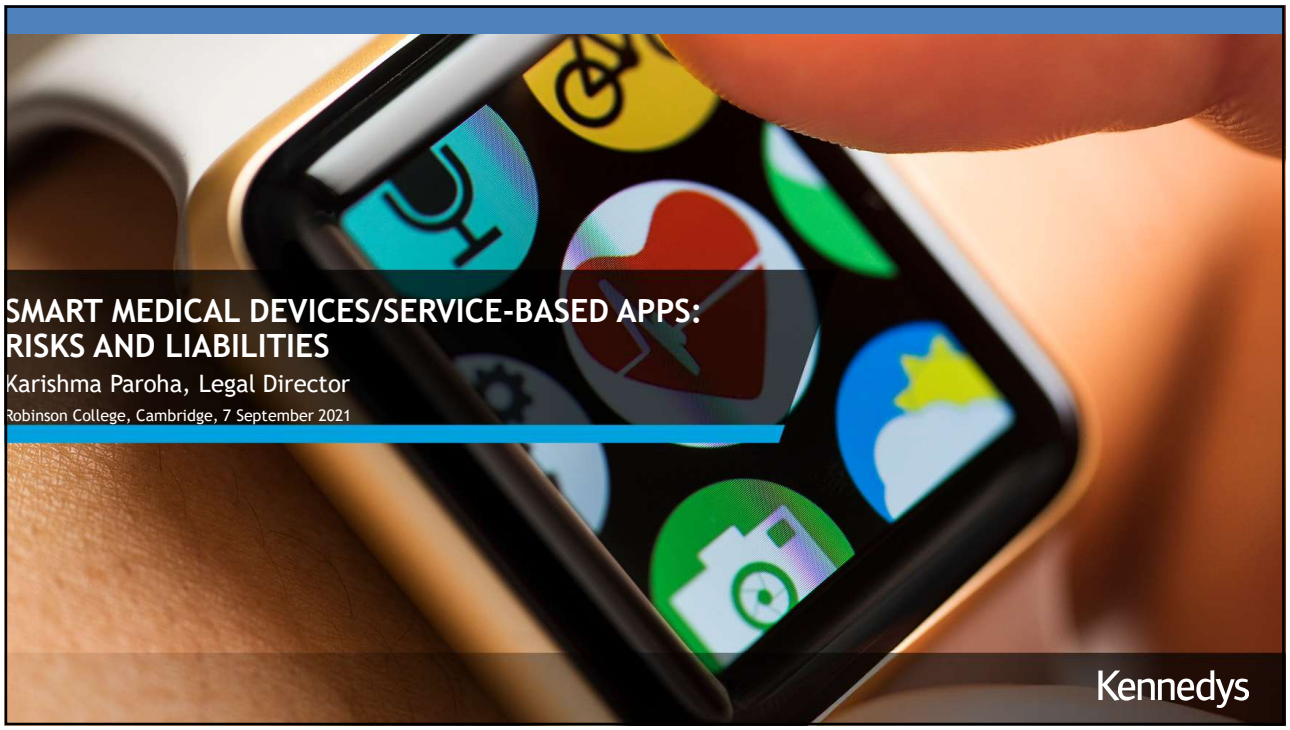


1

What did one smart device say to another smart device?

2

Are you syncing what I am syncing?

3

Agenda

4

UPDATE ON STATISTICS & PREDICTIONS

Kennedys

5

Global Market Value Predictions

- Recap - according to Deloitte:
  - Global Internet of Medical Things (IoMTs) market estimated to be worth **USD 158.1 billion** by 2022
  - Global market for smart medical devices (stationary, implanted and wearable external) segment (diagnose, monitor & treat) predicted to grow to **USD 52.2 billion** in 2022:
- Update - according to Precedence Research:
  - Global smart healthcare market size is predicted to hit around USD **482.25 billion** by 2027

6

Kennedys

6

Growth of Global Medical Device Security Market

- According to Reports and Data:
  - The global Medical Device Security Market Size was worth **USD 5.10 Billion** in 2020
  - Market Growth – 8.5%
  - Major factors - expanding pharmaceutical industry, increasing healthcare cyber attacks & threats & an emphasis on health care digitalisation
  - The Global Medical Device Security Market size is expected to reach **USD 9.78** billion by 2028

Growth Driving Factors

- Aging population
- Increasing healthcare expenditure
- Technology advancement
- Global adoption of smartphones
- Increasing focus on health & fitness
- Covid19 pandemic

Update - Impact of Covid19 Pandemic on Smart Healthcare

- Healthcare system pushed to its limits
- Lockdowns & taking care of ourselves
- Highlighted importance of smart medical devices & wearable remote monitoring devices (hospital & home)
- Surge in use of emerging technologies such as genomics, telehealth & AI, & a greater reliance upon data-driven technologies & related products
- Heightened risk of cybersecurity cases involving potential software data breaches

McKinsey & Company Report: *Telehealth: A quarter-trillion-dollar post-COVID-19 reality?* July 2021

- Telehealth usage in US has stabilised at levels 38 times higher than before pandemic
- US investment in virtual care & digital health was 3 times higher in 2020 than in 2017
- Around 40% of surveyed US consumers stated will continue to use telehealth going forward — up from 11% prior to COVID-19
- 58% of US physicians continue to view telehealth more favourably now than before COVID-19 & as of April 2021, 84% were offering virtual visits

Smart Healthcare Ecosystem - Products & Services

Telemedicine	Chatbots & E-prescriptions	E-physio	Genomic data & biomarkers
Remote monitoring	Smart Patient monitoring tools & RFIDs	Smartdiagnostic tools & health apps	AI imaging, detection & diagnosis
Smart hospital monitoring equipment	Smart pill bottles	Medical robots for surgery & hospital logistics	Virtual reality & augmented reality

Virtual hospitals/wards

- Remote care to patients in their homes via medical wearables technology
- Smart medical wearables enabling the creation of hospitals 'without walls'
- Virtual hospitals being trialled Australia, UK & Middle East – Sydney virtual care giving unit for Covid19 patients
- July 2020 - Northampton General NHS Trust carried out a trial with Doccla, a virtual hospital care start-up, to remotely monitor recovering Covid-19 patients

Smart Healthcare Eco-System – Recap on Key Players

- Healthcare services
  - E-triages & '*the digital front door*'
  - Digital hospitals/Virtual caregiving units/wards
  - Virtual GPs
  - Virtual pharmacists
  - Virtual dentists
- Patients & Users
- Software developers (& investors)
- Life Sciences Companies & Manufacturers

15

Definition under new Medical Device Regulation ("MDR")

- MDR fully applicable since 26 May 2021
- Definition of medical device under Article 2 (1) of the MDR:

> *"'medical device' means* ***<u>any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:</u>***
>
> ***<u>diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease…"</u>***

16 Kennedys

16

When a Smart Medical Device

- So if smart medical product/smart service based app makes a diagnosis or prognosis or prevents, monitors, treats or alleviates a disease it will be considered a medical device
- Also considered a medical device if it is *intended* as one by the manufacturer
  - Data on labelling, IFUs & packaging considered to establish intention

Kennedys

VARIETY OF EMERGING SMART MEDICAL DEVICES

Kennedys

A year ago

- **Wearable smart contact lenses** to diagnose & treat diabetic retinopathy
- **FDA approved wireless smart glucometer**, which measures glucose levels & shares with doctor & maintains history of readings
- **A one use smart insulin adhesive microneedle patch** which mimics the pancreas - human clinical trials anticipated to start in few years
- **FDA-cleared mobile personal ECG monitor**, which delivers a medical-grade electrocardiogram (ECG) to smartphone in just 30 seconds
- **Remote home testing kit** with teleconferencing app to connect to certified healthcare provider for remote consultation

Further Products

Featured at Consumer Electronics Show 2021 (CES 2021):

Portable helmet

- Detects brain activity & signs of early Alzheimer's dementia using AI analytics & brain mapping technology
- App that serves as a telemedicine platform, allowing doctors to monitor patients remotely. Capable of providing an EEG by simply placing it on the head
- Has technology to discriminate between Alzheimer & non-Alzheimer types of cognitive impairment with over 90% accuracy in multicentre clinical trials

Prototype of non invasive wrist-wearable glucose monitor

- allows healthcare providers to remotely keep a check on their patients

Further Products

Wearable biosensors

- Small, lightweight & enable monitoring of vital signs such as body temperature, heart rate, breathing rate & posture
- One such sensor used at a hospital in the Netherlands in isolation rooms of patients suspected of COVID-19 & did not require ventilation

Smart watches becoming healthcare tools

- Able to take an echocardiogram (ECG) using an electrical heart sensor & check for an irregular rhythm
- September 2020, a top brand launched their product with a new blood oxygen measuring functionality

Further Products

App enabled smart thermometers

- In one of most widely-talked-about apps of smart technology during the pandemic
- Published anonymised aggregated data across USA revealed clusters of high temperatures that might indicate an outbreak of Covid-19

Smart inhalers

- Connected with an AI platform
- Account for seasonal triggers & record medical history & provide reminder alerts to take medication & what dosage
- Will be trialled initially with NHS Scotland

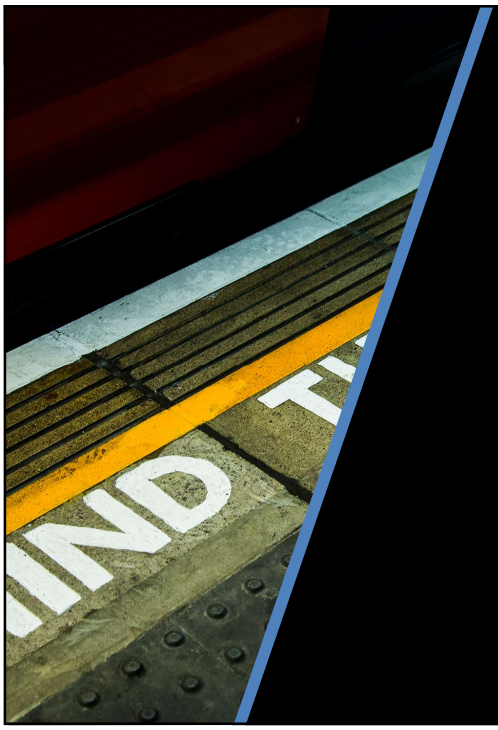
Recap on Next generation of smart medical implants

- Revolution of implantable nanoelectronics & smart chips

- Smaller, smarter & more lightweight & connected & packed with functionality:
  - More energy efficient
  - Biocompatible
  - Better performance
  - Increased patient comfort
  - Customised diagnosis
  - Chargeable wirelessly with portable device
  - Sends data it generates to external devices/attending physicians

23 Kennedys

23



RISKS

Kennedys

24

Risks – Factors inherent to device/app

- Defective design
- Inaccurate or out of date content/readings/advice
- Fails to diagnose
- Fails to update automatically
- Programming malfunctions
- Vulnerability to hacking
- Lack of support for users to report potential safety issues
- Inadequate warnings/unclear instructions

Risks - External Factors

- Usage outside design intended for by developer
- Inappropriate training
- High usage
- Out of date systems
- Low detection environment
- Lack of connectivity e.g. natural disaster
- Cyber attack

Cyber Attacks

- 2017 WannaCry ransomware attack exploited a vulnerability in older Windows machines & UK's NHS was among the worst affected organisations worldwide
- In 2019, according to Emisoft, 764 US healthcare providers were subje to a ransomware attack
- In September 2020 – A German woman died after hackers caused the failure of IT systems at a major hospital in Dusseldorf

Data Protection

- Personal data regarding health
- Take into account GDPR obligations at outset of design
- Limit to strictly necessary personal data
- Adopt adequate security measures against potential data breaches:
  - Encryption of users' data; &
  - Users' authentication
- 30 times more expensive to fix security flaws than to incorporate features in first place

PRODUCT LIABILITY RECAP

Kennedys

29

Product Liability

- On assumption software is a '*product*' not a '*service*'
- Smart medical devices & health app manufacturers could face product liability claims under the Consumer Protection Act 1987 (CPA)
- Under CPA 1987 strict liability on producer if use of product results in property damage &/or personal injury & is not as safe "*as persons are generally entitled to expect*"
- Following *Boston Scientific* - where claim relates to a software vulnerability &/or cyber security risk(s), allegations are likely to be made that the product has a design defect

30

Kennedys

30

Recap on Product Liability

- **Reasonable expectation**:
  - Does the consumer expect that hackers will be able to infiltrate the smart medical device?
  - Does the consumer expect that the smart medical device can malfunction if software is not updated in a timely manner, or if the software update is interrupted?
- If answered in the negative, the manufacturer may be subject to liability

Product Liability

- Potential multiple defendants from delivery & supply chain e.g. designer, manufacturer, shipper, seller, hospital, treating physician, patient user
- Difficult to apportion and determine liability
- Although anticipate manufacturers are likely to bear major share of any liability

Product Liability - Potential Crucial Questions

- Nature of the product's defect? Internal or external defect or both?
- How did the defect occur?
- Who designed the various components of the smart medical device/app?
- Where routine software updates provided:
  - What was the quality of the update?
  - Who was responsible for the ensuring the update? User? Provider? Manufacturer?
- Was manufacturer or software designer capable of designing a system that was immune to the alleged cybersecurity attack?

Modernisation of Product Safety & Liability Regimes

- Ongoing EU review of fitness of product liability laws for modern technologies
- Current debate regarding application of CPA to new technologies
  - whether software can indeed be considered a product under CPA
  - if software is considered a product under CPA, who will have the responsibilit (& associated potential liability) to update over-the-air (OTA) software
  - how the state of the art defence & limitation will apply to updated OTA software
  - whether a data breach can be considered a defect under CPA if the data breach causes injury such as psychological damage. If so, may see a proliferation of product liability group actions where data breach in relation to smart consumer products

Intermediaries

- If app aids healthcare professionals in diagnosis/management of patient treatment app provider could owe duty of care to both healthcare provider & patients
- Healthcare professional may be expected to exercise judgement to apply diagnostic information provided by app
- Claims could arise against a hospital for clinician's failure to properly interpret data & to intervene quickly when data shows there to be an imminent risk to a patient's health
- Clinicians performing data analysis from wearables should be:
  - Insured to do so; &
  - Properly trained in data analytics in their field to minimise claims against them

Contributory negligence

- Onus on patients to monitor their vital signs & health via wearables & seek medical intervention when their vital signs suggest potential problem
- Harm could arise as a result of the patients' own failure to:
  - Care for devices
  - Use them in accordance with manufacturer's instructions
  - Maintain the product with necessary updates
- Clinics may have patients sign user agreements with disclaimers for harm caused as a result of device misuse

Recap on US academic commentary - Bethany Corbin 2019

- Going forward we need to seek a balance between:
  - A liability system that will hold software manufacturers accountable for their failure to adequately secure their products

  BUT

  - Guard against unfettered liability for smart device manufacturers who adequately secure their codes & products
- Aim - "*safe harbor*" statute that limits civil liability if smart device manufacturers/software companies comply with voluntary, industry-approved cybersecurity frameworks

Kennedys

US UPDATE

Kennedys

FDA Recalls

- More FDA recalls for medical devices and pharmaceuticals in 2020 than in 2019
- BD Alaris issued recalls for more than a million infusion pumps and pump modules in 2020 for software & hardware problems
- 3 recalls in August 2020 were class I FDA recalls i.e. a reasonable probability that product "*will cause serious adverse health consequences or death*"
- Top reason for medical device recalls in 2020 was software issues

Kennedys

"Software is the main driver with [medical device] recalls. It's been the top reason for 17 of the last 18 consecutive quarters. I predict that will continue to be a large focus just as more of these devices become more connected."

Chris Harvey
Vice President of Crisis Solutions
Stericycle Expert Solutions

US Update

Medical Device Cybersecurity

- **Feb 2021** - FDA appointed Kevin Fu as acting director of its new Center for Devices & Radiological Health
- Fu a prominent medical device security researcher has promised a new FDA cybersecurity draft guidance this year

Artificial Intelligence/Machine Learning-Based Medical Software

- **Jan 2021** - FDA issued its Action Plan for Artificial Intelligence/Machine Learning (AI/ML) Based Software as a Medical Device (SaMD)
- Intends to formulate guidance planned for later this year

Digital Health

- FDA expected to continue efforts to improve review & availability of smart medical devices

EU/UK UPDATE & REGULATORY CHANGES

UK's Medicines and Medical Devices Act 2021 (MMDA)

- Royal Assent on 11 February 2021
- A streamlined enforcement regime for ensuring safety & quality of medical devices in the UK
- Over-arching focus on patient safety
- While EU frameworks remain in place (through retained EU law) MMDA seeks to fill a regulatory gap that would otherwise arise when updating those frameworks

UK's Medicines and Medical Devices Act 2021 (MMDA)

- Wide-ranging powers to Secretary of State for Health to make regulations in relation to human medicines, clinical trials, veterinary medicines & medical devices
- Power to Secretary of State to share information about medical devices where safety concerns
- Also introduces civil sanctions as alternative to criminal prosecution for breaches of MDR

MDR – May 2021

- Far stricter pre-market scrutiny with conformity assessment by Notified Bodies
- EU database with sophisticated unique device identification traceability system
- Tougher post-marketing surveillance rules for manufacturers
- Greater co-ordination between EU countries on vigilance & market surveillance
- Heavier burden on medical health app developers to bring new products to the market

Connected Products & Cyber Security

April 2021

- UK government published a policy paper providing overview of its intentions for proposed legislation to regulate cybersecurity of connected consumer products
- Aim to implement a new robust scheme of regulation to protect consumers from insecure connected products

Artificial Intelligence

21 April 2021

- European Commission published its proposal for a regulation laying down harmonised rules on artificial intelligence with first ever legal framework on AI to address the risks & trustworthiness of AI
- Anticipate UK government will seek to implement similar measures in the UK

Kennedys

LOOKING INTO THE FUTURE

Kennedys

Recap on Futuristic Scenario & Other Issues

Scenario Facts

- Smart contact lenses app user
- Software malfunction results in delayed diagnosis of diabetic retinopathy

Potential Assigned Liability

- Lens Manufacturer
- AI app developer
- Patient for failing to update software as advised by manufacturer

Jurisdiction & Law

- If medical advice provided remotely via an app & accessed via roaming in multiple countries, which jurisdiction & what law will govern the medical treatment?

Data of wearable medical devices as evidence in litigation

- Key data from device relating to a user's health could become as important as medical records in personal injury claims to determine severity of an alleged injury & to either support or undermine such claims

CONCLUDING REMARKS

Mitigating Liability Risks:

- Robust software design & development
- Rigorous safety/security testing & monitoring pre-market
- Close & continuous post market surveillance & scrutiny of risk/benefit profile
- Effective procedures for investigating consumer complaints
- Adequate labelling, warnings & instructions clearly defining the intended use of device/service app
- Clear disclaimers
- Robust product recall & traceability procedures
- Cybersecurity & data privacy protection
- Risk management & incident responses for cyber attacks
- Implement AI machine learning to detect & deal with emerging cyber crime
- Keep up-to-date with evolving legal & regulatory requirements
- Product liability & recall insurance should be maintained and kept under review
- Seek indemnities to protect from product liability claims within supply chain

- Smart medical devices & service based apps
  - Potential to vastly improve healthcare & patient outcomes

BUT

  - Potential complex risks & liabilities

???

karishma.paroha@kennedyslaw.com

53

@KennedysLaw

linkedin.com/company/Kennedys

kennedyslaw.com

Kennedys

54