2022 – Krankenhauszukunftsgesetz (KHZG), KRITIS und Sicherheitsgesetz 2.0: Sind Ihre Cybersecurity Investitionen und Zuschüsse effizient geplant?

Das Krankenhauszukunftsgesetz – haben Sie bewilligte Förderungen aus dem 4.3 Mrd € Topf erhalten?

Da in einigen Bereichen seit 2021 die beantragten Gelder ausgeschüttet werden, stellt sich zunehmend die Frage, in welche Cybersecurity Maßnahmen diese sinnvoll investiert werden sollen?

Das Krankenhauszukunftsgesetz, über dessen Basis nach dem Beschluss seit dem 01.01.2021 die Gelder ausgeschüttet werden, soll die Digitalisierung der Infrastruktur in Krankenhäusern vorantreiben. Mit dem Gesetz wird das durch die Koalition am 03.06.2020 beschlossene „Zukunftsprogramm Krankenhäuser" gefördert und das KHZG ist am 29.10.2020 offiziell in Kraft getreten.

Dieses Vorhaben wurde inzwischen mit insgesamt 4.3 Milliarden Euro gefördert. Die Länder und/oder die Krankenhausträger übernehmen dabei 30 % der jeweiligen Investitionskosten. Vorhaben an Hochschulkliniken können ebenfalls mit bis zu 10 % des Fördervolumens des jeweiligen Landes gefördert werden.

Was genau wird und wurde gefördert?

„Gefördert werden Investitionen in moderne Notfallkapazitäten und eine bessere digitale Infrastruktur, z.B. Patientenportale, elektronische Dokumentation von Pflege- und Behandlungsleistungen, digitales Medikationsmanagement, **Maßnahmen zur IT-Sicherheit** sowie sektorenübergreifende telemedizinische Netzwerkstrukturen. Auch erforderliche personelle Maßnahmen können durch den KHZF finanziert werden." (Auszug aus dem KHZG)

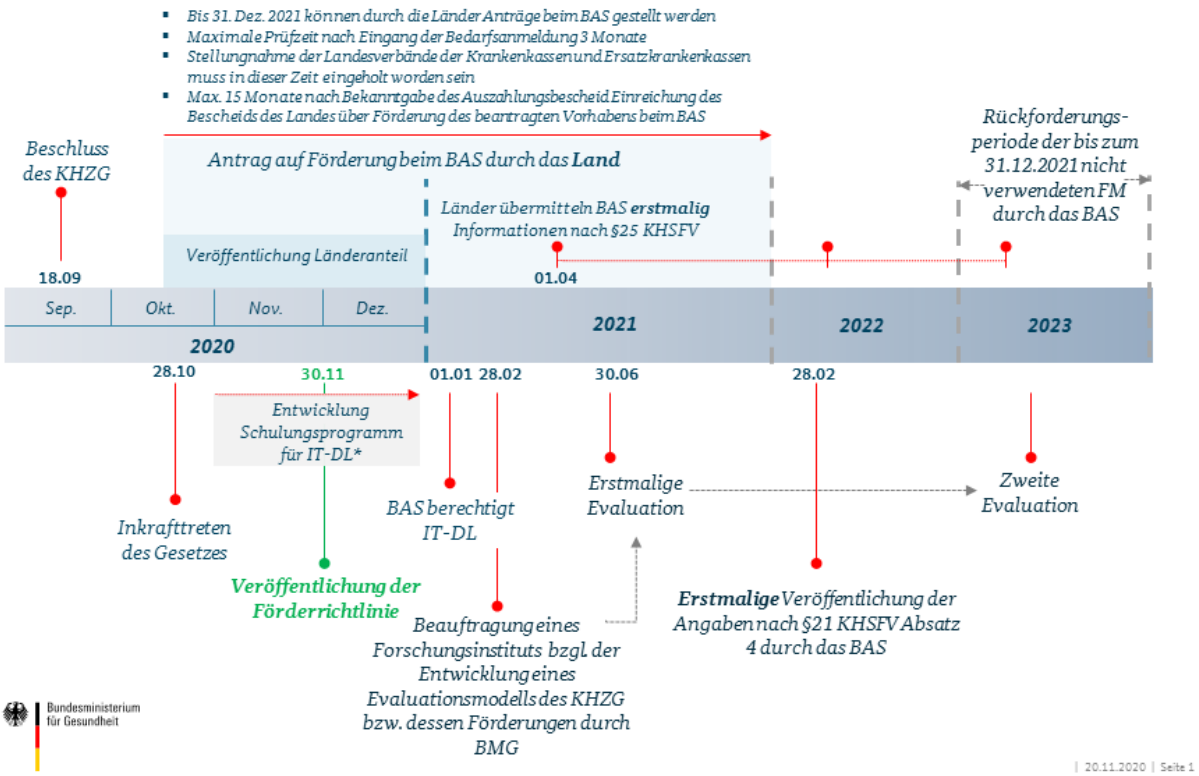
Hierunter fallen somit u.a. die Cybersecurity-Investitionen der Krankenhäuser, die durch Bund und Länder unterstützt werden.

Wie sieht der Zeitplan für diese Förderung aus?

Bis zum 31.12.2021 konnten Anträge durch die Länder beim BAS gestellt werden, einen genauen Zeitplan finden Sie auf der Seite des Bundesgesundheitsministeriums:

WHITE PAPER

Zeitplan nach KHZG



Quelle: Bundesgesundheitsministerium

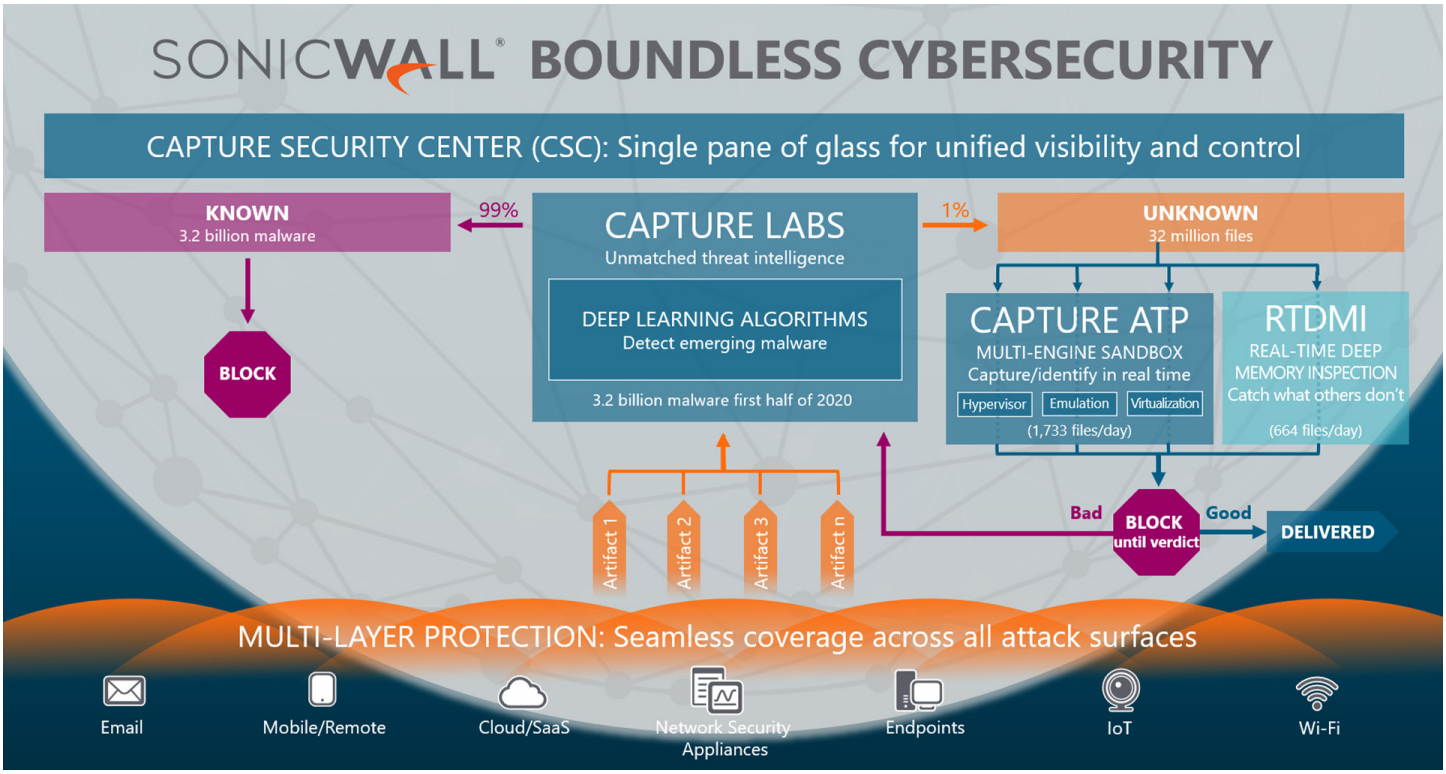
Cybersecurity Maßnahmen für den Healthcare Bereich: z.B. im Netzwerk, bei Fernzugriff und bei Next-Gen Firewalls

Immer häufiger kommt es im Bereich Healthcare zu schweren Vorfällen. Im vergangenen Jahr hatte in Düsseldorf ein solcher Cyberangriff auf das Netzwerk sogar ein Todesopfer zur Folge. Ein Praxisbericht zur aktuellen Situation in Krankenhäusern findet sich hierzu im Handelsblatt.

Um schwerwiegende Szenarien wie dieses zu verhindern, fördert der Bund den IT-Schutz u.a. in Krankenhäusern, Kliniken, Reha- und Pflegeeinrichtungen.

Empfohlene Maßnahmen für oftmals veraltete und nicht mehr zeitgemäße Hardware (z.B. durch fehlende Updates) sind unter anderem Wireless Access Points für das Patienten-Netz, das Netz für den internen Krankenhausbetrieb oder die Übertragung der medizinischen Daten von Intensivgeräten. All dies sind gern genutzte Eintrittspunkte für Hacker und Schadsoftware. Auf vielen Intensivgeräten sind noch veraltete Betriebssysteme im Einsatz, trotzdem müssen diese Geräte an das interne Netz angeschlossen bleiben. Zudem ist seit dem Beginn der Pandemie der Homeoffice- oder Remote-Zugriff eine zusätzliche große Bedrohung. Die Sensibilisierung der Mitarbeiter ist dabei ebenso wichtig wie die Technologie selbst.

Sehen Sie hier eine schematische Darstellung, über welche Einfallstore Angriffe üblicherweise stattfinden und wie das Konzept der Multi-Layer-Protection von SonicWall diese im Rahmen der Boundless Cybersecurity abwehrt:



Ebenfalls gefördert: Cybersecurity in KRITIS Einrichtungen

Auch im Jahr 2022 kommen weitere Herausforderungen speziell auf die Einrichtungen zu, die zukünftig unter das Thema „Kritische Infrastrukturen"/KRITIS fallen. Hierzu wurde z.B. die Anzahl der Betten herabgesetzt. Durch den immer häufiger werdenden Zusammenschluss von Einrichtungen und Häusern werden nun auch immer mehr kleinere Häuser im KRITIS Bereich angegliedert. Dies heißt im Umkehrschluss, dass durch den Zusammenschluss eine Größe erreicht wird, die für KRITIS-Förderungen berechtigt sein können. Zudem ändert sich zum 01.01.2022, dass alle Krankenhäuser den Stand der Technik überprüfen und bei Defiziten in Cybersecurity investieren müssen.

Förderfähig sind laut Auszug des BGM folgende Organisationen: „Krankenhäuser, die Kritische Infrastrukturen darstellen, sind von den Fördermaßnahmen des Krankenhauszukunftsgesetzes grundsätzlich erfasst. Speziell für Vorhaben, durch die eine Verbesserung der IT- bzw. Cybersicherheit erreicht werden soll (§ 19 Absatz 1 Satz 1 Nummer 10 KHSFV), gilt jedoch, dass Krankenhäuser, die als Kritische Infrastrukturen nach dem Krankenhausstrukturfonds (§ 12a Absatz 1 Satz 4 Nummer 3 KHG in Verbindung mit § 11 Absatz 1 Nummer 4 Buchstabe a KHSFV) förderfähig sind, von der Förderung über den Krankenhauszukunftsfonds ausgeschlossen sind. Dadurch soll eine Doppelförderung ausgeschlossen werden."

Fragen und Antworten zum Gesetzestext des KHZG finden sich auf der Seite des Bundesgesundheitsministeriums. Den Gesetzestext des KHZG können Sie ebenfalls dort downloaden. Zum Thema KRITIS-UP und IT Sicherheitsgesetz finden Sie hier weitere Informationen.

Das IT-Sicherheitsgesetz 2.0 für Unternehmen, Telekommunikation und andere Bereiche

Eine weitere Komponente, die mit der IT-Sicherheit einhergeht, ist das seit 07. Mai 2021 in Kraft getretene IT-Sicherheitsgesetz 2.0, das auch auf die im medizinischen Sektor zuständigen Unternehmen und Dienstleister Auswirkungen hat. Das IT-Sicherheitsgesetz ist auch Bestandteil von KRITIS_UP. Zum im Jahr 2015 in Kraft getretenen IT-Sicherheitsgesetz wurden für 2022 nun weitere Aspekte und Punkte ergänzt, u.a.:

- Detektion und Abwehr
- Cybersicherheit in den Mobilfunknetzen
- Verbraucherschutz
- Sicherheit für Unternehmen
- Nationale Behörde für Cybersicherheitszertifizierung

Für den Bereich Healthcare ist das eine gute Nachricht, da auch andere Unternehmen und Dienstleister nun mehr Wert auf den Bereich der Sicherheit legen müssen.

Quelle BSI

SonicWall Boundless Cybersecurity – ein Fallbeispiel aus der Praxis eines Krankenhauses

Wie die SonicWall Boundless Cybersecurity als gesamtheitlicher Ansatz bei einem Krankenhaus aussehen kann, erläutern wir Ihnen gerne am Fallbeispiel eines realen Krankenhausprojekts in Nordrhein-Westfalen:

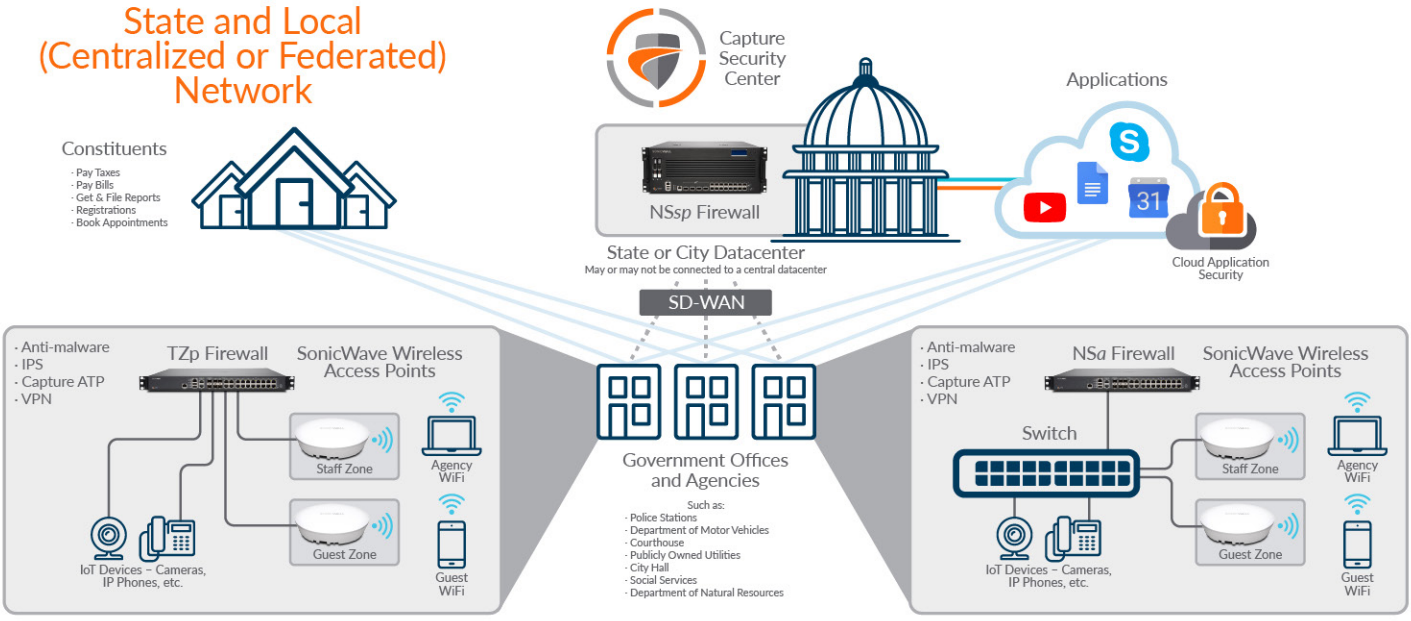
Der Kunde nutzt für seinen Hauptstandort ein SonicWall Next-Generation NSa 6650 HA Firewall Cluster, unterstützt wird dieses von den SonicWall TZ470 Firewalls zur Segmentierung der weiteren Standorte. Der SonicWall NSM (Network Security Manager) ist die Zentrale für Management, Reporting und Analyse des gesamten Netzes inkl. der SonicWall Switche zur Segmentierung. Die Wireless Access Points SonicWave aus der 400er Serie decken das kabellose Netzwerk ab, welches in Patientennetz, internes Krankenhausnetz und den sensiblen Bereich Intensivmedizin unterteilt wird. Insgesamt könnten bis zu acht Netze mit Security Features realisiert werden. Des Weiteren hat der Kunde eine E-Mail Security Appliance im Einsatz, welche SPAM und AV Schutz für eingehende E-Mails liefert. Für den Remote Zugriff setzt der Kunde die SonicWall SMA (Secure Mobile Access) 8200v auf seiner eigenen VMware Umgebung als Virtuelle Appliance ein. Diese garantiert eine problemlose Umstellung zwischen Homeoffice oder dem Arbeiten vor Ort im Krankenhaus – insbesondere für die Krankenhausverwaltung während der Lockdown-Phasen in der Pandemie – und erlaubt ein sehr granulares Konzept der Zugriffsregelung, auch für Dienstleister, die nur auf bestimmte Netzbereiche Zugriff erhalten sollen, um z.B. Remote-Updates zu fahren. Mit der SMA Lösung kann man Fremdgeräte ebenso wie Trusted-Devices kontrollieren und sicherstellen, dass kein unerlaubter Zugriff von außen stattfindet. Der Kunde setzt ein fast vollständiges Konzept aus dem SonicWall Produktportfolio ein – einheitlich über eine Konsole gesteuert und überwacht.

Sehen Sie hierzu auch unser Video, das das Boundless Cybersecurity Konzept in nur 10 Minuten anschaulich erklärt.

Welche SonicWall Produkte eignen sich besonders zum Schutz von Krankenhäusern oder anderen sensiblen Bereichen?

In der Praxis zeigt sich, dass die Herausforderungen von Krankenhäusern vor allem mit den folgenden SonicWall Lösungen sicher abgedeckt werden können:

- SonicWall Next Generation Firewalls
- SonicWall SMA Secure Mobile Access
- SonicWall E-Mail Security
- Advanced Threat Protection
- SonicWall Wireless Access Points



Übrigens: Unsere ATP (Advanced Threat Protection) hat bereits dreimal in Folge im ICSA Labs Test 100% der unbekannten Bedrohungen entdeckt – bei 0 Fehlalarmen! Ein perfektes Ergebnis – lesen gerne mehr dazu in unserem Blog.

100%
Erkennung von unbekannten Bedrohungen

0
Fehlalarme

Mehr zum Thema hören Sie auch in der Folge des SonicWall IT-Security Podcasts „Grenzenlos sicher?“: Operation KRITIS - Das Gesundheitswesen im Fokus von Cyberkriminellen

Das Gesundheitswesen zählt nicht ohne Grund zu den Kritischen Infrastrukturen – Cyberbedrohungen erstrecken sich in diesem Bereich vom Missbrauch von Patientendaten bis hin zur Manipulation von lebenserhaltenden Maschinen. Die beiden SonicWall Cybersecurity Experten Timo Lüth und Silvan Noll sprechen in dieser Folge mit Georg Stirnberg, Inhaber der Stirnberg IT, über KRITIS, die Rolle des BSI, die sich immer schneller verändernde Bedrohungslage im Gesundheitswesen und welche Auswirkungen diese auf die IT Sicherheit hat. Hören Sie außerdem Wichtiges zum Krankenhauszukunftsgesetz (KHZG), anschauliche Fallbeispiele für ein umfassendes Cybersecurity Konzept - von der kleinen Arztpraxis bis hin zur großen Klinik - und vieles mehr!

Intelligenz von Weltklasse. Modernste Sicherheit. Netzwerke in Enterprise-Größe – die neuen Next-Generation Firewalls (NGFWs) der NS*sp*-Serie

Die SonicWall Netzwerk-Security Services-Plattform (NSsp) High-End Firewall Serie bietet Advanced Threat Protection, hohe Geschwindigkeiten und ein hervorragendes Preis-Leistungs-Verhältnis – perfekt für große öffentliche Einrichtungen, Landes- und Bundesbehörden, kommunale Rechenzentren und Service Provider.

Optionen für Architekturen mit Multi-Instanzen bis zur Erstellung einheitlicher Richtlinien machen die Sicherung Ihrer Umgebung einfacher und effektiver – so erhalten Sie maximale Sicherheit, ohne Kompromisse eingehen zu müssen.

Die NSsp-Serie wurde speziell für große, dezentrale Einrichtungen, Rechenzentren und Service Provider bzw. Dienstleister entwickelt und kombiniert fortschrittliche Technologien wie Real-Time Deep Memory Inspection (RTDMI™) mit Hochgeschwindigkeitsleistung.

Erfahren Sie in unserem Gen 7 NS*sp* Firewall Video mehr über die SonicWall NSsp-Serie, außerdem finden Sie hier alle wichtigen Informationen, Daten und Funktionen auf einen Blick, welche Vorteile und Einsatzmöglichkeiten die NSsp Serie bietet sowie eine kostenlose Demo-Version.

Sie möchten mehr zum Thema Sicherheit und Lösungen für den Krankenhausbetrieb erfahren?

„Hallo, mein Name ist Marcus Lind, als Enterprise Account Manager bei SonicWall bin ich Ihr Ansprechpartner Rund um das Thema Cybersecurity für den Bereich Healthcare. Mit meiner langjährige Erfahrung in der Hardware- und IT-Security Branche sowie im KRITIS Umfeld berate ich Sie gerne hinsichtlich Ihrer individuell Anforderungen im Gesundheitssektor.

Ich freue mich auf den Austausch mit Ihnen– schreiben Sie mich gerne per E-Mail an. “

Besuchen Sie unsere SonicWall Website oder tauschen Sie sich gerne auch direkt mit unseren Sicherheitsexperten aus. Gemeinsam unterstützen wir hierbei und schaffen Lösungen, um Ihre Einrichtung maximal vor Angriffen zu schützen!

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Wirtschaftlichkeit ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMUs weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2022 SonicWall Inc. ALL RIGHTS RESERVED.
SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

WhitePaper-HospitalFutureAct-DE-JK-5926