Die Geister, die ich rief.

Folgende These stelle ich auf:

In spätestens 10 Jahren sind unsere jetzt noch gut verschlüsselten Patientendaten der Telematik für viele Internet-Dienstleister einsehbar.

Wie komme ich zu dieser Annahme?
1. Verschlüsselungsverfahren haben die Tendenz, dass sie mit der Zeit schwächer werden.
2. Sicherungskopien/Backups konservieren auch die Methode der Verschlüsselung
3. Die Speicherung bzw. Absicherung von Backups erfolgt nicht mehr lokal, sondern zunehmend über das Internet.
4. Die aktuell eingesetzte Verschlüsselungstechnik berücksichtigt nicht die Möglichkeiten von Quantencomputern.

Anders formuliert bedeutet es, dass ein Datensatz, der heute gut verschlüsselt abgespeichert wird, in Zukunft entschlüsselbar ist, ohne dass eine Kenntnis vom Schlüssel erforderlich sein wird.
Die Lagerung von Sicherungskopien und die Aufbewahrung von Patientendateien liegt nicht mehr unter der alleinigen Kontrolle einer behandelnden Praxis, sondern wird von externen Internetdienstleistern oder der Telematik übernommen (s. a. Online-Datensicherung, Cloud-Storage).

Die Aufbewahrungszeiträume für medizinische Daten liegen bei 10-30 Jahren (Link).

Eine kleine Praxis wird die Backups getrennt von den Praxisräumen und auf einfachen Datenträgern lagern (ext. Laufwerk, Bandlaufwerk, früher DVD u. Floppy-Disk). Größere Datenmengen aus Kliniken werden von eigenen Rechenzentren betreut. Allgemein besteht die Neigung, die Datensicherungen über das Internet zu realisieren. Die gematik hat sich auf eine Speicherung von Patientendaten in zentralen Datenbanken festgelegt.

Es ist sehr bequem, die physische Trennung der existenziell wichtigen Backup-Datensätze nicht mehr selbst organisieren zu müssen (kein Bankschließfach, keine private Lagerung, kleineres Rechenzentrum,…).

Aber ab hier beginnt das Problem.

Die verschlüsselten Backup-Datensätze oder die verschlüsselten Patientendaten befinden sich dann nicht mehr nur irgendwo bei der lokalen Praxis. Sie wurden auch an einen externen Dienstleister bzw. an die Telematik weitergegeben. Beide legen ebenfalls weitere Sicherungskopien an.

Das Erstellen und Aufbewahren von Sicherungskopien oder von Patientendaten ist ein sehr komplexes Themengebiet. Nur zwei Punkte dazu:

Thema Löschklausel:
Nehmen wir einmal an, dass alle Datensätze die älter als 10 Jahre sind, in einem Cloud-Speicher gelöscht werden müssen. Der Kunde sendet einen Löschbefehl und die Datei verschwindet aus dem Cloud-Verzeichnis. Was passiert aber mir den Sicherungskopien, die der Cloud-Storage-Anbieter selbst angelegt hat?

Ab hier beginnt oftmals der Denkfehler, dass mit einem Löschbefehl auch automatisch immer die Inhalte in den dort erstellten Backups gemeint sind. Ein gezieltes Löschen von Daten aus alten Backups ist je nach Speicherorganisation sehr schwierig bis unmöglich. Mit Löschvorschriften und Speicherverfahren kann man im besten Fall in Europa die "offiziellen" Verarbeiter in der EU binden.

Das sieht aber ganz anders bei nicht EU-Anbietern aus. Erfolgt beispielsweise in den USA eine Datenspeicherung, gelten dort nur die Amerikanischen Datenschutzgesetze (s. a. Patriot Act). Daten von Nicht-US-Bürgern haben dort faktisch keine Rechte. Den global Player in Asien brauch ich wohl erst gar nicht zu erwähnen.

Thema Umverschlüsselung:
Es stellt sich die Frage, ob man die älteren, verschlüsselten Backups dann mit einem sicheren Verfahren nochmals neu verschlüsseln kann (Zwiebelschale)? Im Prinzip ist das richtig. Allerdings kann nie ausgeschlossen werden, dass noch Sicherungskopien mit der älteren/schwächeren Verschlüsselung irgendwo existieren und genau das ist das Problem. → „Das Internet vergisst nichts.“

Zudem macht es eine Verwaltung der Datensätze sehr aufwendig, denn mit jeder neuen Verschlüsselungstechnik müssen nicht nur die neuen Schlüsselsysteme verwaltet werden, sondern auch die Sicherung und Wartung der alten Schlüssel und Verarbeitungsprogramme muss weiterhin gewährleistet werden.

Schwächelnde Verschlüsselungsverfahren

Verschlüsselungsverfahren haben die Tendenz, dass ihre Schutzfunktion mit der Zeit immer schwächer wird. Folgende Möglichkeiten, die ein Verfahren oder eine gewählte Schlüssellänge gefährden könnten, sind hier stark vereinfacht aufgelistet:

- *Dummheit*

Zukünftig entdeckte Implementierungsfehler (Programmierung des Verschlüsselungsverfahrens) sind Schwachstellen, die nicht das Verfahren an sich, aber die bis dato generierten Dateien betreffen.

Selbst das BSI (Bundesamt für Sicherheit in der Informationstechnik Link) ist nicht unfehlbar (s. Unsichere Verschlüsselung – trotz Zertifikat vom Bundesamt

Zitat: *„… die Kosten auf etwa 20.000 bis 40.000 Dollar pro angegriffenem Schlüssel, wenn man die nötige Rechenleistung bei Amazons Clouddienst AWS kaufen würde. Doch die Auswirkungen wären enorm. Man kann zwar jetzt die betroffenen Schlüssel austauschen, aber alles, was damit in der Vergangenheit verschlüsselt wurde, ist potenziell unsicher und kann von einem entsprechend finanzkräftigen Angreifer geknackt werden...“*

Es wurde ein Schlüsselsystem vom BSI zertifiziert, das einen zu kleinen Primzahlen-Zahlenraum verwendet.
Zum Erraten eines Schlüssels waren nun weniger Primzahlen erforderlich, die ausprobiert werden mussten.
Eine Folge des fehlerhaften Zahlengenerators, im vielfach eingesetzten Chip-Design war, dass Estland das Verschlüsselungsverfahren und die ID-Cards wechseln musste. (Link, Link).

- *Intelligenz*

Neu zu entdeckende, mathematische „Tricks“ bieten weitere Möglichkeiten, die eine Sicherheit/Stärke eines Verschlüsselungsverfahrens in Frage stellen können. Allerdings haben viele der etablierten Verschlüsselungsverfahren so lange durchgehalten, weil es sehr sehr schwierig ist, mathematische Verfahren zu finden, die eine einfache Umgehung der Verschlüsselung ermöglichen. So bleibt nur das blinde Erraten der Schlüssel übrig – s. u. Brute-Force Link .

- *Rohe Gewalt*

Ein Verschlüsselungsverfahren gilt als sicher, wenn das Erraten eines Schlüssels (Brute-Force Link) statistisch gesehen und mit heutiger Rechenleistung extrem lange (viele mrd. Jahre) benötigen würde.
Brute-Force Angriffe auf heutige Verfahren/Schlüssellängen sollten erst in Zukunft ein Problem darstellen. (s. Mooresches-Gesetz- Verdopplung der Rechenleistung ca. alle 18 Monate)
Aus diesem Grund wird vom BSI empfohlen, u. a. die aktuellen *RSA* Schlüssellängen in Zukunft zu erhöhen, damit wieder mehr Rechenleistung/Zeit/Kosten/Aufwand erforderlich wird. (BSI Link s. S. 15, Tabelle 1.2). 2023 ist für mich allerdings eine sehr nahe Zukunft.
AES gilt mit 256 Bit auch unter Quantentechnologie noch als sicher. (Im Anhang s. „Verschlüsselung“ sind die Anwendungen *von RSA und AES genauer beschrieben.)*

Um mit dem technischen Fortschritt mitzuhalten, also um genügend Abstand zu den technisch möglichen Angriffen beizubehalten (s. a. Seitenkanalattacke), wird u. a. eine Sicherheitstechnik meist weit vor ihrem funktionalen Ende ausgetauscht. Wir kennen dass, wenn wir eine neue EC-Karte alle paar Jahre erhalten. Eine gute Ökobilanz ist bei sicherheitstechnischen Produkten zweitrangig.

Zu empfehlen: BSI Link , s. S. 16 Kap 1.2 - Über die Zuverlässigkeit von Prognosen zur Sicherheit. Dort werden die Entwicklungen im Bereich der Quantencomputer ausgeklammert bzw. keine relevanten Änderungen erwartet. - Das sehe ich ganz anders.

- *Magie*

Den Todesstoß für unsere bisherigen Verschlüsselungsverfahren sollen die neuen Quantencomputer ermöglichen. Quantencomputer können unsere noch oft verwendeten Verschlüsselungsverfahren (RSA) dann quasi in Sekundenbruchteilen aushebeln.
IBM rechnet mit einem Durchbruch schon in 5 Jahren. Das ist sehr zeitnah!
Hier ein Link von vielen: https://futurezone.at/science/ibm-quantencomputer-werden-bald-jede-verschluesselung-knacken/400038388

Dass es keine Fiktion bleibt und sehr ernst genommen werden sollte, zeigen Standardisierungs-bemühungen und die Entwicklung neuer Verschlüsselungs-Algorithmen, die schon jetzt stattfinden („Erster Standard für Post-Quantum-Signaturen“- Link).

Möglicherweise müssen die Quantencomputer keine vollständige Entschlüsselung vornehmen, um an den Inhalt von verschlüsselten Dateien zu gelangen.
Vielleicht sind Verfahren möglich, die mit einer technisch einfacheren Quanten-Entschlüsselung, die Schlüssellängen so weit herabsetzen, dass die zur Verfügung stehende „traditionelle“ Rechenleistung ausreichend ist. Quasi eine Hybride-Decryption;-)

Bei den Anbietern von Datenbanken und Serverfarmen ist die primäre Geschäftsbasis der Umgang mit Dateien. Es ist daher naheliegend, auch den Inhalt zur Monetarisierung zu verwerten (s. Facebook).
Die Akkumulation von sehr vielen Datensätzen macht es zudem attraktiver, in mehr Rechenleistung und neue Technik zum Entschlüsseln der Datensätze zu investieren.

Nebenbei bemerkt, was machen die ganzen Bitcoin-Miner, wenn es mal langweilig wird? Unter „Health-Mining“ sind dann wohl neue Geschäftsmodelle zu verstehen, die alte Datensätze aufbrechen.

„Ich hab doch nichts zu verbergen.“ - Oh doch!

Es werden mit Big-Data dann nicht nur die offenen Datenschätze gehoben, sondern auch viele persönliche „Leichen im Keller“.
Hier ist eine Tabelle von besonders schützenswerten Patienteninformationen zu finden (s. S.14 Link). Es gibt bestimmt Punkte darunter, die ein Arbeitgeber auch nicht in 10 Jahren erfahren sollte.

Alte Backups mit dann schwacher Verschlüsselung, werden der Schatz für Versicherungen und Jobagenturen sein. Die Anfragen zum Persönlichkeitsprofil gehen dann an darauf spezialisierte Unternehmen (Übersee), die nicht an unseren Datenschutz gebunden sind.

In wie weit ein Internetanbieter die Datenströme mitschneidet und dauerhaft auf Vorrat speichert (Geheimdienste) oder verschlüsselte Daten durch Hackerangriffe kopiert wurden, ist schwer zu beurteilen. Gerade wenn versichert wird, dass bei einem Hackerangriff nur verschlüsselte Datensätze gelesen werden konnten, kann das nach Jahren doch noch zum Problem werden.
Dann wird aus einem gut gelagerten Datensatz ein Datenschatz.

Meine Forderungen für Arztpraxen wären:

- *Datensparsamkeit*
Die sichersten Daten sind die, die erst gar nicht eine Praxis verlassen (müssen).
Eine Praxisverwaltung darf nur als Intranet betrieben werden. Nur absolut notwendige Daten dürfen über das Internet versendet werden.

Das BSI empfiehlt unter Kap 1.2 „Allgemeine Leitlinien“ s. S. 16 Link:
„Da ein Angreifer Daten speichern und später entschlüsseln kann, bleibt ein grundsätzliches Risiko für den langfristigen Schutz der Vertraulichkeit. Als unmittelbare Konsequenzen ergeben sich ...

- Die Übertragung und die Speicherung vertraulicher Daten sollte auf das notwendige Maß beschränkt werden. ...“

- Schadensbegrenzung
Keine automatische Speicherung von verschlüsselten Patientendaten an irgendeinem Ort im Internet.

- Pflicht zur lokalen Speicherung von Backups, physisch getrennt vom Internet/Intranet
Beispielsweise auf mobilen Datenträgern. *(Eine Diskussion über den Lagerort und Verfahren würde hier ausufern, wäre aber notwendig.)*

Kritiker würden jetzt sagen, der Datenträger kann verlorengehen. Ja, das stimmt. Allerdings ist der Schaden dann sehr begrenzt, wenn die Dateien in Zukunft entschlüsselt werden könnten. Der momentane Wert ist für einen zufälligen Finder gleich null. Eine Abschätzung, ob es den Aufwand wert ist, die Daten über einen längeren Zeitraum aufzuheben, um sie dann erst zu entschlüsseln. Das ist sehr schwierig. Der Datenträger hat so gesehen als Hardware mehr Wert und wird neu formatiert. Das war‘s.
Etwas ganz anders ist es, wenn viele Praxen ihre verschlüsselten Backups irgendwo in einer externen Datenbank speichern oder verschlüsselte Patientendaten bei einem externen Dienstleister lagern (Cloud-Storage, Online-Datensicherung). Das würde einem permanenten Datenverlust, vieler Praxen, an eine zentrale Stelle entsprechen.
Gerade große Unternehmen werden als erste das Know-How und die Technik haben, um in solchen Datensammlungen schürfen zu können.
Die Wahrscheinlichkeit, dass man von einem Datenleck selbst betroffen ist, steigt so ebenfalls.

- Keine Freigabe/Entschlüsselung der Datensätze von Verstorbenen
Beispielsweise „Erbkrankheiten“ - Die genetischen Erben werden bestimmt nicht begeistert sein, wenn eine private Krankenkasse oder eine Berufsunfähigkeits-Versicherung nun aufgrund einer genetischen Erblast einen höheren Beitrag ermittelt. Es wird keinen Bankkredit geben, wenn die Eltern depressiv waren…
(Eine Offenlegung von Bewertungsalgorithmen sehe ich daher ebenfalls als zwingend erforderlich an.)
Freiwillige Datenspenden müssen ebenfalls verboten werden. Denn durch sie wird das Persönlichkeitsrecht der genetisch Verwandten verletzt.

Bisher wurde nur enterbt, zukünftig geht noch die eigene Patientenakte an die Versicherungen der ungeliebten Erben;-)

Zusammenfassung:

Die jetzt als sicher geltenden Verschlüsselungsverfahren (RSA) könnten in (naher) Zukunft gebrochen werden. Unsere Sicherngskopien mit den verschlüsselten Daten, müssen nur lange genug aufbewahrt werden, bis deren Verschlüsselung keinen Schutz mehr darstellt. Dies kann durch eine neue Technik, wesentlich mehr Rechenleistung, einen neuen mathematischen Trick oder einen zuvor nicht erkannten Implementierungsfehler der Verschlüsselungsalgorithmen passieren.

Alte Dateien, die mit DES (Link) verschlüsselt wurden, können heute entschlüsselt werden. In einer Zukunft, die bestimmt viele von uns noch erleben werden, halte ich es für sehr wahrscheinlich, dass wir auf unsere heute noch gut verschlüsselten Daten genauso zurückblicken werden. Der Unterschied wird nur sein, dass diese Dateien dann weit über das Internet verteilt wurden.
Auch alte Datens(ch)ätze haben für Versicherungen, Jobagenturen u. a. noch einen Wert.

Meine Meinung

Die Tatsache, dass eine Verschlüsselung von Sicherungskopien kontinuierlich schwächer wird und nun zusätzlich durch Quantencomputer aufgehoben werden kann, wurde bisher nicht ausreichend berücksichtigt. Sie muss in den Diskussionen aufgegriffen werden, besonders wenn es um eine zentralisierte Verarbeitung und Speicherung von Patientendaten geht. Eine gelegentliche Evaluierung und Anpassung der Verschlüsselungstechnik betrifft immer die in Zukunft neu erzeugten Daten. Es werden aber nicht die Datensätze berücksichtigt, die mit veralteter Verschlüsselungstechnik generiert wurden.

Allein durch eine Technik, die auf einer zentralen Lagerung von Daten und angreifbaren Sicherungskopien basiert, wird ein Patient nie Eigentümer seiner Daten sein können oder tatsächlich ein Recht auf Vergessen und Nichtwissen durchsetzen können.

Wenn jemand behauptet, dass unsere verschlüsselten Daten sicher sind, sollten wir immer hinterfragen, ob sie dies auch in Zukunft sein werden. Wir werden es erst merken, wenn es zu spät sein wird. Den Geist kriegen wir dann nicht mehr in die Flasche zurück.

Eine schwächer werdende Verschlüsselung, sehe ich als triftigen Grund, die Speicherung von Daten außerhalb* einer Praxis oder Klinik abzulehnen.

8.7.2018

PraxisITler

**Nicht als „lokal bzgl. Ort“ zu verstehen, wenn die Praxis abbrennt war‘s das, sondern eher im Zuständigkeitsbereich/Kontrollbereich einer Praxis.*

Quellen/Hinweise:

Aufbewahrungszeitraum medizinischer Daten:
https://gesundheitsdatenschutz.org/doku.php/med_daten

Verschlüsselung:

Ein wesentliches Problem in der verschlüsselten Kommunikation ist der Schlüsselaustausch.
Wie übertrage ich zur geheimen Nachricht auch den Schlüssel, damit diese Nachricht auch wieder mit diesem Schlüssel entschlüsselt werden kann (symmetrischer Schlüssel, bspw. AES), ohne dass jemand unberechtigtes den Schlüssel mitlesen kann?

Ab hier kommen die unsymmetrischen Schlüssel mit Public- und Private-Key ins Spiel (Public-Key, s. a. PGP) .
RSA ist so ein Verfahren. Das Verfahren beruht auf zwei Schlüsseln, die mathematisch so miteinander gekoppelt sind, dass wenn eine Nachricht mit dem einem öffentlichen Schlüssel verschlüsselt wird, diese Nachricht dann nur mit dem anderen, privaten Schlüssel, entschlüsselt werden kann.
Der Schlüssel zum Entschlüsseln bleib geheim (sog. Private-Key) und ist nur dem Empfänger bekannt. Der Public-Key wird verteilt. Mit einem Public-Key verschlüsselte Nachrichten können so nur vom Empfänger, der den Private-Key hat, gelesen werden.

RSA hat den Nachteil, dass es langsam ist. Folgendes Hybrid-Verfahren wird daher angewandt:

Große Datenmengen werden mit einem symmetrischen Schlüssel (Session Key, AES) schnell verschlüsselt.
Dann wird der Publik-Key (RSA) vom Ziel verwendet. Den darf jeder mitlesen.
Mit diesem öffentlichen Schlüssel wird nun nur der kleine symmetrische AES-Schlüssel verschlüsselt.
Der mit AES verschlüsselte Datenblock und der mit RSA verschlüsselte AES-Schlüssel werden zum Ziel gesendet.
Dort wird der verschlüsselte symmetrische Schlüssel mit dem Private-Key (RSA), den nur der Empfänger kennt, wieder entschlüsselt. Nun liegt der symmetrische Schlüssel lesbar vor. Mit ihm werden dann die Daten selbst auch wieder entschlüsselt. (s. a. PGP- Pretty Good Privacy Link)

Also ein asymmetrischer RSA-Key wird zum Transportieren der wesentlich sicheren Symmetrischen Schlüssel (AES) verwendet. RSA wird sich aber vermutlich in naher Zukunft aufbrechen lassen (s. Quantencomputer), so dass die damit verschlüsselten symmetrischen Schlüssel wieder gelesen werden können. Ein Verschlüsselungsverfahren ist nur so sicher, wie seine schwächste Absicherung.

Verschlüsselungsverfahren im Überblick
https://hosting.1und1.de/digitalguide/server/sicherheit/verschluesselungsverfahren-ein-ueberblick/

Deutlich wird der Aufwand der bei AES betrieben werden muss, so dass AES-256 bisher noch als sehr sicher gilt. Ein gutes Gegenbeispiel ist DES mit 56 Bit Schlüssellänge. DES gilt heute als nicht mehr sicher, da es schon mit Brute-Force-Attacken angegriffen werden kann.
Haben Sie noch alte Datenspeicher mit DES-56 verschlüsselten Daten?
Vermutlich schützt nun die nicht mehr vorhandene Technik (Floppylaufwerk, alte Praxissoftware) zum Lesen der Daten besser vor einer Einsichtnahme, als der Verschlüsselungsalgorithmus selbst.

Public-Key
https://www.mathematik.de/spudema/spudema_beitraege/beitraege/hillebrand/mathe2002/publickey.htm

PGP- Pretty Good Privacy
https://de.wikipedia.org/wiki/Pretty_Good_Privacy

Tabelle zum Entschlüsselungsaufwand mit Brute-Force und Kosten:
http://www.tcp-ip-info.de/security/key_length.htm

Die Tabelle ist von 1996. Der Text ist von 2008. Aktuell müssen die angegebenen Zeiten/Kosten ungefähr durch 32.000 Dividiert werden ($2^{(22*12/18)}$ → Faktor ca. 2^{15}), um dem Mooreschen Gesetz Rechnung zu tragen. Die sehr großen Werte für 256 Bit (AES) wurden in der alten Tabelle noch nicht berücksichtigt.

Quantencomputer und Verschlüsselung:
https://futurezone.at/science/ibm-quantencomputer-werden-bald-jede-verschluesselung-knacken/400038388

Shor-Algorithmus
https://de.wikipedia.org/wiki/Shor-Algorithmus

Spektrum der Wissenschaft -Quantencomputer als Kodeknacker - 6/2016 ab S. 64
https://www.spektrum.de/magazin/quantencomputer-als-kodeknacker/1408645

Empfehlenswert zu lesen - Leider nur für Abbonenten erreichbar
Für mich die wichtigsten Punkte:
- Quantencomputer können sehr gut Faktorisierung → RSA wird ausgehebelt
- Chiffriersysteme müssten sich eigentlich jetzt schon auf die neue Technik einstellen
→ IMHO - das wird bei der eGk und Telematik momentan total verschlafen

Spektrum der Wissenschaft -Die nächste Quantenrevolution 6/2018
https://www.spektrum.de/inhaltsverzeichnis/quantentechnologien-vor-dem-grossen-sprung-spektrum-der-wissenschaft-6-2018/1516369

Empfehlenswert zu lesen - Leider nur für Abbonenten erreichbar
Für mich der wichtigste Punkt:
- Unerwartet große Fortschritte innerhalb der letzten 2 Jahre

BSI- Studie Entwicklungsstand Quantencomputer Mai 2018:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Zusammenfassung.html

100-Tage für einen Datensatz sind sehr hoch, wenn eine Berechnung die ganze Verarbeitungskette blockiert:→ Pipelining?

Mooresches_Gesetz/Weltweite Rechenleistung:
https://de.wikipedia.org/wiki/Mooresches_Gesetz

BSI und Verschlüsselung:

BSI-Technische Richtlinien:
BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2018-02

Unsichere Verschlüsselung – trotz Zertifikat vom Bundesamt:
https://www.zeit.de/digital/datenschutz/2017-10/infineon-verschluesslung-personalausweis-tpm-bsi-zertifiziert

Estland: Sicherheitslücke in fast 750.000 ID-Cards
https://www.heise.de/newsticker/meldung/Estland-Sicherheitsluecke-in-fast-750-000-ID-Cards-3822597.html

Estland schränkt Funktionen von 760.000 ID-Cards ein
http://www.spiegel.de/netzwelt/web/estland-schraenkt-funktionen-von-760-000-id-karten-ein-a-1176355.html

Tallinn, wir haben ein Problem
http://www.faz.net/aktuell/feuilleton/debatten/estland-sicherheitsluecke-bei-elektronischen-personalausweisen-15186516.html

Estland dichtet Sicherheitslücke in E-Ausweisen ab
https://www.heise.de/newsticker/meldung/Estland-dichtet-Sicherheitsluecke-in-E-Ausweisen-ab-3877828.html

In den Texten ist sehr gut der Aufwand zu sehen, wenn es zum GAU kommt.
Dokumente müssen vor dem Update erst mit dem alten Verfahren entschlüsselt werden und dann können sie erst wieder neu Verschlüsselt werden. (Wer darf und kann das machen?)
Wenn ein Schlüsselsystem abgeschaltet wird, dann funktioniert auch die dafür aufgebaute Infrastruktur nicht mehr.
Ärzte und Polizei müssen als erste neue Chipkarten bekommen…
Wenn alles auf eine Karte gesetzt wird, dann sind auch gleichzeitig alle Applikationen davon betroffen. Daher ist es ein unverantwortliches Risko, mit einem einheitlichen Ausweis alles erledigen zu wollen (->keine Zusammenführung von ePerso und eGk).

Brute Force Tool- advanced password recovery:
Hashcat https://en.wikipedia.org/wiki/Hashcat, https://hashcat.net/hashcat/

eGk - Verfügbare-Verschlüsselungsverfahren:
http://www.informatik.uni-oldenburg.de/~iug13/eg/Technisches/Sicherheit.html

-Die eGk verwendet zur Zeit Triple-DES (3TDES) mit 168 Bit und RSA 2048
Ab 2017/2018 soll die eGK mit den Blockchiffren AES-128, AES-192 und AES-256 ausgestattet werden.
Ab 2023 empfiehlt das BSI RSA mit mindestens 3000 Bit Schlüssellänge zu verwenden, um das Sicherheitsniveau zu erhalten.
Ein eGk Kartentausch und mit Sicherheit auch der SMB Kartentausch im VPN-Konnektor sind da vorprogrammiert. Interessant auch unter informatik-uni-oldenburg:
„Wie werden Patienten gegenüber Fremdzugriffen geschützt?“ Link
Zitat: “Seit der 2. Generation der HBA-Karten kommen zur Verschlüsselung der Daten elliptische Kurven, AES und SHA-256 zum Einsatz. Diese Generation wurde 2011 eingeführt. Vorher, bei der 1. Generation, wurde mit RSA 2048 Bit, 3TDES und SHA-256 verschlüsselt, was wesentlich anfälliger war.“

Meine Frage hierzu wäre: Was ist in der Zwischenzeit mit den damaligen Sicherungskopien und Datenlogs passiert?

Eine sehr bekannte Brute-Force Software
Hashcat- BruteForce Tool, https://hashcat.net/hashcat/

Online-Datensicherung
https://de.wikipedia.org/wiki/Online-Datensicherung

Cloud-Storage
https://en.wikipedia.org/wiki/Cloud_storage

egk: DIE GRÖSSTE GEFAHR: DIE INNENTÄTER, *Dr. Klaus Günterberg*
https://docplayer.org/22903192-Egk-die-groesste-gefahr-die-innentaeter.html

Mal ein typisches Beispiel für einen Seitenkanalangriff:
https://www.blackhat.com/us-18/briefings/schedule/#tlbleed-when-protecting-your-cpu-caches-is-not-enough-10149
*„… Our TLBleed exploit successfully leaks a 256-bit EdDSA key from cryptographic signing code, which would be safe from cache attacks with cache isolation turned on, but would no longer be safe with TLBleed. We achieve a 98% success rate after just a single ob*servation of signing operation on a co-resident hyperthread and just 17 seconds of analysis time.“

Parallel im Speicher ablaufende Programme können den Schlüssel auslesen. Das ist kein prinzipieller Fehler vom Verschlüsselungsverfahren oder in der Programmierung des Verschlüsselungsverfahrens.