and better privacy, HealthLink security solutions cut down on the amount of time providers must spend filling out paperwork. The result is more time to focus on the needs of the person seeking care.

> By combining ingenuity with trusted security, HealthLink has established a working solution that continues to provide integrity and peace of mind to Australasia's healthcare system and millions of patients.

The HealthLink chain of communication

From end-to-end, every step, every point, every person involved—it's all secured by PKI.

1 Provider orders labs

2 Labs results securely transmitted to provider and to patient

3 Provider updates medical records

4 Patient referred to specialist

5 Provider transmits all records, labs and emails to specialist

6 Specialist completes treatment and orders prescription medication

7 Pharmacist accesses records using a digital certificate

8 Provider receives updated records from specialist and pharmacist

9 Patient has secure access to their medical information at home via their patient portals

The DigiCert difference

The better way can't become common practice until someone finds it. At DigiCert, building a better way to secure the internet is the single-minded pursuit that goes all the way back to our roots. That's why our TLS/SSL certificates are trusted everywhere, millions of times every day by 89% of the Fortune 500, 97 of the 100 top global banks, and for 81% of global e-commerce. It's why our customers consistently award us the most five-star service and support reviews in the industry. It's why we're modernizing PKI by building the DigiCert ONE platform and management tools to help enterprises and governments secure identities, access, servers, networks, email, code, signatures, documents and IoT devices. In SSL, IoT, PKI, and beyond—DigiCert is the uncommon denominator.

Want to hear more about trust and identity solutions delivered at scale? Contact one of our experts to talk about PKI security and authentication digicert.com/digicert-enterprise-pkimanager/pki_info@digicert.com