BSSH Guidance on the Use of Imaging, Digital Tools, and AI in Hand Surgery

Disclaimer: This guidance is issued by the British Society for Surgery of the Hand (BSSH) as an advisory document. It is intended to support best practice across all clinical levels in hand surgery, but it is not legally binding. Clinicians should exercise professional judgment and comply with local policies and laws when implementing this guidance.

1. Purpose and Scope

This document provides comprehensive guidance on the integration of medical imaging, digital technologies, and artificial intelligence (AI) in hand surgery practice. It may be of benefit to clinicians involved in hand surgery, including surgeons, trainees, and allied health professionals, across both NHS and private settings. The guidance covers the following sections:

- **Core Principles** for the use of imaging, digital tools, and AI in hand surgery.
- **Legal and Regulatory Framework** in the UK (including UK GDPR/Data Protection Act 2018, GMC confidentiality standards, MHRA regulations for software/AI as medical devices, ICO guidance, NHS England requirements, and intellectual property considerations).
- **Imaging Modalities** relevant to hand surgery (radiographs, ultrasound, CT, MRI, and 3D imaging) and their proper use.
- **Digital Tools** such as PACS, electronic PROMs, communication platforms, and telemedicine, with guidance on safe and effective use.
- **Artificial Intelligence** applications in hand surgery, outlining types of AI, clinician responsibilities, potential risks, and governance requirements.
- **Practical Guidance** providing real-world examples and recommendations for daily practice.
- **Governance and Audit** considerations to ensure ongoing compliance, safety, and quality improvement.

This guidance aims to promote patient safety, data security, and effective clinical outcomes when adopting new technologies in hand surgery. It supplements – but does not supersede – existing laws, regulatory standards, and hospital policies. All

recommendations should be interpreted in conjunction with mandatory legal requirements and ethical duties.

2. Core Principles

When utilising imaging, digital systems, or AI in hand surgery, clinicians and healthcare providers should adhere to the following core principles:

- **Patient Safety:** Prioritise patient safety and clinical efficacy. New tools should never compromise the standard of care. Technologies (from imaging devices to AI algorithms) must be validated and used only within their proven capabilities. If an AI or digital aid suggests an output that conflicts with clinical judgment or guidelines, the clinician must carefully evaluate and, if necessary, override it in the patient's best interest.

- **Confidentiality and Data Privacy:** Protect patient confidentiality and privacy at all times. Medical images and digital records contain personal health information and must be handled according to UK GDPR and the Data Protection Act 2018. Only authorised personnel should access patient data, and information sharing must be justified on a need-to-know basis. All staff have a personal responsibility to safeguard information as outlined by GMC confidentiality guidance.

- **Compliance with Law and Regulation:** Ensure all imaging and digital tools are used in compliance with relevant laws and regulations. Health data is considered "special category" personal data under UK GDPR, requiring a lawful basis for processing and stringent safeguards. Software and AI systems used for diagnosis or treatment planning may be regulated as medical devices; such tools must have appropriate MHRA approval or UKCA/CE marking before clinical use. Clinicians should confirm that any AI-driven software has been certified for its intended purpose and meets Medicines and Healthcare products Regulatory Agency (MHRA) requirements.

- **Transparency and Informed Consent:** Maintain transparency with patients regarding the use of new technologies in their care. Patients should be informed when novel digital tools or AI are being employed as part of diagnosis or treatment. Obtain informed consent for any recording or use of patient images beyond direct care. For example, explicit written consent is required before using patient photographs in research, publications, or teaching materials. When AI is used to assist decision-making, patients should be made aware of its role, especially if it involves any form of automated decision support.

- **Accountability and Human Oversight:** Use AI and digital aids to support – not replace – clinician judgment. The clinician remains ultimately responsible for clinical decisions and patient outcomes. AI outputs or algorithmic suggestions must be reviewed by a qualified hand surgeon or clinician, who will make the final decision in consultation with the patient. If an AI tool is unsure or flags an unusual result, clinicians must investigate further rather than accept the result at face value. Clear accountability structures should be in place: for example, who oversees the validation of an AI diagnostic tool, who responds if the tool fails, and how to address errors.

- **Data Security and System Integrity:** Maintain robust cybersecurity and data protection measures for all digital systems. This includes using secure, encrypted channels for communication, strong access controls (passwords, two-factor authentication) for systems containing patient records or images, and compliance with NHS England's data security standards (such as the Data Security and Protection Toolkit). Personal devices should not be used to store patient data unless absolutely necessary and permitted; if used, they must be encrypted and data transferred to secure storage as soon as possible. Any data breaches or unauthorised access must be reported promptly in line with NHS incident protocols – including to the Information Commissioner's Office.

- **Quality, Audit and Efficacy:** Adopt technology that has a clear clinical benefit, is auditable, and is evidence-based. Digital tools and AI algorithms should undergo quality evaluation and, where available, meet relevant evidence standards (e.g. NICE evidence frameworks for digital health technologies). Hand surgery units are encouraged to trial new tools in controlled settings and gather outcome data – auditing after deployment. If a tool does not demonstrably improve care or efficiency, its use should be re-assessed. Regularly review the literature and emerging evidence on imaging techniques or AI in hand surgery to ensure practice remains up-to-date.

- **Education and Training:** Ensure all staff are appropriately trained to use imaging equipment, digital platforms, and AI tools. Competency is crucial – for instance, surgeons and radiologists should be familiar with proper image acquisition techniques and interpretation, and clinicians should know the functioning and limits of an AI diagnostic aid. Training on data protection and confidentiality should be included as part of the introduction of any new digital tool. Users must know how to securely handle patient images, how to interpret AI outputs, and how to troubleshoot errors. Training should be ongoing, especially as software is updated or new features introduced.

- **Ethical Use and Equity:** Deploy technologies in an ethical manner, ensuring equitable care. Be vigilant to avoid bias: for example, AI systems should be monitored

for performance across different patient demographics to ensure one group is not disadvantaged. The ICO's guidance on AI emphasises evaluating "allocative harms" and "representational harms" – e.g. an AI trained mostly on data from one population may perform worse on others. Hand surgeons should therefore use AI that has been developed and tested on appropriately representative data (or be aware of its limitations). Moreover, access to digital tools should be equitable for patients; for instance, if using an electronic PROMs system or telemedicine follow-ups, provide alternatives for patients who are less digitally literate or lack access to technology to avoid exacerbating healthcare disparities.

By adhering to these core principles, hand surgery teams can integrate imaging, digital tools, and AI in a way that enhances patient care while upholding legal, ethical, and professional standards.

3. Legal and Regulatory Framework

Hand surgeons and healthcare organisations must navigate several UK legal and regulatory requirements when using imaging, digital platforms, or AI. This section outlines the key frameworks and standards:

3.1 UK GDPR and Data Protection Act 2018

All patient data – including radiographs, clinical photographs, and digital health records – is protected under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Health information is classified as "*special category personal data*", which means it warrants a high level of protection.

Under these laws, any processing of patient data must satisfy a lawful basis (for clinical care, this is typically *"direct care"* or *"medical purposes"* under the umbrella of consent or vital interest, and in NHS settings often covered as provision of care under implied consent) and meet an Article 9 condition for special category data (such as provision of health or social care). Key GDPR principles must be followed: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. In practice, this means hand surgery units should only collect necessary information, keep it accurate and up-to-date, store it securely (e.g. in the UK hand registry), and not retain it longer than needed.

Healthcare providers are Data Controllers for patient information and must ensure compliance with GDPR. They should have data protection policies and training in place. Notably, if introducing a new digital system or AI that will handle patient data, a Data

Protection Impact Assessment (DPIA) is usually required before deployment. The Information Commissioner's Office (ICO) recommends DPIAs especially for new technologies like AI due to potential high risk to privacy. A DPIA helps identify and mitigate risks (for example, assessing if an AI image analysis tool might inadvertently expose patient data or produce biased outcomes).

Patients have rights under GDPR, including the right to be informed about how their data is used, the right of access (patients can request copies of their imaging and records), and rights to rectification or objection in certain cases. Clinicians should be aware that patients can request their medical images and records – usually facilitated as a Subject Access Request – and these should be provided within the legal timeframe (typically one month) unless an exemption applies. However, copyright of clinical images is separate from data access rights (see Section 3.5).

3.2 Common Law Duty of Confidentiality and GMC Guidance

Aside from data protection statutes, clinicians must uphold the common law duty of confidentiality and professional guidelines. Information given by a patient in a medical context is confidential and generally should not be disclosed to others without the patient's consent. This duty covers not only verbal and written information but also photographs, X-rays, and any other patient-identifiable data.

The General Medical Council (GMC) in its guidance "Confidentiality: good practice in handling patient information" sets out fundamental principles: doctors should seek to disclose the minimum *necessary information*, share information on a need-to-know basis for care, and usually obtain patient consent for any disclosure outside the care team. There are defined exceptions (such as legal reporting obligations or if withholding information would pose a serious risk to others), but these are applied case-by-case. When using digital communication or telemedicine, the same standards apply – e.g. a video consultation should be conducted in a private setting to prevent others overhearing patient information, and if screenshots or recordings are needed for clinical reasons, patient consent and secure storage are required.

GMC confidentiality guidance (2018) also emphasises doctors' personal responsibility in protecting information: you must make sure any personal patient data you control is effectively protected at all times, whether it's on a hospital computer, a personal phone, or being transmitted electronically. In practical terms, clinicians should not use unapproved apps or personal email accounts to send patient details. NHS policies typically dictate using official secure email (e.g. nhs.net accounts) or approved messaging systems. According to NHS Digital guidance, *"You must never send personal, sensitive or confidential information to a non-secure email address unless it is*

encrypted." This applies if, for example, sending imaging to a patient or colleague – only use secure/encrypted channels.

Consent is a crucial part of confidentiality. For direct care, sharing among the treating team is considered implicit in the patient's consent to treatment. However, if using patient data for secondary purposes (research, teaching, publication), explicit consent should be obtained unless data is fully anonymised or another legal basis applies. For instance, if a surgeon wishes to use an intra-operative photo or other image (e.g. photo of an x-ray) of a patient's hand in a conference presentation, they must get the patient's consent (often documented via a photography consent form) because this use is outside normal care. Most NHS Trusts have specific consent forms for medical photography indicating whether images may be used for education or publication. Patients have the right to refuse or to place limitations (e.g. images can be used for teaching within the hospital but not published online).

Additionally, the common law duty of confidentiality extends beyond a patient's death – health records of deceased patients should still be handled respectfully and disclosed only for valid reasons. The Access to Health Records Act 1990 covers who can request records of the deceased (usually next of kin or executors).

3.3 Medicines and Healthcare products Regulatory Agency (MHRA) – Software as a Medical Device (SaMD)

Digital health tools and AI algorithms that perform medical functions (such as diagnosing conditions, guiding treatment, or providing clinical decision support) may be classified as medical devices. In the UK, the MHRA regulates medical devices to ensure they are safe and effective. Software (including AI) that provides diagnosis or influences treatment is very often considered a medical device and thus must comply with medical device regulations. This holds true for many innovative tools in hand surgery – for example, an AI that analyses wrist X-rays to detect fractures would likely be deemed a medical diagnostic device.

Manufacturers (or developers) of such software are responsible for obtaining the appropriate conformity marking (currently UKCA for Great Britain, CE for Northern Ireland or if EU compliance is sought) before the product can be used clinically. The classification of software devices typically depends on risk: an AI that provides information for diagnosis or therapeutic decisions often falls into Class IIa or IIb under EU/UK rules, due to the potential to significantly impact patient care. Hand surgery units adopting an AI tool should verify its classification and approval. Using an uncertified medical device is not permitted in routine practice – doing so could breach regulations

and put patients at risk. The MHRA's guidance "Software and AI as a Medical Device" provides detailed criteria for qualification and classification. Key points include:

- Determining if the software has a medical purpose (diagnosis, prevention, monitoring, treatment, or alleviation of disease or injury). If yes, it's likely a medical device and must meet device regulations.
- Assigning the correct risk class based on potential harm if the software fails or is inaccurate. Higher risk (e.g. software that drives clinical decisions in acute care) demands more stringent controls and oversight.
- Pre-market requirements: the developer must ensure the product meets safety, performance, and quality standards (for example, following UK Medical Device Regulations 2002 as amended, which encompass design controls, risk management, and clinical evaluation of the software). Documentation such as a technical file and clinical evidence must be in place to demonstrate that the software is effective for its intended use and safe.
- Post-market surveillance: once deployed, any incidents or adverse events involving the software should be tracked and reported. The MHRA operates the Yellow Card Scheme for reporting adverse incidents with medical devices, including software. If, for example, an AI tool in hand surgery repeatedly misses a certain type of tendon injury on ultrasound leading to delayed treatment, these incidents should be reported as they might indicate a safety issue requiring investigation or improvement of the tool.

The MHRA is actively updating guidance and regulations to keep pace with AI. Specific challenges like algorithm "drift" (AI performance changing if it learns from new data) and transparency (the "black box" issue of machine learning[1]) are being addressed in policy development. The MHRA, in collaboration with international counterparts, has published 10 guiding principles for Good Machine Learning Practice (GMLP) to ensure AI/ML medical devices are safe and effective across their lifecycle. Hand surgeons should prefer AI tools developed in accordance with these best practices.

In summary, before deploying any software or AI system for clinical use in hand surgery, confirm it is appropriately certified as a medical device if required. If a hospital develops its own tool "in-house" (e.g. a custom algorithm for research), there are exemptions in certain cases (like the MHRA's guidance on Health Institution Exemption for devices made and used within the same organisation), but strict conditions apply and patient

[1] The concept that AI reason and function occurs within a "black box" that humans may not always be able to understand or explain.

safety must remain paramount. Always liaise with your institution's medical device/clinical governance committee or the manufacturer to ensure regulatory compliance.

3.4 ICO Guidance and Information Governance (IG) in NHS

The Information Commissioner's Office (ICO) is the UK's regulator for data protection. The ICO has issued specific guidance on AI and data protection, which, while aimed at industry broadly, contains points highly relevant to healthcare. Key aspects of the ICO guidance include:

- **Accountability and governance:** Organisations deploying AI are accountable for how those systems process personal data. There should be clear governance structures overseeing AI projects. For healthcare providers, this means involving your Data Protection Officer (DPO), Caldicott Guardian, and Information Governance leads from the outset. For example, if a hand surgery department wishes to use a machine learning model to predict patient outcomes, they should have approval from their IG committee and a named person responsible for ensuring compliance (e.g. the DPO reviewing the DPIA, the Caldicott Guardian confirming that patient confidentiality is respected in the data usage).

- **Data minimisation and quality:** Only the necessary data should be used to train or run AI, and it should be of good quality. If using patient datasets to develop an AI (say, feeding thousands of x-ray images to an algorithm), anonymise or pseudonymise data whenever possible to protect identities. If identifiable data is essential, consider if you need patient consent or support under the law (projects not directly related to care might need research approvals and potentially Section 251 support via the Confidentiality Advisory Group for using confidential data without consent in England). The ICO expects organisations to assess bias and representativeness in datasets – ensuring fairness. For instance, if creating an AI to identify bone tumours on hand x-rays, the training data should include a wide range of ages, ethnicities, and image qualities, or else note its limitations, to avoid an AI that only works well on certain subgroups.

- **Transparency to individuals:** Patients (data subjects) should be informed about AI involvement in an understandable way. The ICO's updated guidance includes how to explain AI decisions and usage to people in plain language. In practice, NHS hospitals often include information in their privacy notices about AI tools in use. If an AI tool makes a significant recommendation or decision about a patient's care , clinicians should be ready to explain how that decision was reached in general terms (recognising that complex algorithms can be difficult to fully explain, but the effort should be made to increase trust).

- **Automated decision-making:** GDPR Article 22 gives individuals rights regarding solely automated decisions that have legal or similarly significant effects on them. In healthcare, fully automated decisions without human oversight are rare (and arguably unethical). Typically, AI in hand surgery will be advisory (e.g. "the AI suggests this X-ray shows a fracture") rather than final. As long as a human clinician is making the ultimate judgment, it's not solely automated. Nonetheless, providers should ensure a human in the loop for critical decisions to avoid crossing into prohibited automated decision-making territory or, if they ever contemplate automation, ensure explicit patient consent and other safeguards.

- **Data Protection Impact Assessments (DPIAs):** As noted, performing a DPIA is usually mandatory for health AI projects. The ICO expects a DPIA to detail how data is used, potential risks to privacy, and measures to mitigate those risks. For example, a DPIA for implementing a telemedicine app might note the risk of unauthorised access if a video link is intercepted and describe encryption and access codes as mitigations.

- **Retention and data lifecycle:** Organisations must consider how long digital data (including images) will be kept. NHS records policies often specify retention periods (for example, adult medical records are kept for a minimum of 8 years in England after last treatment; x-rays typically the same). If AI models are trained on patient data, the data should not be kept indefinitely without reason. Also, if an AI system creates new data (like analytics or risk scores), those become part of the medical record and need proper retention and disposal schedules.

NHS-specific IG requirements also come into play. NHS England mandates annual compliance with the Data Security and Protection Toolkit, which covers the National Data Guardian's 7 Caldicott Principles and data security standards. Trusts and practices must demonstrate training, access controls, incident response, etc. for all systems. Any digital tool introduced should be compatible with these requirements. For communication tools, for example, NHS policy might allow use of certain messaging apps under specific conditions (e.g. WhatsApp in urgent situations if no alternative, but notes must be transferred to the record and the conversation deleted thereafter). Always check local IG policies.

3.5 NHS England Governance and NHSX Requirements

At a national level, NHS England (formerly through NHSX) has established frameworks to govern the introduction of digital technology and AI:

- **Digital Technology Assessment Criteria (DTAC):** The NHS Digital Technology Assessment Criteria is a standard checklist that health technologies must meet to be

used in NHS settings. DTAC covers five key areas: clinical safety, data protection, technical security, interoperability, and usability/accessibility. Before a new app, software, or device is procured or rolled out, the hospital's procurement or digital health team should ensure the product has been assessed with DTAC. For example, if a hand surgery unit wants to implement a smartphone app for patients to upload rehabilitation progress photos, the app should be evaluated for DTAC compliance – does it keep data encrypted, has it been through clinical risk management (perhaps to the standard of DCB0129/0160 clinical safety standards), is it user-friendly and accessible to those with disabilities, and can it integrate with NHS systems (like sending data to the electronic health record)?

DTAC essentially brings together legal requirements (like GDPR) and best practices. By meeting DTAC, a technology demonstrates it has met NHS expectations for safety and governance. NHS England has made it clear that any new digital tool, even if piloted, should go through a DTAC assessment. Health tech developers are encouraged to self-assess their products against DTAC and provide evidence to hospitals. Clinicians championing a new technology should liaise with their IT and IG departments to complete this process. Using DTAC helps protect patients and the organisation, by catching issues early – such as inadequate encryption or lack of a proper clinical risk management file.

- **NHS Code of Conduct for Data-Driven Health and Care Technology:** This code (initially published by NHSX) outlines principles for digital health tools, especially those involving AI. Principles include understanding user need, defining the outcomes, ensuring diversity of data, making tools secure, and being transparent about performance. While not legislation, this code is a best practice guideline that commissioners and clinicians should expect vendors to follow. It complements the regulatory requirements by focusing on ethical deployment (for instance, AI used in hand surgery should have an underpinning evidence base and be piloted to ensure it actually benefits patients).

- **Clinical Safety Regulations:** In the NHS, any software deployed that could affect patient care should have a clinical safety officer assigned and comply with standards like DCB0129 (for manufacturers/developers) and DCB0160 (for deploying organisations). These standards require hazard identification, risk assessment, and mitigation to be documented. For example, a trust rolling out a digital patient scheduling system must consider safety risks (like, what if an appointment booking fails to notify the patient?), and an AI triage tool for hand injuries must consider mis-triage risks. Governance processes should include reviewing these safety cases. It's often the Chief Clinical Information Officer or another senior clinician who signs off on the safety assessment before go-live.

- **NHSX/NHS AI Lab programs:** The NHS AI Lab (part of NHS England) has been conducting AI procurement frameworks and regulatory sandboxes to help evaluate AI in real-world settings. If a hand surgery department is part of an AI trial (say an algorithm reading hand x-rays), they should adhere to any guidance from these programs, which usually align with the principles above and often include extra monitoring and evaluation.

- **NHS England & Improvement guidance on telemedicine and digital consultations:** NHS England has provided guidance on running video clinics and using remote monitoring, much of which highlights confidentiality, ensuring the standard of care (e.g. doing an appropriate physical examination via video or arranging in-person review if not adequate), and making reasonable adjustments for those who struggle with technology. While not a separate legal framework, these guidelines should be followed for quality care.

In summary, NHS England expects organisations to have strong governance for digital health. This includes fulfilling IG requirements, assessing new tools against national criteria, and engaging in continuous oversight. Hand surgery departments should work within their hospital's digital governance structures – typically a digital or IT committee, IG committee, and possibly a medical devices group – to get approval and support for any new system or AI. Adhering to these processes not only ensures compliance but also usually gives access to resources (like IT support, training, and funding opportunities).

3.6 Intellectual Property (IP) and Copyright Considerations

The use of imaging and AI in hand surgery raises questions about intellectual property rights in images and in AI-generated materials:

- **Clinical images (photographs, radiographs, videos):** Under UK law, the creator of a photograph generally holds the copyright. In a hospital context, this typically means the photographer or the employer (NHS Trust) if the photo/x-ray is taken as part of their duties. For example, an x-ray image is generally treated as a photograph in legal terms. The radiographer who took it (or their employer) would own the copyright, not the patient. Indeed, many NHS Trusts explicitly state that they hold copyright on clinical photographs and videos made of patients. Patients, however, have rights to access those images as part of their medical record (data protection) but cannot sell or license them, since they are not the IP holder. Patient are required to go through formal trust processes in order to acquire their images in line with GDPR requirements.

  Even though the hospital holds copyright, patient consent and confidentiality still govern usage. A hospital cannot freely publish a patient's x-ray or clinical photo

without consent just because it owns the copyright – the patient's privacy rights intervene. Thus, from a clinician's perspective, any use of patient images must be cleared both in terms of consent and respecting that the image can't be used by others without permission of the copyright owner (usually the hospital). If a surgeon leaves a hospital, for instance, they should not take patient images to use elsewhere without permission. Always explain to patients when taking clinical photographs or videos for their record or for treatment planning. Use your hospital's consent forms for medical photography. If images may be used beyond the record (teaching, publication), secure specific written consent.

If a patient requests copies of their images (common with x-rays or MRI scans), the hospital will usually provide them under data protection rights or as a courtesy, but this does not transfer copyright. In practice, patients often share their x-rays (e.g. on social media) – while that might technically breach confidentiality from the hospital's perspective, the ICO has indicated if the patient themselves shares it, it's no longer confidential in the same way. Still, clinicians should advise patients about appropriate use of their medical images (especially if images contain identifiers).

- **AI-generated images or content:** With the advent of generative AI, one might create synthetic medical images (for teaching, for example) or use AI to generate patient education materials. UK copyright law (Copyright, Designs and Patents Act 1988) has a concept of *"computer-generated works"* where if a work has no human author, the author is deemed to be the person who undertook the arrangements necessary for its creation. In other words, if an AI produces an image without a specific human creating the artistic elements, the person (or entity) that directed the AI or provided the prompt/data might hold the copyright. This is a complex area and evolving; as of now, UK law gives a level of copyright protection to computer-generated images (unlike some other countries that might not). However, it's critical to note that such AI-generated images must not include or reveal real patient data unless authorised. If an AI is trained on patient scans and then generates a "composite" image, one must ensure it is sufficiently anonymised. There have been concerns that AI-generated outputs could inadvertently resemble real individuals from training data, so caution and possibly technical de-identification measures are needed.

  Clinicians using AI tools that create images (for example, an AI that reconstructs a 3D model from 2D images) should check the terms of the software – who owns the output? Many AI tool providers include clauses that either give the user a license or claim ownership. Ensure that using such outputs for patient care or publications does not infringe any IP. If a hospital staff member develops an AI algorithm or software as part of their job, typically the IP belongs to their employer (the Trust),

unless there's an agreement stating otherwise. This is analogous to inventions and patents in the NHS.

- **Educational materials and publications:** When including medical images in presentations or articles, be mindful of both patient consent and copyright. Journals often require a statement that you have patient consent for any identifiable images. Even anonymised x-rays can sometimes be identifiable (e.g. unique jewellery on an x-ray could identify a patient). If publishing AI-generated data or analysis, ensure you're not violating any dataset licenses. For example, using an open dataset of hand radiographs might come with conditions on attribution.

- **Software Intellectual Property:** If a department creates a novel digital tool (e.g. a mobile app for hand therapy exercises), the code and design can be IP that the hospital might want to protect (via copyright or patent if very novel). While this is beyond daily clinical practice, the team should involve their R&D or innovation office. Conversely, when using third-party software, respect their IP – e.g. do not attempt to reverse engineer proprietary AI algorithms or use them beyond licensed indications.

In summary, clinical images are both personal data and intellectual property. The NHS or clinician likely owns the image copyright, but ethical and legal use requires patient permission. Always follow local policies for medical photography (most hospitals have a photography consent procedure and policies about storing and using images). For AI outputs and other digital content, stay aware of IP rights – if in doubt, consult the hospital's legal or R&D department for guidance, especially if there's commercial or research use in view.

4. Imaging Modalities in Hand Surgery

High-quality imaging is central to diagnosing and treating hand conditions. Hand surgeons rely on various modalities – from traditional x-rays to advanced 3D imaging – each with specific uses and considerations. This section provides guidance on the main imaging modalities, ensuring their proper and safe use in practice.

4.1 3D Imaging and Emerging Modalities

"3D imaging" in hand surgery usually refers to technologies that provide three-dimensional data or outputs from imaging modalities:

- **3D Reconstructions from CT or MRI:** Modern CT scanners allow volumetric data that can be rendered into 3D images. Workstations or software can reconstruct bones in 3D, which is useful for understanding complex anatomy. 3D reconstructions of a comminuted intra-articular fracture can be rotated on screen to see undercuts

and hidden fragments that 2D slices might miss. Surgeons should request 3D reconstructions when they anticipate benefit, and radiology departments can often provide them. Be cautious, however – sometimes 3D reconstructions can be misleading if artifacts are present; always cross-check with raw slices.

- **3D Printing:** With the rise of 3D printing, patient-specific models are increasingly feasible. In hand surgery, this might be used for planning an osteotomy (e.g. printing a model of a malunited distal radius to plan corrective cuts and pre-contour plates) or for creating patient-specific guides. For instance, if you need to drill K-wire paths for a complex phalangeal osteotomy, a 3D-printed drill guide that fits on the bone can be designed. These applications are still specialised and often require collaboration with bioengineers. Turnaround time and cost need to be justified by clear benefit (complex deformity corrections, unusual anatomy, etc.). In paediatric hand deformities or congenital cases, 3D models can help parents understand the planned surgery better, improving consent and education. Any transfer of the information or images (e.g. between hospital and third party) needs to follow local information governance policies having undergone legal and security risk assessments.

- **Optical 3D Scanning:** This involves using devices (cameras or infrared scanners) to capture the surface anatomy in 3D. For example, to design a custom orthosis or prosthetic, a 3D scan of the patient's hand or stump might be done. These scans are non-invasive and have no radiation. In practice, occupational therapists or prosthetics labs might use this to ensure a snug fit for devices. Another application is mirrored hand scanning: scanning the normal hand and mirroring it to create implants or guides for the injured side (like mirror-image finger prostheses or templates for reconstruction).

- **Fluoroscopy with 3D (C-arm CT):** Some advanced theatres have C-arm machines that can do a rotational spin and reconstruct a 3D image (essentially an intraoperative CT of the hand). This can verify fracture reductions or implant placements in 3D before the patient leaves the operating theatre. For example, after scaphoid screw fixation, a 3D C-arm spin can confirm the screw is fully within the bone and not penetrating the cortex at an unseen angle. If available, this can reduce re-operation by catching issues immediately.

- **Nuclear Medicine (Bone Scans, PET):** While not "3D" in the same sense, it's worth mentioning that occasionally a bone scan (Tc-99m) or even a PET scan might be used in hand surgery scenarios – e.g. to detect multiple areas of infection or tumour metastasis. These provide metabolic imaging rather than structural. A three-phase bone scan can help confirm complex regional pain syndrome or occult fracture by showing increased uptake. PET CT might be used in cancer cases (like sarcomas) to

stage disease. These are specialised and guided by relevant protocols (like oncology input for PET).

- **Emerging Modalities:** Technologies like diffusion tensor imaging (DTI) for nerves, ultra-high field MRI (7 Tesla), or functional MRI of muscle movements are being researched. They aren't standard yet. However, AI-enhanced imaging is coming: e.g. AI algorithms that can generate a high-quality MRI image from a faster, lower-quality scan (to reduce scan time), or AI that can instantly create 3D reconstructions or even highlight pathology on images (like detecting a fracture automatically). These will likely become part of imaging workflows – early examples include algorithms that auto-detect wrist fractures on X-rays and flag them for review. The same clinical and legal cautions apply to those as discussed in the AI section.

In conclusion, each imaging modality has a role. The clinician's job is to choose the right test at the right time, and to work with radiology colleagues to interpret results in context. The advances in ultrasound, CT, MRI and beyond have greatly improved care of hand surgery patients. Hand surgery services should ensure they have sufficient access to these imaging tools and skilled radiologist.

5. Digital Tools in Hand Surgery

The digital revolution in healthcare extends to hand surgery in many forms: digital imaging storage, electronic health records, outcome tracking, communication platforms, and telemedicine. These tools can streamline workflows and improve patient engagement but must be used responsibly. Below we discuss major categories of digital tools and provide guidance for their use in hand surgery practice.

5.1 Picture Archiving and Communication System (PACS) and Image Management

PACS is the standard system for storage and retrieval of medical images in hospitals. Hand surgeons use PACS daily to view radiographs, CTs, MRIs, and ultrasound images. Key points for PACS and image management:

- **Timely Access:** All clinicians should have access to PACS terminals or viewers (including remotely via secure VPN if needed) to review images. Delays in loading images or inability to access certain modalities can impact care. Surgeons should familiarise themselves with PACS features: e.g. zoom, measurements (to measure angulation or distances on images), and comparison view (to view old and new images side by side).

- **Image Annotation and Sharing:** PACS often allows adding annotations or notes to images. Use these for teaching or surgical planning (without altering the original

image). For example, a surgeon might measure carpal alignment angles or mark a suspected fracture line and save that as a screenshot for discussion in MDT. However, be careful – any annotation saved can be seen by others and might be mistaken as a radiologist's label. Prefer using PACS-integrated tools that clearly mark it as user-added.

- **Security:** PACS is generally a closed system accessible only within the hospital network or via secure login. Never export patient images out of PACS to unsecured personal devices or email. If images need to be sent to another hospital or specialist, use approved methods (like image exchange portals or encrypted media). It's against policy to, for instance, take a photo of a PACS screen with your smartphone – not only does that create an uncontrolled copy of patient data, but the image quality is inferior. NHS guidelines emphasise that clinical images are confidential and must be treated with the same care as medical records.

- **Retention and Backup:** PACS archives images according to local retention schedules (often many years, and important images indefinitely). Clinicians don't usually need to worry about backup but should trust that PACS is the source of truth. If an image seems to be missing or mis-filed (e.g. an X-ray appears under the wrong patient), report it to PACS administrators immediately – misfiling is a patient safety issue as one person's images might be viewed as someone else's.

- **Integration with EHR:** Many hospitals have integrated PACS with electronic health records so that clinicians can click a link in a patient's chart to view images. Use these integrations to ensure you're looking at the right patient's images. Always double-check patient identifiers on images in PACS (name, DOB, hospital number) against your patient to avoid mix-ups.

- **Personal Image Management:** In clinic or theatre, surgeons sometimes capture their own images (like clinical photos or intra-op images on their phone endoscope). It is strongly advised to use hospital-provided photography services or secure apps designed for clinical photography and approved by national or local governance processes. If a surgeon does capture an image on a personal device in an urgent situation, it must be transferred to the official record system as soon as possible and deleted from the personal device. Many Trusts now provide encrypted digital cameras or secure camera apps to facilitate this process while maintaining compliance. For example, some NHS sites use apps where a photo taken through the app is directly uploaded to the EHR/PACS and never stored in the personal camera roll. Surgeons may believe that their devices are secure but they are at risk of being stolen, hacked, or lost. Additionally, cloud back-ups provide an extra portal of concern as servers may be compromised which can risk patient data. Therefore,

there are very limited circumstances in which saving photographs on personal devices without NHS and governance-approved software is justifiable.

5.2 Electronic Patient-Reported Outcome Measures (PROMs)

Measuring outcomes from the patient's perspective is crucial in hand surgery (e.g. DASH or QuickDASH score for upper limb function, pain scores, satisfaction surveys). Digital PROMs platforms allow these to be collected efficiently:

- **Platforms and Tools:** There are web-based or app-based PROMs systems that can email or text patients standardised questionnaires at set time intervals (e.g. pre-operatively, 3 months post-op, 1 year post-op). Some are integrated into the hospital's patient portal or EHR, others are third-party services specialising in outcomes collection. Choose a system that is user-friendly and secure.

- **Consent and Data Use:** Make sure patients are informed that their responses will be used as part of their care and quality monitoring. Filling these is voluntary (though highly encouraged). Data from PROMs might also feed into national audits or research, so governance approval might be needed if used beyond individual care. An advantage of digital PROMs is the ease of anonymising and aggregating data for audit – but still, treat any extracted dataset carefully as it may contain sensitive health information.

- **Implementation:** Hand surgery units implementing digital PROMs should address: accessibility (are all patients able to use it? If not, provide paper alternatives or phone follow-ups for those not online), timing (ensure PROM invitations aren't sent at inappropriate times, and that responses are actually reviewed by someone), and integration (ideally the PROM results should flow into the patient's record or at least be easily viewable by the clinical team). If a patient reports a worrying outcome (e.g. very high pain or disability score) post-surgery, there should be a mechanism to flag this for clinical review.

- **Data protection:** PROMs data is patient data. If using a third-party service, ensure there is a data processing agreement in place and that data is stored on secure servers (preferably UK or equivalently protected territory). The system should comply with NHS's data protection standards. Avoid free survey tools that are not health-specific, as they might not meet required security (for example, using an open Google Form for patients to input health info would not be appropriate without assurances on data security).

- **Utilisation:** Collecting PROMs is only worthwhile if the data is used. Periodically, the hand unit should analyse the PROMs to see how patients are doing and identify areas

for improvement. Also, discussing a patient's PROMs with them in clinic can be helpful (e.g. "I see your disability score has improved from 60 to 20 after surgery – that correlates with your subjective improvement").

Examples: A common PROM for hand surgery is the QuickDASH (Disabilities of the Arm, Shoulder, and Hand) questionnaire. A digital system can calculate the score automatically once the patient fills it, saving clinician time and reducing errors. Some units also use Patient Activation Measure (PAM) or satisfaction surveys delivered via email after clinic visits – to gauge patient experience digitally.

5.3 Digital Communication and Collaboration Tools

Communication technology is ubiquitous, but its use in clinical practice must be thoughtful:

- **Email:** Many patients and professionals communicate via email. Always use an NHS email account (nhs.net) or other secure, approved system for any identifiable patient information. NHSmail is encrypted to other NHSmail addresses. If emailing patients, one must consider encryption – NHS Digital guidance allows emailing patients on their personal email *with patient consent* and provided they are informed of risks (email isn't completely secure). A common approach: if a patient wants to receive info by email, have them sign a disclaimer or document that they understand the risk. Double-check the recipient's address before sending (wrong address errors are unfortunately common breaches).

- **Instant Messaging (IM):** Apps like WhatsApp or Signal have end-to-end encryption and are sometimes used by clinical teams for quick communication or sending images within a team. Officially, NHS guidance prefers the use of dedicated secure clinical messaging platforms (like Microsoft Teams on NHS accounts or others that log and secure data). If WhatsApp is used informally among a team, never send patient identifiers or full details – some trusts allow sending a photo of an X-ray within a closed clinical group chat if urgently needed for advice, but this should be anonymised (e.g. no name visible on X-ray, just the image) and deleted after use as even a unique x-ray can potentially be identifiable. No patient images or details should be stored long-term on personal messaging apps or personal devices. It is highly recommended to use Trust-approved messaging services to protect yourself, the patient, and to retain communications as part of the medical record.

- **EHR Messaging:** Many electronic health records offer internal messaging or tasking systems (e.g. messages to notify physio of a new referral, or to ask a colleague a question within the system). Use these for internal communication about patient

care instead of external apps. They keep a trail and are more secure within the firewall.

- **Teleconferences and MDTs:** Collaboration with colleagues is increasingly digital (e.g. MDT meetings on MS Teams, case discussions via teleconference). Ensure any patient data shared on screen (like showing imaging or documents) is treated confidentially – only authorised staff in the meeting, and no recording unless everyone agrees and it's for legitimate reasons. If using third-party conferencing, try to use NHS-procured solutions (which have appropriate data agreements). Avoid using personal video chat accounts for clinical discussions involving patient data.

- **Patient Communication:** Text messaging services (often automated from clinics) are used for appointment reminders or even initial triage (some practices allow patients to send in a picture via a secure link). These are acceptable as long as they are one-way or controlled via a secure system. Two-way patient texting for clinical advice is tricky – it can be convenient, but important details might be missed, and it's hard to document in the record. Many units instead use e-consultation platforms where the patient submits info or images via a web form which then goes into the clinical system.

- **Social Media:** As a rule, do not use social media (Facebook, Twitter, etc.) for any patient-specific communication. Some surgeons maintain professional social media accounts for education or public engagement, but patient queries should be redirected to official channels. Never share patient cases or images on social media without explicit consent and appropriate anonymisation, and even then, consider whether it's appropriate professionally.

- **Collaborating with External Providers:** If sending information to another hospital (e.g. referring a patient to a tertiary centre with their images and notes), use official channels like NHS e-Referral Service, secure email, or encrypted file transfer. Do not rely on patient-carried USB drives unless encrypted, as those can be lost or contain viruses. Many radiology departments can electronically transfer images via an Image Exchange Portal (IEP) – leverage those rather than giving a CD to the patient (which has patient data unencrypted).

- **Etiquette and Documentation:** Just because communication is digital doesn't mean it isn't clinical correspondence. Important decisions or consultations done via email or messaging should be documented in the patient's record. For instance, if a specialist gives advice over email about managing a tricky case, that email should be copied into a note in the EHR for completeness.

Clinical Example: A hand surgeon might take an intraoperative photo of an unusual finding (with patient consent) and later want to discuss it with a colleague at another hospital. The proper way: store the photo in the secure system, then use secure email to send it, or discuss via an online meeting where the image is shown. The improper way: sending it via a personal WhatsApp chat – which might be convenient but is not auditable and could be considered a breach – especially if the phone is lost or if the recipient's phone is compromised. One should use secure, confidential, and locally approved software for the transfer and storage of images.

5.4 Telemedicine and Remote Care

Telemedicine refers to clinical services provided remotely via technology – in hand surgery this commonly means video or phone consultations, virtual follow-up for postoperative checks, or remote therapy supervision. The COVID-19 pandemic accelerated adoption of telehealth in all specialties, including orthopaedics and plastic surgery. Guidance for telemedicine:

- **Patient Selection:** Not all hand surgery visits are suitable for telemedicine. New acute injuries may require in-person assessment (for physical exam). However, many follow-ups (reviewing wound healing, discussing scan results, checking on therapy progress) can be done by video or phone. Screening consultations can also be done remotely to decide if/when the patient needs to come in. Triage carefully: ensure that by doing a visit remotely you are not compromising the ability to detect something important. If unsure, err on the side of in-person.

- **Platform and Setup:** Use an approved video consultation platform (e.g. NHS Attend Anywhere / Near Me, MS Teams if set up for patients) that meets privacy standards. Both clinician and patient should be in a private environment. The clinician should use a headset or ensure no one else can overhear. Verify the patient's identity at the start (like asking them to confirm name, DOB, or use the EHR-integrated video invite that already confirms identity). Document that the consultation was via telemedicine and note who was present on both ends (if the patient had a family member with them, etc.).

- **Examination via Video:** While limited, some aspects of exam can be done: the patient can be asked to move their fingers or wrist in front of the camera to demonstrate range of motion, make a fist, do specific provocative tests (like Phalen's test for carpal tunnel by flexing wrists, or Froment's sign for ulnar nerve by pulling paper). The clinician can observe wounds or scars if the camera resolution allows – patients can be asked to position the camera or use a good light. For wounds, some patients send a photo ahead of time which might be higher resolution. Always consider: if the video quality is poor or you cannot adequately assess something (e.g.

skin temperature, precise tenderness), arrange a prompt in-person review. It's acceptable to do a hybrid model (video first, then bring in if needed).

- **Consent and Security:** At the start of a teleconsultation, confirm the patient is comfortable proceeding in this format and remind them it's a private medical consultation. They should not record it without permission (and likewise, the clinician should not record it unless there are a specific need and consent, or if hospital policy allows recording for clinical documentation – which is rare and must be transparent). If connection is lost, have a backup plan (like calling their phone to continue audio, or reschedule).

- **Tele-triage with images:** Some services have patients send photos of injuries (like lacerations) to decide if they need to come in. For instance, a patient with a fingertip injury might email a photo to the hand unit; a consultant can judge if it likely needs surgery or can be managed conservatively. This can be useful but ensure images are handled via secure methods (like a web portal or NHS mail, not the surgeon's personal email or number). If a patient sends a photo to a doctor's phone number (e.g. via WhatsApp), that photo becomes stored on the phone – which, unless managed, is a data protection concern. It's better to redirect patients to official submission channels. If none exist, one might view it and then immediately delete, but it is much better to avoid this situation and push for official solutions.

- **Home Monitoring:** In some cases, patients can use digital tools at home – e.g. a smart device that measures finger range of motion or grip strength and uploads data. These are emerging technologies that can feed into telemedicine but again one needs to ensure that they meet local and national guidelines.

- **NHS England Guidance:** The NHS has published best practice for virtual consultations, stressing equality (provide for those with disabilities or language barriers appropriately), effectiveness (ensuring similar outcomes to face-to-face for the scenario), and patient choice (patients should be able to opt for face-to-face if they prefer, within reason).

Practical Example: During the COVID-19 period, many hand clinics moved to telephone or video reviews for post-operative check-ups. A typical protocol: after a carpal tunnel release, instead of the patient coming at 2 weeks, the team phones the patient. They ask about wound condition, hand function, any issues; some patients send a photo of the scar to an email checked by the team. If all is well, they discharge the patient with advice. If there are concerns (e.g. signs of infection or persistent numbness), they arrange an in-person review. This kind of protocol can continue beyond the pandemic as it proved efficient for straightforward cases.

In summary, digital communication and telemedicine are powerful tools that, when used under proper governance, can enhance accessibility and efficiency of hand surgical care. Always balance convenience with confidentiality and clinical appropriateness. The goal is to maintain the same quality of care as in-person, while leveraging technology to reduce burden on patients and the system.

6. Artificial Intelligence in Hand Surgery

Artificial Intelligence (AI) in medicine refers to computer systems that perform tasks normally requiring human intelligence – such as visual perception (image recognition), decision-making, or language understanding. In hand surgery, AI is an emerging adjunct, used in areas like diagnostic imaging analysis, predictive analytics for outcomes, and even automated patient communication (e.g. chatbots answering common questions). This section outline types of AI, responsibilities of clinicians, risks, and governance for using AI in hand surgery.

6.1 Types and Applications of AI

AI is a broad field; relevant subtypes in healthcare include:

- **Machine Learning (ML):** Systems that learn patterns from data. Within ML, deep learning (using neural networks) has been particularly successful for image analysis. For example, a deep learning model might be trained on thousands of hand x-rays to identify fractures. A published study might show that an AI can detect a scaphoid fracture on an X-ray with high sensitivity, essentially acting as a diagnostic aid. Other ML models might predict the likelihood of a complication (like whether a patient will develop stiffness after a certain injury, based on big data of similar patients).

- **Computer Vision:** This refers to AI analysing images or videos. Applications in hand surgery include interpreting radiographs, CT or MRI scans; assessing range of motion from video (some prototypes can use a smartphone camera to measure how well a patient can bend their fingers); or identifying surgical landmarks in real-time (experimental systems that could guide a surgeon by recognising anatomy in the surgical field through an AR headset, for instance).

- **Natural Language Processing (NLP):** AI that understands and generates human language. In a hand surgery context, NLP might be used to scan clinic letters or op notes to identify cases meeting certain criteria (like for audit or research), or to help write discharge summaries from dictated notes. Another NLP example is an AI chatbot on a hospital website that can answer patient queries about carpal tunnel syndrome by drawing from a knowledge base.

- **Robotic Process Automation and Intelligent Systems:** Not AI in the cognitive sense, but some digital automation (like scheduling or inventory management for hand surgery equipment) can use simple AI rules. In the operating theatre, surgical robots (like the da Vinci system) aren't AI themselves, they are surgeon-controlled, but there is research on "smart" tool positioning and safety features that rely on AI.

- **Generative AI:** Tools like GPT-5 or image generators might be used to produce easy-to-understand patient education material (simplifying complex language) or even to create training images (though current AI image generators struggle with detailed hand anatomy). One might explore using such technology to draft patient leaflets which a human then edits. Caution is needed to verify accuracy, as these models can produce incorrect information confidently.

Current uses in hand surgery (in practice or research):

- **Diagnostic support:** AI algorithms to detect fractures on X-rays, identify bone tumours, or grade osteoarthritis severity. Some have shown promise with accuracy comparable to radiologists for certain tasks (like fracture detection). They can act as a "second reader" highlighting areas of interest on an image for the clinician to review, potentially reducing misses in busy settings.

- **Ambient note-taking and task completion:** AI tools that listen to interactions and conversations then complete clinical tasks – such as writing ward-round entries, clinic letters, and ordering investigations.

- **Outcome prediction:** ML models that predict outcomes such as which patients will benefit from surgery vs conservative management for conditions like base of thumb arthritis or predict who might have poor range of motion after flexor tendon repair based on patient factors and injury characteristics. These are experimental but could eventually assist in shared decision-making (e.g. an AI risk calculator for complications).

- **Operational efficiency:** AI is used in some hospitals to predict clinic no-show rates or optimise theatre scheduling by analysing past data. While not specific to hand surgery, these can indirectly improve a hand unit's functioning.

- **Rehabilitation:** AI-driven rehab devices (like smart gloves that measure motion and give feedback) use algorithms to tailor exercises to patients. There are also apps with AI chatbots that check in on patients' rehab progress and mental wellbeing, alerting clinicians if needed (for example, a patient reporting unmanageable pain via a chatbot could trigger an alert to the team).

It's important to stress that AI is not mainstream in everyday hand surgery yet – many tools are in research or pilot phases. But the field is moving quickly, and surgeons should be prepared for AI integration, staying informed about developments.

6.2 Responsibilities and Human Oversight

As highlighted under Core Principles, the introduction of AI does not diminish clinician responsibility. If an AI tool is used, clarity is needed on how decisions are made and by whom:

- **Clinical Decision-making:** Any AI used for diagnostic or treatment suggestions must be seen as an aide, not an oracle. The surgeon or treating clinician must verify AI outputs. For instance, if an AI flags an "abnormality" on an X-ray that you disagree with, you should trust your clinical training and investigate rather than automatically follow the AI. Conversely, if the AI misses something obvious to you, you document and proceed as normal. Never defer accountability to "the computer said so." UK law is currently undergoing reform for classifying medical software and decision-making tools as medical devices, but in the interim the law would still judge the human professional's actions, not the machine's, in the event of an error. Thus, always double-check critical findings.

- **Understanding the AI's Scope:** Know what the AI can and cannot do. If an AI is only validated for adult wrist fractures, do not apply it to paediatric cases or elbow images, for example. If it produces a confidence score, take that into account (an AI might say "90% confidence of fracture" vs "50%" – use high uncertainty outputs as a prompt for further examination or additional imaging, not as a clear answer).

- **Training and Skill:** Clinicians using AI should be trained in its use (which may require local or industry organised training sessions). This includes interpreting the interface (heatmaps, probability scores, etc.), and understanding basics of its algorithm (for example, knowing that it analyses only the image pixel data and doesn't incorporate clinical history unless explicitly designed to). If an AI gives an unexpected answer, consider factors like image quality (was the X-ray rotated, leading the AI astray?), or patient factors (is there hardware in the image the AI wasn't trained on?). Training should also cover recognising AI errors and bias.

- **Communication with Patients:** If an AI contributes to a clinical decision, should the patient be told? Ethically, transparency is encouraged. For instance, one might say, "We use a computer program that helps double-check the x-rays. It didn't show anything concerning, and I agree with that." Or if it did highlight something: "Our AI tool flagged a potential issue on your scan – I've looked at that area and here's what

we'll do…". Patients will vary in how much they want to know, but being open maintains trust.

- **Supervision and Override:** Healthcare organisations should have policies on AI overrides. If a junior clinician is using an AI tool, is a senior reviewing as well? (Analogy: a resident reads an X-ray with AI assistance, but a consultant radiologist still issues a final report). Currently, AI is usually a second reader, but if there's any move to automation (like AI pre-populating a report), a human must sign off. Also, if a clinician consistently finds the AI is making concerning errors, there must be a mechanism to report this and perhaps suspend use until resolved.

- **Ethical Practice:** Clinicians have a responsibility to ensure AI is used ethically – e.g. if an AI scheduling system suggests shorter follow-up for certain patients due to predicted outcomes, clinicians must ensure that doesn't inadvertently cause inequality or reduced care quality. Ethical use also means not blindly trusting AI tech without evidence – which ties into responsibilities around validating efficacy.

In summary, the clinician is the final common pathway for patient care. AI can augment your eyes (image analysis) or memory (data crunching) or process (automation), but it does not have compassion, holistic judgment, or accountability. The surgeon must maintain those elements. GMC's guidance on good medical practice (though not specific to AI) would likely consider uncritical reliance on an AI as a failure in duty if it harms a patient. By contrast, judicious use of AI with human oversight is just like using any other medical tool properly.

One way to ensure oversight is to integrate AI results into multidisciplinary discussions: for example, if an AI reads all postoperative X-rays for loss of reduction, any flags could be discussed in the next day trauma meeting rather than acted on by a single clinician alone. This way, multiple human eyes review the scenario.

6.3 Risks and Limitations of AI

While AI holds promise, there are significant risks and limitations that must be acknowledged:

- **Diagnostic Errors and Bias:** AI systems can make mistakes, sometimes inexplicably from a human perspective. They might misidentify normal variants as pathology or miss an abnormality due to subtle reasons (like an unusual presentation that wasn't in its training set). For example, an AI trained mostly on Caucasian patient images might be less accurate on patients with darker skin on photographs or different bone density on X-ray (if training data lacked diversity, an example of bias). Bias can also be along lines of sex, age, etc. It is crucial to validate AI tools on the local population

or broad datasets to uncover any bias. Using biased AI could perpetuate health inequalities by mis-serving certain groups.

- **Overreliance and Deskilling:** If clinicians become too reliant on AI, their own skills might atrophy. A hand surgeon who always trusts an AI to read radiographs might lose some acumen in spotting subtle injuries. If the AI fails or is withdrawn, the team could be left vulnerable. Moreover, resident doctors need to learn pattern recognition; if they're just seeing what the AI marks, they might not learn to systematically review images.

- **Technical Failures:** AI systems are software – they can crash, have downtime, or produce no result if something is formatted incorrectly. Imagine an AI integrated into PACS that one day goes down: workflow might be disrupted if radiologists or clinicians had come to depend on it for triage. Always have a backup plan (the traditional workflow should be ready to take over). Also, cybersecurity is a concern – an AI system could be hacked or manipulated (though theoretical in healthcare, one can imagine malicious tampering with outputs).

- **Interpretability ("Black Box" issue):** Many AI, especially deep learning, operate in a way that is not easily interpretable by humans. They might flag an image as abnormal but not clearly explain why. This is problematic for trust and for edge cases. There are methods (like heatmaps that highlight which part of an image influenced the decision) that improve transparency somewhat. But ultimately, if an AI says "this tendon repair will fail with 80% probability," we need to be cautious because we may not see the rationale. If the rationale was spurious (like it picked up some confounding correlation in data), following it blindly could be wrong. Transparency and explainability of AI decisions is an active area of development, and in regulated medical devices, manufacturers should provide at least some understandable info.

- **Data Requirements:** AI needs data to train on. Large, high-quality datasets in hand surgery (especially labelled data) may be limited. An AI model might be trained on one hospital's data and not generalise well to another (maybe due to different equipment, population, or protocols). If a hand unit wants to leverage AI, perhaps participating in data-sharing consortia or multi-centre studies is necessary to get robust AI. Beware of "data hunger": pushing lots of patient data into AI projects can conflict with data protection if done without proper anonymisation or approvals. Also, training an AI on data that has inherent biases or errors will yield an AI that perpetuates those.

- **Regulatory and Legal Risk:** If an AI device malfunctions or gives a harmful suggestion, there could be legal consequences. There is ambiguity over liability – does it fall on the clinician, the hospital, or the AI manufacturer? Right now, since clinician oversight is expected, it is likely the clinician/hospital carry responsibility.

To mitigate this, stick to AI that is properly approved (so it meets safety criteria), use it within its intended use, and document decision-making (if you diverge from AI advice for a sound reason, document that; if you follow AI advice on a borderline call, also document your rationale). Always retain the ability to explain why a decision was made without just saying "AI said so."

- **Patient Perception and Acceptance:** Some patients may be uncomfortable with the idea of AI in their care, worrying about being treated by a "robot" or not getting personal attention. Others might overestimate AI ("is the robot surgeon doing my operation?" – expecting perhaps unrealistic perfection). Managing expectations is part of risk management. Public trust can be fragile – a high-profile AI mistake could cause backlash. Thus, any rollout of AI should include patient engagement and transparency to maintain confidence.

- **Impact on Workflow:** Introducing AI can inadvertently increase workload or cause new inefficiencies if not integrated well. For instance, if an AI flags lots of false positives on X-rays, radiologists or surgeons might spend extra time chasing those. Or if an AI requires manual data input in a specific way, it could add to clerical burden. Thus, evaluate whether the AI truly streamlines things or not. Ideally, do a pilot study and measure outcomes (time saved, accuracy improved, etc.).

- **Ethical concerns:** AI could be used unethically, such as by predicting things like "risk of non-compliance" or other sensitive traits that could prejudice care. Or using AI to analyse patient's facial expressions or tone for pain assessment – some may find this intrusive. Another scenario: insurance or systems might misuse AI predictions to limit care (e.g. denying a surgery because an algorithm predicts a poor outcome – this would be ethically problematic if done without clinician and patient input). The hand surgery community should advocate for AI to enhance, not ration, quality care.

In summary, AI is not infallible. It brings new types of error modes – systematic, sometimes not obvious – unlike human error which is often random or due to fatigue. We must remain vigilant, continuously monitor AI performance in our context, and be ready to intervene when it errs. Recognising these limitations is key to safe AI adoption.

6.4 Governance of AI Systems

Given the potentials and pitfalls of AI, robust governance is essential. Governance ensures that AI tools are introduced safely, used appropriately, and monitored continually. Here are governance considerations for AI in hand surgery:

- **Approvals and Oversight Committees:** Before an AI tool is deployed in a clinical setting, it should be vetted by appropriate bodies. Many institutions have a digital or

AI governance board (sometimes part of the IT or clinical governance structure). As per NHS guidance, involve your Data Protection Officer, Caldicott Guardian, and clinical safety officers in decisions to implement AI. They will ensure data privacy compliance (DPIA done, patient info handled lawfully) and that safety standards are met. If the AI is considered a medical device (most diagnostic/support ones are), confirm that the MHRA registration or exemption is in order. The board might also look at ethical aspects and alignment with the hospital's strategy.

- **Pilot Testing and Validation:** Do not simply install an AI and deploy it broadly without local validation. A governance plan should include an initial pilot phase where the AI runs in parallel with usual care to gauge performance. For example, you might run an AI on all hand X-rays for a month but not show the results to clinicians initially, then compare how it did versus the radiologist reports, to ensure it is accurate and maybe calibrate its thresholds. Alternatively, show it to clinicians but don't act on it, just collect feedback. Define success criteria (e.g. does it improve detection rate of certain injuries without too many false alarms? Does it save clinician time?). Proceed to full implementation only if it proves beneficial and safe.

- **Training and Competency:** Governance includes making sure users are trained. This might involve formal training sessions, and maybe a competency checklist. The hospital might restrict use to those who have completed training. For instance, radiographers might need to know how an AI triages images so they can manage workflow accordingly.

- **Monitoring and Audit:** Once live, AI tools require ongoing monitoring. Assign responsibility for this – e.g. a consultant lead for AI in the orthopaedic department, who will review the AI's outputs at set intervals. Key metrics might include: sensitivity/specificity over time (is performance drifting?), any adverse events or near-misses involving the AI, user feedback (are clinicians actually finding it helpful?), and usage stats (how often is it used or ignored). Periodic audit is crucial. If an audit finds that the AI missed several cases that humans caught (or vice versa), adjustments or retraining might be needed. It might also reveal need for more training or that the threshold for alerts should be changed.

- **Incident Reporting:** Incorporate AI into the clinical incident reporting system. If a case is misdiagnosed or delayed and the AI was involved, log it as such. Also encourage staff to report if they notice the AI doing something odd or making a likely mistake (without harm). This will help accumulate data on its reliability. The MHRA's Yellow Card scheme can be used to report device software issues at a national level, which is important for regulatory oversight and improvement.

- **Updates and Change Control:** AI software may update or "learn" over time (if adaptive). Governance must manage changes carefully. If the vendor issues a new version, treat it like a new device – consider validating major changes, and certainly ensure they inform you of what changed. If the AI is adaptive (learns from new data continuously), one must have triggers to decide when it has changed enough to warrant re-approval (ongoing performance within expected range can be one measure). The MHRA is working on frameworks for adaptive AI significant change determinations. Locally, one may choose to lock the AI model from continuous self-update to avoid unmonitored drift.

- **Interdisciplinary Approach:** Governance should include various stakeholders: hand surgeons, radiologists, IT specialists, data scientists if available, nurses/therapists if they will interact with it, patient representatives (for perspective), and legal/IG advisors. This ensures all viewpoints are considered (clinical relevance, technical feasibility, ethical implications, patient acceptability).

- **Documentation and Protocols:** Develop protocols for how to use the AI. For example, if an AI flags a critical finding (e.g. "possible tendon rupture on ultrasound"), specify that a human must verify it within X hours. If an AI's suggestion contradicts a human's, perhaps protocol could suggest seeking a second human opinion to resolve (to avoid either blindly following AI or dismissing a correct AI alert due to bias). The protocols should also cover downtime (what to do if AI system is unavailable – usually revert to standard care).

- **Integration:** Aim to integrate AI into existing workflows seamlessly. A poorly integrated tool might be ignored. For example, if an AI for X-ray reading is not integrated into PACS but requires uploading images separately to a software, clinicians might not bother due to inconvenience. So involve IT to integrate outputs into PACS or EHR (like an AI result appears as an annotation or separate tag in PACS). Integration reduces risk of error (like looking at the wrong image) and makes it more likely to be used consistently.

- **Compliance with Standards:** Keep an eye on emerging standards and guidelines. For instance, NICE may develop specific evidence standards for AI (NICE has an evidence standards framework for digital health tech). Compliance with these can give confidence. If the AI is doing diagnostic tasks akin to a lab test, it should meet similar validation standards as lab diagnostics.

- **Contract and Liability Clarity:** As part of governance, if using third-party AI, have clear agreements about support, maintenance, and liability. While a contract won't override clinician's duty to patients, it can ensure the vendor provides prompt fixes if

issues arise and clarifies what happens if the AI fails. The trust should also inform its indemnity insurer or relevant body about AI usage as part of risk management.

A well-governed AI implementation in hand surgery can enhance care while minimising risks. It should be a continuous loop: **Plan -> Pilot -> Implement -> Monitor -> Review -> Refine**. This aligns with the standard clinical governance cycle. With these measures, hand surgery units can responsibly innovate with AI and digital tools, leading the way in improving outcomes and efficiency while upholding the trust and safety of our patients.

7. Practical Guidance for Clinicians

This section distils the above into concrete, day-to-day guidance and examples for hand surgeons and teams incorporating imaging, digital tools, and AI. It serves as a quick-reference set of do's and don'ts, ensuring safe and effective practice:

- **Obtain Proper Consent for Imaging and Photography:** Always explain to patients when taking clinical photographs or videos for their record or for treatment planning. Use your hospital's consent forms for medical photography. If images may be used beyond the record (teaching, publication), secure specific written consent. Remind patients that these images become part of their confidential record and are protected.

- **Protect Patient Identifiers on Images:** When sharing images for consults or in presentations, remove identifying details (names, hospital numbers) unless absolutely necessary. For example, if emailing an X-ray to a colleague for advice, crop out the name or use an anonymised copy. This reduces risk if it's intercepted or seen by unauthorised persons.

- **Use Secure Channels for Communication:** Do not send patient information or images via unsecured methods (e.g. standard email to a Gmail address, or messaging apps). Instead, use NHSmail, secure messaging apps endorsed by your organisation, or formal referrals systems. If a patient or GP emails you directly, consider moving the conversation to a phone call or a reply via a secure method rather than continuing over personal email.

- **Manage Digital Images Responsibly:** If you capture images (say of a wound in clinic on a tablet or camera), upload them to the EHR/PACS as soon as possible and then delete them from the device. Ensure devices used for this purpose are encrypted and access-controlled. Never keep a stash of patient photos on personal devices – this has led to serious breaches and GMC investigations in the past.

- **Follow "Clean Desk" and "Lock Screen" Practices:** When working on digital records or viewing imaging, be mindful of who can see your screen. Don't leave patient data visible if you step away – lock your computer. This prevents accidental disclosures to patients or visitors passing by.

- **Double-Check Before Sharing/Posting:** It may seem obvious, but many incidents occur when an email or letter goes to the wrong person due to an autocomplete error or similar. Before sending any patient-related information, verify the recipient. When posting imaging on teaching forums or social media (if allowed with consent), triple-check that no identifiers are present and that you have the necessary permissions. A good practice is to have a colleague verify de-identification.

- **Verify Identity in Virtual Encounters:** In telemedicine sessions, confirm you are speaking to the correct patient (ask for two identifiers like name and DOB). Likewise, if discussing a case with a colleague via phone/email, ensure you both refer to the right patient (use at least two identifiers in correspondence, e.g. "John D., DOB 3/4/1980, hospital number 12345"). This avoids mix-ups.

- **Use AI as an Aid, Not Autopilot:** If an AI tool is available (e.g. for x-ray interpretation), use it to complement your assessment. Always perform your own evaluation first, then see what the AI suggests. If there's disagreement, investigate further or get a second human opinion. Do not rely on AI for final decisions, especially life/limb-altering ones, without human confirmation.

- **Stay Skeptical of AI Outputs:** Treat AI findings or predictions as you would a lab result – consider the context. If an AI flags something surprising, question it just as you would an out-of-character lab value (you might re-run a lab test; similarly, perhaps have the image re-reviewed by someone else or cross-check with another modality). And if an AI fails to flag an obvious issue you see, note that discrepancy and ensure the issue is addressed (and possibly feed that info back to the AI team for system improvement).

- **Maintain Your Skills:** Continue practicing your diagnostic skills in reading images and making clinical judgments. Use technology to enhance, not replace, your expertise. For trainees: don't skip doing your own image reports or assessments because "the computer will catch it." Your training should include learning to interpret outputs critically and understanding false negatives/positives.

- **Perform Regular Audits:** Incorporate digital tools into your audit cycle. For example, audit compliance with imaging protocols (e.g. was an MRI done per scaphoid protocol in all applicable cases?), or audit whether patient communication guidelines are followed (e.g. staff using approved channels of communication). If

using AI, audit its performance and impact (did it shorten time to diagnosis, or reduce missed injuries?). Use audit results to refine processes and provide feedback/training to staff.

- **Keep Software and Systems Updated:** Ensure that you are using the latest approved versions of software as updates often patch security issues or improve functionality. However, follow your IT department's lead – don't install unapproved updates or software on work systems as that could introduce vulnerabilities.

- **Respect Copyright and IP Rules:** Do not use images from textbooks or online sources in your patient care or presentations without permission if they are not public domain. Conversely, remember you cannot give patients full ownership of clinical images – but you can give them copies. If a patient wants to take a photo of their X-ray on the screen, technically the Trust owns it, but most wouldn't object for personal use. However, caution them about posting it publicly (others might identify them or misinterpret it).

- **Plan for Downtime:** Consider how you'd manage if a digital system fails. For example, if PACS is down, do you know how to request urgent films be printed or viewable via contingency? If the EHR is down, are there paper note procedures? If your outcomes collection app fails, have a backup way to get critical info from patients. Being caught off guard in downtime can harm patient care, so familiarise yourself with your organisation's downtime protocols.

- **Engage Patients in Digital Transitions:** When introducing telemedicine or electronic PROMs, explain the why and how to patients. Provide clear instructions (like how to log into a video visit, or how to complete an online questionnaire). Solicit their feedback – if many patients find a tool difficult, that's important to know and address (maybe by offering training or refining the tool).

- **Ensure Confidentiality in Tele-settings:** For video consults, advise patients to be in a private area. If a family member is present, have the patient confirm they're okay with them hearing. Likewise, on your end, use a private room or headset. Document those present. And never record the session without consent. If you need photos (say the patient shows their wound on camera), ask them to send a photo via the secure method. Screenshots on your device should be avoided unless absolutely necessary and then treated like any other patient photo (transferred to record, then deleted).

- **Follow MHRA Guidance for Device Issues:** If you suspect a software tool contributed to an error or posed a safety risk, use official channels to report it (internally and to MHRA via the Yellow Card for devices). Similarly, if you encounter any malfunction of imaging equipment or software, report to your medical

physics/clinical engineering and through clinical incident systems. This triggers investigations that protect future patients.

- **Stay Informed on Legal Changes:** Laws and regulations in digital health evolve. For instance, data protection laws may be updated (as happened with GDPR), or new medical device regulations may come post-Brexit. Keep an eye on communications from your Trust, BSSH, GMC, and regulators about changes affecting digital practice. If, say, a new statutory requirement for AI transparency arises or a new ICO code of practice on AI is released, ensure your practice aligns. When in doubt, consult your DPO or medicolegal advisor.

- **Consult Early with Experts:** If planning a project involving patient data (like a research project using machine learning on patient images), consult with IG and R&D offices early. For example, using patient X-rays to develop an AI will likely require not just research ethics approval, but also careful anonymisation and perhaps Section 251 approval if identifiable data leaves the organisation. Getting these steps right from the start will save time and prevent compliance issues.

- **Use Digital Tools to Enhance Patient Education:** Embrace safe digital methods for improving patient understanding. For instance, use approved apps or videos to show hand therapy exercises on a patient's own phone (if your hospital has a library of verified content), or direct them to trustworthy websites (like BSSH patient information pages). Digital does not only mean risk; it offers great opportunities to educate and engage patients beyond the clinic walls.

Example Application: A resident doctor in clinic sees a patient who is 6 weeks post distal radius fracture fixation. The clinic uses digital X-rays on PACS. The doctor reviews the latest X-ray: as per training, they check alignment and healing. An AI overlay on PACS suggests "possible screw protrusion in joint." The doctor doesn't immediately alarm the patient; first they carefully re-examine the images, including different planes, and indeed see a hint that one screw might be long. They call in a senior who confirms it's subtle but possibly intra-articular. Because of that, they schedule the patient for an earlier follow-up and CT scan to verify screw position. They explain to the patient that the X-ray looks generally good but they want to double-check one detail with a CT. They do not mention AI to avoid confusion, but internally they acknowledge the AI prompt may have caught something. They document the finding and plan. Separately, they inform the department's clinical lead about this near-miss that AI helped catch – so it can be included in audit data, showing value added. This scenario highlights: using AI with human oversight, disclosing appropriately to patient (but focusing on the plan rather than technology), documenting, and learning from it.

By following such practical measures, clinicians can confidently integrate modern imaging, digital workflows, and AI tools into their hand surgery practice, while maintaining the gold standards of patient care, safety, and confidentiality.

8. Governance and Audit

Effective governance and regular audit are the backbones of implementing imaging, digital, and AI innovations in a safe, sustainable manner. Hand surgery units should embed these technologies into their clinical governance framework to continuously monitor compliance, performance, and patient outcomes. This section outlines the governance structures and audit processes recommended:

8.1 Governance Structures and Roles

- **Clinical Governance Group:** The department or hospital should have a committee that oversees clinical governance related to digital health. This might be a subcommittee of the Surgical Directorate or a multidisciplinary Digital Health Board. Ensure hand surgery representation on relevant committees (since imaging/IT decisions for the hospital will affect you).
- **Named Leadership Roles.** Assign champions or leads for key areas:
    - *Imaging Lead:* A consultant who liaises with radiology, ensuring imaging protocols (like the scaphoid pathway) are followed and updated in light of evidence. They might also oversee radiation protection matters and reporting discrepancies review.
    - *Digital/EHR Lead:* Someone in the hand team who is the point of contact for EHR improvements, templates for hand clinic notes or operation notes, and who monitors that digital workflow issues (like referral systems or outcome forms) are working.
    - *AI Lead:* If AI projects are underway, a clinician (with interest/knowledge in AI) should be designated to supervise these. They coordinate with the hospital's AI governance (including DPO and Caldicott Guardian), ensure DPIAs are done, present updates on AI performance, etc.
    - *Audit Lead:* Overlaps with normal practice, but ensure audits cover these topics, not just traditional clinical metrics.
- **Interdepartmental Collaboration:** Hand surgery governance of imaging and AI inherently involves radiology, IT, therapy, etc. Maintain strong communication channels with those departments. For example, a quarterly meeting between the

Hand Unit and Radiology could review: imaging turnaround times, any incident (like an MRI missed a tendon tear that surgery later found), protocol changes, and new tech proposals. Similarly, link with the hospital's information governance and IT security teams regularly to address any new risks or requirements (like updated encryption protocols or new policies from NHS England).

- **Policies and Protocols.** Develop clear local policies that reflect this guidance:
    - **Medical Imaging Policy** that, for instance, references that all hand traumas should get standard views and how urgent scans are requested.
    - **Clinical Photography Policy** (often trust-wide) which covers consent levels and copyright ownership – ensure staff are aware of it.
    - **Electronic Communication Policy** that says what is acceptable (like use of NHSmail, prohibition of patient info on WhatsApp except in exceptional circumstance with immediate transfer to record).
    - **AI Use Policy** if applicable – possibly referencing that any AI must be approved by appropriate committees, staff must be trained, patients informed as appropriate, and a procedure for withdrawing AI if issues arise.
    - **Data Breach Response Plan:** All staff should know or have quick access to steps to take if, say, a device with patient images is lost or an email is sent in error. Reporting to the IG team quickly can mitigate damage and is a professional obligation.
- **Regulatory Compliance Monitoring:** The department should ensure that it meets external requirements:
    - **CQC (Care Quality Commission) expectations:** They will look at how you use tech in providing effective, safe care. They may ask about data security and patient consent for telemedicine, etc., during inspections.
    - **MHRA Compliance:** If any in-house development is done (like 3D printing guides or an algorithm used in practice), check if you operate under Health Institution Exemption or need MHRA registration.
    - **ICO and Data Protection:** The organisation's DPO might do spot checks or require quarterly reports on info governance training completion, etc. Engage positively with these; ensure 100% of your team have up-to-date data security training, for example.

- **NHS Digital/NHS England audits:** If participating in national digital projects or using central systems (like NHS e-Referral or summary care records access), comply with any monitoring or audits they do.

- **Risk Register:** Include risks related to imaging and IT on your departmental risk register. E.g. risk of PACS downtime affecting patient care, risk of data breach via unauthorised photo, risk of AI missing a critical diagnosis. Having them on the register means you acknowledge and actively manage them, with mitigation plans (like training, backup systems, etc.). Review these periodically to see if risk level has changed.

8.2 Audit and Quality Improvement

Regular audits should be conducted to ensure adherence to this guidance and identify areas for improvement. Some suggested audit topics:

- **Compliance Audits:**
  - **GDPR/Data Handling:** Audit if clinical photographs in last 6 months all have documented consent forms. Check if any staff are storing images on personal devices.
  - **Email Use:** Audit clinic correspondence – were any emails sent to patients? If yes, were they documented and done via nhs.net?
  - **Imaging Protocol Adherence:** Audit a cohort of hand trauma patients to see if correct imaging was done (e.g. all scaphoid fracture suspects got MRI by 2 weeks if this local protocol – measure against standards BSSH guidelines).
  - **Report Discrepancies:** Work with radiology to audit discrepancies in imaging interpretation (e.g. compare surgeon's initial read vs final radiologist report for 100 cases; categorise discrepancies by critical, minor, etc., and see if there's a pattern needing addressing via training or system change).
  - **Telemedicine Outcomes:** Audit if telemedicine follow-ups had similar outcomes (e.g. complication identification, patient satisfaction) as in-person. If there were cases that had to be brought in after a tele consult due to missed findings, analyse those.
- **Outcome Audits:**
  - **PROMs Data:** Use the digitally collected PROMs to audit surgical outcomes (e.g. average DASH improvement after trapeziectomy, or re-operation rates in

trigger finger). Also audit what percentage of patients are returning PROMs via the system (if low, that's a process issue to fix).

- **AI Performance:** If an AI tool is in use, audit its sensitivity and specificity in actual practice. For instance, if AI is reading all wrist x-rays, gather cases where AI said "fracture" and see if there truly was a fracture (positive predictive value) and conversely if any fractures were not flagged (false negatives). Also gather clinician feedback – maybe through a survey – to gauge if it's helping or causing alert fatigue.

- **Clinical Effectiveness Audits:**
  - **Time to Be Seen:** Audit time from referral to surgery for common conditions with vs without telemedicine triage.
  - **Detection Effectiveness:** Audit if digital or AI tools improved detection of clinical outcomes such as infection.
- **Governance Audits:** For example, audit documentation: did notes reflect that patient consented to video consult and others present (a quality criterion)? Did operation notes in the EHR have required minimum content as recommended by the Royal College of Surgeons?

8.3 Continuous Improvement and Learning

Governance is not just policing compliance; it's about learning and improving:

- **Morbidity & Mortality (M&M) and Case Conferences:** Include cases where digital issues played a role, not just surgical technique issues. For instance, discuss a case where an x-ray was misinterpreted leading to delayed treatment – focus on system learnings (do we need better training? was PACS image quality an issue? should that have been MRI earlier?). Or if a breach happened, discuss generically at M&M to reinforce lessons (without patient identifiers in that forum likely).
- **Training and Refreshers:** Based on audits or incidents, provide refresher training. If an audit finds many staff unaware of the trust's photo policy, do a short teaching at a departmental meeting. If telemedicine was found to miss some hand exam elements, maybe create a checklist for teleconsults to remind clinicians to ask certain things or have patient demonstrate certain movements.
- **Patient Feedback:** Solicit patient input on digital initiatives. Governance should incorporate patient satisfaction surveys especially for new modes like telehealth or e-consent processes. If patients report issues (like difficulty logging in to video calls

or concern over privacy), then address them (e.g. provide a simple how-to leaflet, provide longer initial consultations, or video help).

- **Sharing Best Practices:** If your hand unit develops a successful protocol or tool (for example, an AI tool that helped detect problems with rehabilitation early), share it through BSSH or publications. Likewise, learn from others – keep an eye on BSSH, BOA, and journals for innovations and incorporate those that fit your context. The BSSH might in future have official guidelines or accreditation for centres using advanced digital care – staying involved in the professional community ensures you won't be left behind or out of compliance.

- **Legal Updates Watch:** As mentioned, ensure the governance lead or IG lead disseminates any new laws or guidance. For instance, if the government updates the Data Protection Act or introduces an AI regulation, the governance group should adapt local policies accordingly. Keeping policies up-to-date (with version control and review dates) is part of good governance.

- **Risk Mitigation Drills:** Occasionally simulate scenarios: e.g. a PACS outage drill – does the team know how to request urgent films or use plain film if needed? Or simulate a data breach scenario to test response (some trusts do "IT/fire drills" for cybersecurity). These can identify weaknesses in readiness.

Effective governance is an ongoing process. It ensures that the use of imaging, digital tools, and AI in hand surgery not only complies with legal and ethical standards but also truly serves to improve patient care. With strong governance, the hand surgery service can confidently innovate and adapt to technological advances, knowing there is a safety net of oversight and quality control. As a result, patients benefit from both cutting-edge care and the assurance that their rights and safety are safeguarded.