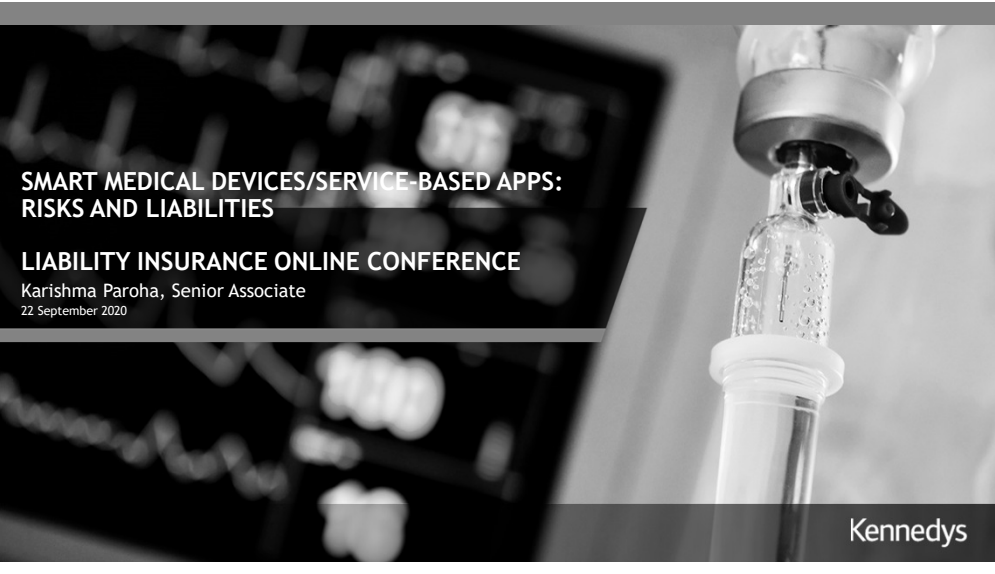
WELCOME TO:

SMART MEDICAL DEVICES/SERVICE-BASED APPS: RISKS AND LIABILITIES

KARISHMA PAROHA

THE LECTURE WILL START SOON !

Kennedys



SMART MEDICAL DEVICES/SERVICE-BASED APPS: RISKS AND LIABILITIES

LIABILITY INSURANCE ONLINE CONFERENCE

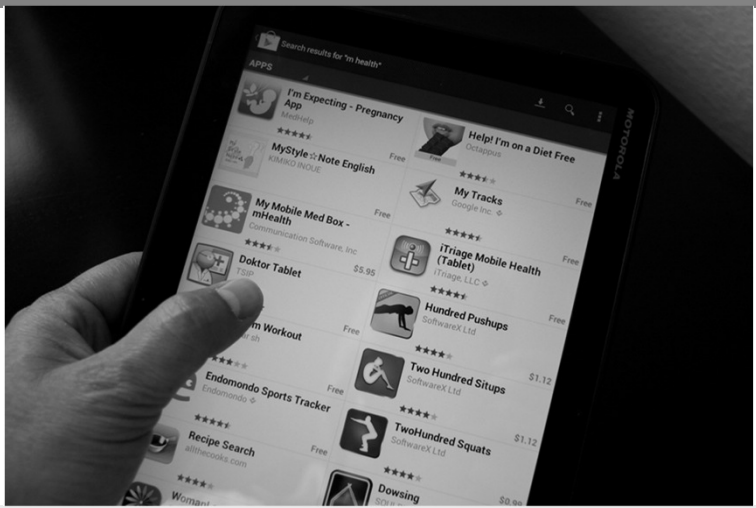
Karishma Paroha, Senior Associate

22 September 2020

Kennedys

Agenda

- Statistics & Predictions
- Definitions of Medical Devices
- Variety of Smart Medical Devices
- Risks
- USA Recalls
- Product Liability
- Jurisdiction & Law
- FDA Recommendations & US Law Update
- EU/UK Regulatory Changes
- Case Scenario & Concluding Remarks


Search results for "m health"
APPS
I'm Expecting - Pregnancy App
MedHelp
Free
MyStyle☆Note English
KIMIKO INOUE
Free
My Mobile Med Box - mHealth
Communication Software, Inc
Free
Doktor Tablet
TSIP
$5.95
m Workout
Free
Endomondo Sports Tracker
Endomondo
Free
Recipe Search
allthecooks.com
Free
Help! I'm on a Diet Free
Octappus
My Tracks
Google Inc.
Free
iTriage Mobile Health (Tablet)
iTriage, LLC
Free
Hundred Pushups
SoftwareX Ltd
Free
Two Hundred Situps
SoftwareX Ltd
$1.12
TwoHundred Squats
SoftwareX Ltd
$1.12
Dowsing
MOTOROLA

Impact of Covid19 Pandemic

- Healthcare system pushed to limits
- Lack of space in hospitals
- Remarkable increase in medical health apps
  - assist with tracking progress of virus
  - monitoring the vital statistics of potential sufferers
- Highlighted importance of smart medical devices & wearable remote monitoring devices (hospital & home)
- Taking care of ourselves

STATISTICS & PREDICTIONS

Kennedys

Smart Devices

- As of September 2020 7.62 billion humans on our planet

- How many smart devices globally are predicted to up and running by 2021?

Medical Devices & Predictions

- Grace Market Data predicted in 2012 -2020 Global Medical Devices Market Forecast:

  - Global medical devices market sales revenue would reach $543.9 billion by 2020

  - Driven by driven by:
    - Aging population;
    - Increasing healthcare expenditure; &
    - Technology advancement

Smart Medical Devices & Predictions

- According to Deloitte:
  - Worldwide market for smart medical devices predicted to grow to $52.2 billion in 2022:
    - Stationary medical devices - $17 billion
    - Implanted medical devices - $18.9 billion
    - Wearable external medical devices - $16.3 billion

Smart Medical Devices & Predictions

- According to Grand Review Research:
  - Factors propelling market growth:
    - Increase in adoption of smartphones globally
    - Rising demand for wireless & smartphone-compatible medical devices
    - An increasing awareness & focus on health & fitness
    - Growing demand for home healthcare

Smart health world

- Key Players:
  - Healthcare services
  - Patients & Users
  - Software developers (& investors)
  - Manufacturers
  - Virtual GPs
  - Virtual pharmacists

Smart health world

- Products & Services:
  - E-prescriptions
  - Remote monitoring
  - Smart diagnostic tools & health apps
  - Smart hospital monitoring equipment
  - Genomic data, biomarkers
  - AI imaging, detection & diagnosis

DEFINITION OF MEDICAL DEVICES

Kennedys

What is a medical device?

Art. 1 (2) of Directive 93/42/EEC Medical Devices Directive:

"*any* ***instrument, apparatus, appliance, software, material or other articles****…, for the purpose of:*

> ***diagnosis, prevention, monitoring, treatment or alleviation of disease****;*

What is a medical device? … continued

- Software in its own right in well-being setting is not a medical device
- Once data is processed to make a diagnosis smart medical product/smart phone service app is a medical device
- Considered medical device if it is ***intended*** as one by the manufacture
- Data on labelling, IFUs & packaging will be considered to establish intention

So what is not a medical device?

- If no diagnosis or treatment then smart product/service app is not a medical device
- Not medical devices where there is information with no input from the user e.g.
  - medical dictionaries
  - medical flash cards
  - patient education

VARIETY OF SMART MEDICAL DEVICES

Kennedys

Smart & Internet of Things (IoT) medical devices

- Deep brain neuro-stimulators, cochlear implants, food drop implants, gastric stimulators, defibrillators, pacemakers

- New health gadgets + smartphone:
  - Monitor vital signs; &
  - Self-manage chronic conditions

- Wearable technology
  - Melanoma detection
  - Bed sores prevention

Wearable smart contact lenses

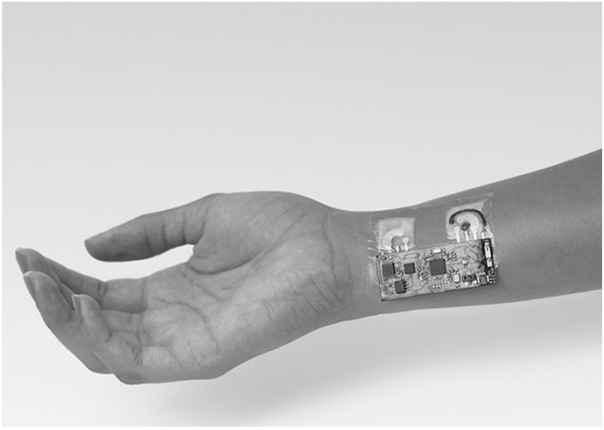
- Findings *Science Advances*:
  - Wireless powered
  - Biocompatible polymers
  - Diagnose & treat diabetic retinopathy
  - Drug delivery with biosensors & electrical signals
  - Glucose level in tears of diabetic rabbits analysed by smart contact lenses matched blood glucose level
  - Research conducted to expand scope of using electrical stimulations to treat brain disorders such as Alzheimer's & mental illnesses

Wireless smart glucometer

- FDA approved
- Measures glucose levels in blood
- Displays results on smartphone
- Keep a history of all measurements
- Share results with doctor

A smart insulin adhesive microneedle patch

- Size of a coin, one day use
- Monitor & manage glucose levels in diabetic
- Delivering necessary insulin dosage & mimics regulatory function of pancreas
- Help prevent overdosing, hypoglycemia, seizures, coma & potential death
- Currently tested on mice & pigs & accepted by FDA's Emerging Technology Program
- Application for FDA approval for human clinical trials anticipated to start in few years
- Smart patch could be adapted with different drugs to manage other medical conditions



Remote home testing kit

- Basic medical exam at home equipped with:
  - Digital camera
  - Thermometer
  - Tongue depressor
  - Otoscope
  - Stethoscope - heart, lungs & abdomens

- Teleconferencing app - connects with certified healthcare provider
- Remote consultation
  - Diagnosis
  - Treatment plan
  - Prescription if needed

A personal ECG

- FDA-cleared mobile ECG monitor
- Track your heart health anytime, anywhere
- Dedicated app
- Delivers a medical-grade electrocardiogram (ECG) to smartphone in just 30 seconds

Next generation of smart medical implants

- Revolution of nanoelectronics & smart chips

- Implantable devices - smaller, smarter & more lightweight & connected & packed with functionality:
  - More energy efficient
  - Biocompatible
  - Better performance
  - Increased patient comfort
  - Customised diagnosis

- Wireless technology
  - Charging the implant with portable device
  - Sending data it generates to external devices/attending physician

RISKS

Kennedys

Smart medical devices/service apps & risks

- Inherent to the App
  - Defective design
  - Inaccurate or out of date content/readings/advice
  - Failure to diagnose
  - Programming errors - malfunctions
  - Lack of support to users to report potential safety issues
  - Inadequate warnings/unclear instructions
- External Factors
  - Usage outside design
  - Usage by others not intended for by developer
  - Inappropriate training
  - High usage
  - Low detection environment
  - Lack of connectivity
  - Cyber attack

Smart medical devices/service apps & risks

- Purdue University Professor Shreyas Sen (specialising in smart device connectivity & security):

  "Even if these devices did have encrypted signals, they are still on a radio frequency that a hacker could detect 5 to 10 meters away from the medical device."

- Convince consumer & manufacturer necessary security features worth increasing cost
- 30 times more expensive to fix security flaws than to incorporate features in first place
- Recommends updating devices with a software-based encryption algorithm as a patch

Cyber Attacks

- Vulnerability issues - software is hacked, malfunctions, or fails to update
- Cyber-attacks on connected medical devices could result in "*severe consequences on patient safety*"

Data protection

- Personal data regarding health
- Take into account GDPR obligations at outset of design
- Only strictly necessary personal data processed for a specific purpose
- Adopt adequate security measures against potential data breaches:
  - Encryption of the users' data; &
  - Appropriate users' authentication mechanisms

US FOOD & DRUG ADMINISTRATION (FDA) RECALLS

Kennedys

FDA Recalls

- FDA smart medical device recalls in 2004, 2012 & 2016
- Software issues allegedly leading to patient overdoses, injuries & death
- August 2017 - Circa 500 thousand radio-controlled implantable pacemakers recalled by FDA:
  - Fears of lax cybersecurity - hacked to run batteries down or even alter patient's heartbeat
  - Pacemakers not removed (invasive & dangerous)
  - Firmware update applied by medical staff to patch security holes remotely

FDA Warning & Medtronic Recall 27 June 2019

"The FDA has become aware that an unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby MiniMed insulin pump with cybersecurity vulnerabilities. This person could change the pump's settings to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar and diabetic ketoacidosis."

FDA important recommendations

- *"To minimize the potential risk of a cybersecurity attack while you are waiting for a replacement pump:*
  - *Keep your insulin pump and the devices that are connected to your pump within your control at all times whenever possible.*
  - *Do not share your pump serial number.*
  - *Be attentive to pump notifications, alarms, and alerts.*
  - *Monitor your blood glucose levels closely and act appropriately…"*

PRODUCT LIABILITY

Kennedys

Product Liability

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

Product Liability

- **Reasonable expectation:**
  - When a consumer has/uses an IoT medical device does the consumer expect that hackers will be able to infiltrate the software?
  - Does the consumer expect the product will be designed in a manner in which software 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, physician who recommends smart medical device to patient

- Difficult to apportion liability

Crucial potential questions:

- Nature of the product's defect? Internal or external defect or both?
- How did the defect occur?
- Was manufacturer or software designer capable of designing a system that was immune to the alleged cybersecurity attack?
- Was the alleged "defect" reasonably foreseeable given the general public's awareness of cybersecurity issues?
- 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?

US academic commentary

- Seeking a balance between:
  - A liability system that will hold software manufacturers accountable for their failure to adequately secure their products

  BUT

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

Intermediaries

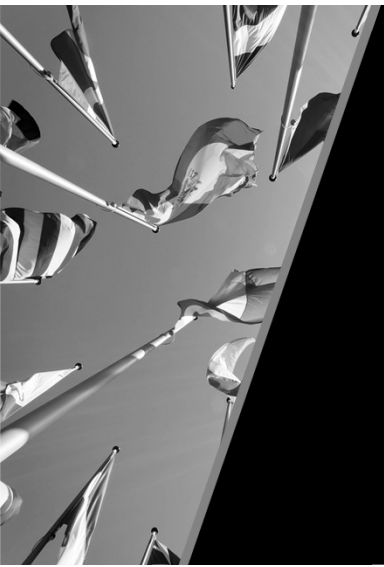
- If app intends to aid healthcare professionals in diagnosis or management of patient treatment app provider could owe duty of care to both healthcare provider & patients
- Healthcare professional may be expected to exercise judgement to apply diagnostic information provided by app
- Claims could arise 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

Intermediaries

- If products supplied by hospital users may seek redress against hospital as well as manufacturers under the CPA 1987
- Ensure contracts with manufacturers clearly stipulate manufacturers will indemnify the supplying clinics where any harm is caused to its patients as a result of defective devices
- Determining liability will be complex but manufacturers likely to bear major share of any liability

Contributory negligence

- May become more commonplace in such litigation
- 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
- Clinics may have patients sign user agreements with disclaimers for harm caused as a result of device misuse



JURISDICTION & GOVERNING LAW

Kennedys

Jurisdiction & Law

- Medical advice provided remotely via an app & accessed via roaming in multiple countries
- Healthcare advice provided from India is accessed by patient in Finland
- Which jurisdiction & what law will govern the medical treatment?
- Can a doctor remotely administer a treatment that has been approved in his country but not in the country in which the patient is located?

FDA RECOMMENDATIONS/US LAW UPDATE

Kennedys

"developers of private apps could limit their liability risks by designing accurate, reliable apps that include built-in procedures reasonably calculated to protect users' data. Developers also should include clear educational materials about products' proper use and warnings about improper use"

California connected devices security law

- 1 January 2020 new law took effect:

*"**a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device**, appropriate to the information it may collect, contain or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification or disclosure, as specified."*

- Requires manufacturers to:
  - Equip a "connected device" with "reasonable security"
  - Protects consumers from attackers gaining access to those devices

California connected devices security law

- "*Connected*":
  - Connects to the internet; &
  - Has an IP or Bluetooth
- Does not generally apply to medical device manufacturers
- Influence how FDA defines cybersecurity for smart medical devices

EU/UK REGULATORY CHANGES

Kennedys

New European Medical Device Regulation ("MDR") & In Vitro Diagnostic Medical Devices Regulation ("IVDR")

- Published May 2017 will replace existing framework under MDD
  - Active implantable devices
  - Devices utilising nanomaterials & medical software
  - Devices intended to be ingested or inhaled
  - Devices utilising non-viable tissues or cells of human origin

- A 3 year transition period for MDR & a 5 year for IVDR

- Impact of pandemic MDR pushed back to 26 May 2021
  - Enable medical device manufacturers to focus on producing medical devices to fight COVID-19

MDR

- **Objectives**
  - Ensure EU legislation adapts to progress in science & technology
  - Ensure users of medical devices have high level of health and safety protection
  - Provide fair & free trade of medical devices

- **Key changes**
  - High-risk devices being subjected to a far stricter pre-market scrutiny
  - Stronger oversight procedures 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

MDR

- Under the MDD majority of software falls under Class I
- Under MDR medical apps may be move into a higher risk class and implies:
  - Notified body involvement in the conformity assessment
  - A heavier burden on medical health App developers
  - More costly & more time

UK's Medicines and Medical Devices Bill 2020

- Received second reading on 2 September 2020
- When passed will consolidate enforcement regime for ensuring safety and quality of medical devices in the UK
- Part 3 of the Bill creates a delegated power for *Medical Devices Regulations(MDR) 2002* to be updated in limited number of areas:
  - the manufacture, marketing and supply of medical devices;
  - the charging of fees in relation to medical devices (eg to register a device);
  - recording information about the safety of devices;
  - creating offences of breaching the provisions in the MDR; &
  - the supply of medical devices in emergencies
- Provides Secretary of State with new information sharing powers relating to the safety of a medical device

CASE SCENARIO

Kennedys

Futuristic scenario

Facts

- 70 year old smart medical device app user Alexa. She is a diabetic who wears smart eye contact lenses, which deliver drugs to her eyes via electric signals as & when required
- The lenses are connected to an AI app & record any macular degeneration & provide Alexa with warnings as and when he should seek medical attention
- The AI app triggers a warning alert to Alexa, her on-line GP, her virtual specialist monitoring Ophthalmologist in South Africa and her local treating hospital team
- The software on the lenses needs to be updated every 12 months & the onus to update is on Alexa as the app user
- Alexa receives a warning from her treating hospital to update the lenses remotely via a request to the manufacturer, but she doesn't pay attention & forgets to update it

Futuristic scenario

Damage Caused:

- When Alexa attends finally hospital for an eye check-up it is noted that she has irreversible diabetic retinopathy, which is likely to lead to bilateral blindness in the future

Proven Defect:

- After a thorough investigation it is discovered that the AI system built into the app had a software malfunction, which meant it had failed to provide warnings to Alexa & her virtual medical team much sooner than it actually did

- It is not as yet clear if the software malfunction was due to the fact that the software was not updated by Alexa

Futuristic scenario

Potential Assigned Liability:

- The smart contact lenses manufacturer, the smart medical device AI app developer and the AI provider could all be potentially held responsible for the failure of the app to provide sufficient warning to Alexa & her virtual medical team

- It is also arguable the Alexa may be held contributory negligent for failing to update the software to her AI app as advised by the manufacturer in the instructions & by the hospital when the lenses were prescribed & regular reminders thereafter

Potential Cost:

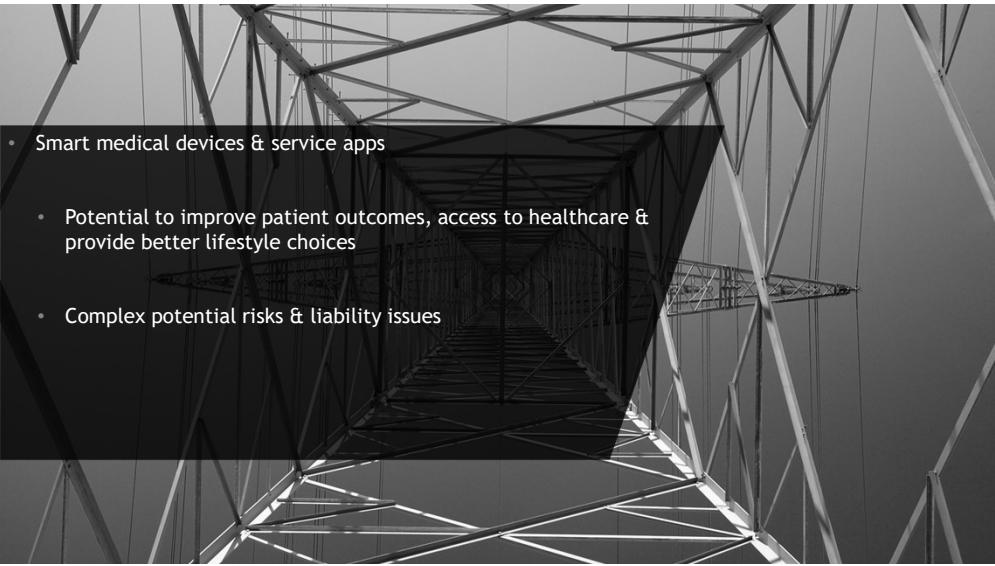
- Compensation for Alexa for pain and suffering of loss of sight in both eyes & related special damages

CONCLUDING REMARKS

- Smart medical devices stakeholders - manufacturers, importers, software designers, app developers must:
    - Be aware of risk of potential product liability claims (software vulnerability &/or cyber security risk allegations)
    - Evaluate insurance coverage & exclusions
        - Insurance policies may not provide coverage for every consequence of a cyber attack
        - Consider cover for technology product liability, clinical negligence, cyber liability

- Mitigating liability risks:

  - Robust software design & development protocols
  - Rigorous safety/security testing & monitoring pre-market
  - Close & continuous scrutiny of risk/benefit profile
  - Effective procedures for logging & investigating consumer complaints
  - Adequate labelling & instructions clearly defining the intended use of the device/service app
  - Robust post market surveillance
  - Clear warnings, contraindications & disclaimers
  - Co-ordinate plans for cybersecurity & data privacy protection
  - Implement risk management & incident responses for cyber attacks
  - Consideration of AI machine learning to detect & deal with emerging cyber crime
  - Keep up to date with expanding legal & regulatory requirements



- Smart medical devices & service apps
  - Potential to improve patient outcomes, access to healthcare & provide better lifestyle choices
  - Complex potential risks & liability issues

???

karishma.paroha@kennedyslaw.com