Austria

Dr. Daniel Larcher

Dr. Mariella Rieder

ATLAS Attorneys at Law
Prewave GmbH

1 Digital Health

1.1 What is the general definition of "digital health" in your jurisdiction?

In Austria, there is no standalone legal or industry definition of "Digital Health" (DH) or "eHealth".

DH refers to the use of information and communication technologies, software, and data to prevent, diagnose, treat, and monitor disease, and to support health system management, including big data and AI. The term "eHealth" traditionally focuses on telematics and infrastructure.

As of 2026, the DH landscape is primarily shaped by the eHealth Strategy 2024–2030 and the planned integration of the European Health Data Space (EHDS). The eHealth Strategy Austria and the Digital Austria Act embed DH in the broader digital transformation of healthcare, covering electronic health records (ELGA), telemedicine, and DH applications.

1.2 What are the key emerging digital health subsectors in your jurisdiction?

- Telemedicine and remote care (virtual consultations, telemonitoring and home monitoring).
- Electronic health records, eHealth infrastructure (ELGA, e-medication, electronic vaccination record) and applications for disease management.
- AI-supported diagnostics and clinical decision support (e.g. imaging, triage).
- Consumer health apps and wearables (health data collection, mental health and lifestyle).
- Health data platforms and analytics.
- Cybersecurity in healthcare.

1.3 What is the digital health market size for your jurisdiction?

The Austrian DH market has been growing steadily, with momentum boosted by post-COVID-19 infrastructure investments. Excluding digital fitness and well-being (around 55% of the broader DH market), it was estimated at about US$600 million in 2024 and roughly US$720 million in 2025.

Based on sector growth expectations (STATISTA) and European trends (where DH markets often grow at 18–22% annually), Austria's DH market could reach approximately US$790–860 million in 2026 if it grows at a conservative 15% per year from the 2024 base. These figures are indicative only and will depend on implementation success and the wider economic environment.

Public-sector DH initiatives (such as ELGA) are substantial in Austria but are often not fully reflected in commercial market estimates. Overall, the market is expected to continue expanding at double-digit annual rates (roughly 10–20% per year) at least through 2029, supported in particular by Austria's eHealth Strategy 2024–2030.

1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

No authoritative public ranking by revenue exists. Many market participants are subsidiaries of international groups (such as GE, Siemens, T-Systems, Oracle Cerner, Phillips) or privately held startups without published financials, and most do not disclose "digital health" revenue as a separate segment. In addition, a substantial part of the DH landscape is organised and funded by the Austrian state (e.g. ELGA and other e-health infrastructures).

1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Official revenue growth rankings are not published for Austria. However, market observers point to fast-growing DH players in areas such as telemedicine, AI-based diagnostics, and remote monitoring, often including venture-backed startups and scale-ups that have recently raised significant funding.

2 Regulatory

2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

Generally, DH is subject to several regulatory regimes and therefore monitored by various authorities/agencies/entities:

- Federal Ministry of Social Affairs, Health, Care and Consumer Protection (BMSGPK).
- Federal Office for Safety in Health Care (BASG).
- Austrian Agency for Health and Food Safety (AGES).
- Austrian Umbrella Organisation of Social Insurance.
- Ethics committees.
- ELGA GmbH.
- Data Protection Authority (*Datenschutzbehörde* – DSB).

- Austrian Competition Authority (*Bundeswettbewerbsbehörde* – BWB).
- RTR/AI Service Desk.

2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?

The main legal regimes touching DH include:
- Medical Devices (MDs): EU Regulations (MDs and *in vitro* diagnostics (IVDs)), and Austrian Medical Devices Act 2021 and adopted ordinances, industry codes.
- Data Protection and Health Telematics: GDPR, Austrian Data Protection Act, Austrian Health Telematics Act 2012, Telecommunications Act 2021.
- EU AI Act.
- Austrian Physicians Act (ÄrzteG).
- Product Liability and Safety laws.

Miscellaneous laws include drugs and hospitals regimes, trade licence law (e.g. for regulated MDs), advertising rules, reimbursement and social insurance law and cybersecurity/ICT security laws.

2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?

(i) Key areas of enforcement:
- Classification of software under EU Medical Device Regulation (MDR)/*In Vitro* Diagnostics Regulation (IVDR) (Software as a Medical Device (SaMD), apps).
- Vigilance and reporting of "serious incidents" for medical software.
- Compliance with clinical evaluation and post-market surveillance requirements.
- GDPR enforcement concerning sensitive health data and secondary data use.
- Cybersecurity and data breach notification.
- Advertising and claims substantiation.

(ii) Emerging areas of enforcement:
- EU AI Act enforcement: AI transparency, bias mitigation, and explainability in clinical decision-support tools.
- Mandatory use of EUDAMED.
- NIS2 cybersecurity compliance for hospital/healthcare organisations (HCOs).
- Secondary use of health data for research and AI training.
- Cross-border DH services and telemedicine platforms.
- Interoperability and data governance obligations under EU health data initiatives.

2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?

Generally, software qualifying as SaMD is regulated under:
- MDR or IVDR.
- Austrian MD law (acts and ordinances).
- GDPR, Data Protection Act and Health Telematics Act (personal health data processing).

Competent authorities:
- BMSGPK/BASG/AGES (enforcing bodies).
- Notified bodies (conformity assessment for higher-risk software Class IIa, IIb, III).
- DSB.

2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?

AI/ML-based digital solutions are generally treated as MD or IVD when they have a medical purpose. AI/ML-powered DH solutions are primarily regulated through:
- EU MDR/IVDR (medical safety and performance if the AI software has a medical purpose).
- EU AI Act classifying most medical AI systems as high-risk AI (data governance, transparency, human oversight).
- GDPR particularly automated decision-making and processing of health data.

Authorities:
- BASG/AGES – MD oversight.
- DSB – data protection and algorithmic processing.
- Future designated AI Act national supervisory authorities (AI Office).

2.6 How, if at all, are these authorities evolving, or planning to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?

Austrian regulators appear to be gradually transitioning from a one-time approval model to a lifecycle management approach, with increased emphasis on post-market surveillance and lifecycle governance requirements (including change management, logging, and human oversight). In practice, many AI systems are currently approved in a relatively "locked" form, with updates treated as regulated modifications rather than as unconstrained continuous learning in the field.

2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?

Clinical validation data is central (make-or-break) to regulatory approval and enforcement under the MDR (Annex 14) and AI Act: Developers must demonstrate safety, clinical benefit, and performance/analytical validity relative to intended use. For AI systems, regulators increasingly expect:
- Training datasets are representative with population and bias-aware datasets (no algorithmic bias).
- Real-world performance evidence.
- Continuous validation through post-market clinical follow-up.

Under the AI Act, high-risk AI systems will also require robust validation datasets and documented risk mitigation measures. Insufficient or poorly designed validation data can lead to refusal or restriction of market access.

2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Austria operates under a centralised model that regulates DH primarily at the federal level. As a result, DH products are not subject to materially different regulatory approval regimes across the regions (*Länder*). The regional level is mainly responsible for ethics committees, healthcare service delivery, public procurement, and the administration of public hospitals.

2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?

Overall, while robust mechanisms exist (such as fines, reimbursement exclusions, system audits), DH enforcement in Austria is integrated into existing legal regimes without unique tailoring for DH. Austria has not recorded high-profile enforcement actions (fines, recalls etc.) in the DH sector.

3 Digital Health Technologies

3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?

- **Telemedicine/Virtual Care**
  Medical advice: Medical advice and treatment may only be provided by licensed physicians (Sec. 3 ÄrzteG); in teleconsultations, the physician must decide case-by-case whether remote care is sufficient or whether a physical examination is required, and must refer the patient to in-person care if the information basis is insufficient.
  Teleradiology: Specific constraints exist for teleradiology (e.g. permitted in basic/special trauma care, dispersed outpatient facilities, and for maintaining night/weekend/holiday operations for urgent cases).
  Infrastructure: As of 2026, all private physicians are legally required to use ELGA, the e-card infrastructure, and the e-vaccination pass.
  Telematics and data transfer: Strict conditions for electronic transmissions of health and genetic data (e.g. GDPR; strong authentication of patients and providers; role-based access; confidentiality and integrity; state-of-the-art encryption and secure implementation).
- **Robotics**
  MD qualification: Robotic systems used for diagnosis, therapy or other medical purposes (e.g. surgical robots) qualify as MD and must undergo appropriate risk classification, conformity assessment and CE-marking.
  Medical advice: In case of robotic assistance in diagnosis or treatment, medical advice and final clinical decisions remain the responsibility of physicians and require supervision.
  Safety and cybersecurity: Manufacturers must address mechanical and software safety, cybersecurity, human-machine interface risks and post-market surveillance.
  Liability: Product liability applies to software and AI components, making manufacturers liable for defects.
  EUDAMED: As of May 28, 2026, robotics manufacturers must have their systems registered in the mandatory EUDAMED modules (Actor, UDI, and Certificates).
- **Wearables**
  Wearables marketed purely for wellness or lifestyle (e.g. step counters) are usually not MDs, unless the device is intended by the manufacturer for one or more medical purposes (monitoring vital parameters for diagnosis, therapy or risk stratification).
  Data Protection laws: Collection and processing of personal health data requires compliance with data protection laws.
  Interoperability/telematics: If integrated into Austrian e-health infrastructures or provider systems, health telematic laws and ELGA-related rules on secure health data exchange and access control become relevant.
- **Virtual Assistants (e.g. Alexa)**
  MD qualification: Virtual assistants are not MDs; however, if natural language processing or dialogue functions are specifically intended to be used for one or more medical purposes (e.g. symptom assessment leading to diagnostic output), MD laws apply.
  Medical advice: Reserved to physicians, consumer-directed virtual assistants must not be positioned as autonomously diagnosing or treating patients.
  Transparency rules: AI-generated content must be clearly identifiable.
  Data and e-privacy: The processing of personal or health data requires compliance with rules for health data, data minimisation, and security requirements.
- **Mobile Apps**
  MD qualification: Wellness-related apps are not MDs, but apps that perform diagnosis, recommend treatment, or control/monitor physiological processes for a medical purpose typically constitute MDs (Class IIa and higher) and must comply with risk classification, clinical evaluation, CE-marking and post-market surveillance.
  Consumer and advertising law: Misleading health claims can trigger unfair-competition and advertising-law issues.
  "App on Prescription": By late 2026, apps that prove positive care effects (medical benefit or structural improvement) can be prescribed and be reimbursed.
  App-specific data risks: Health apps process sensitive data; healthcare professionals (HCPs) or ELGA participants must observe health telematic laws on secure exchange.
- **Software as a Medical Device**
  MD classification and conformity: Software intended for diagnosis, prevention, monitoring, treatment or alleviation of disease is a MD (MDR Annex VIII notably Rule 11); diagnostic or therapeutic software will be class IIa or higher, requiring notified-body involvement.
  Clinical evaluation and lifecycle: SaMD requires appropriate clinical evaluation (including literature, clinical investigations or real-world data), risk management, usability engineering, cybersecurity and continuous post-market surveillance; significant updates may constitute substantial changes requiring reassessment.
  AI: Most SaMD falls into the High-Risk category of the AI Act requiring a quality management system that specifically includes data governance to prevent algorithmic bias.
  Data protection and telematics: Where SaMD processes personal health data.
  EU Product Liability Directive 2026 expands to standalone software.

- **Clinical Decision Support Software**
  MD qualification: CDSS that provides patient-specific assessments, diagnoses or treatment recommendations typically qualifies as SaMD; risk class depends on how directly it drives decisions with corresponding clinical evidence and notified-body requirements.
  Automated decision-making: When CDSS uses personal data to make or drive decisions, data rules on automated individual decision-making and profiling must be considered.
  Medical advice: CDSS must support, not replace, the physician's professional judgment; the physician remains responsible for interpreting outputs and deciding whether they are appropriate for the individual patient.
  Explainability, bias and accountability: For AI-enabled CDSS, regulators increasingly expect documentation of model performance, limitations, bias mitigation and human-oversight mechanisms (human in the loop).
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  MD and AI qualification: AI/ML systems intended for diagnosis, prevention, monitoring or treatment generally qualify as MD or IVD, triggering classification (at least class IIa), CE-marking, clinical evaluation and post-market surveillance.
  Algorithm dynamics and accountability: Changes in AI models can count as significant modifications under MDR, requiring updated documentation and possibly new conformity assessment.
  Data protection and telematics: Training and inference on health/genetic data require compliance
  Austrian authorities currently apply a lifecycle-based compliance approach, relying on post-market surveillance rather than dynamic re-approval for software updates.
- **IoT (Internet of Things) and Connected Devices**
  MD status: Connected sensors and IoT platforms are MDs when intended for medical purposes (e.g. remote vital-sign monitoring, connected blood-pressure systems) and must comply with device safety, cybersecurity and interoperability requirements.
  Continuous data transfer of health parameters requires data protection (special-category data), health telematics compliance, and in some cases the observation of telecommunication/e-privacy rules; secure authentication, encryption and access control are essential.
  Liability analysis must cover hardware, embedded software, cloud components and interfaces to ELGA or hospital IT, in line with MDR post-market surveillance and EU product liability standards.
- **3D Printing/Bioprinting**
  Product classification: 3D-printed medical products may qualify as MD or, for tissue-engineered products (bioprintings), as advanced-therapy medicinal products (ATMPs), the latter requiring drug authorisation and drug quality requirements.
  Data and design files: Patient-specific printing involves processing imaging and other health data under data protection and health telematic rules; design files and printing parameters can raise IP and trade-secret issues.
  Bioprinting, especially of tissues or organs, raises ethical, safety issues, which must be addressed in clinical trials and ethics-committee approvals.
- **Digital Therapeutics**
  MD qualification: Digital therapeutics qualify as high-risk MDs.
  Evidence and reimbursement: Clinical evidence of therapeutic benefit is required for clinical evaluation and potential reimbursement (e.g. future Austrian DiGA/DiPA-type processes under the eHealth Strategy).
  Data and ELGA: Secure integration with ELGA as digital therapeutic solutions process detailed behavioural and health data, alongside clear information on adherence monitoring and secondary data use.
- **Digital Diagnostics**
  MD qualification: Software and connected tools that perform device-controlled diagnostic measures (including image analysis and lab result interpretation) are MDs or IVDs (class IIa or higher).
  Telematics: Diagnostic data are ELGA-relevant health data; their storage and exchange (e.g. lab reports, imaging results) must follow ELGA and health telematics rules on permitted data types, retention and access.
  The closer a diagnostic output is to an automated or decisive finding, the more regulators focus on validation, human oversight and compliance with data provisions on profiling and automated decision-making.
- **Electronic Medical Record Management Solutions**
  Data protection and telematics: Solutions must implement strong authentication, role-based access and logging; patients retain rights to access their data and may opt-out.
  ELGA framework: Regulates how long health data can be stored, and who may access it, as well as interoperability requirements, standardisation and secure connection. ELGA and integrated services (e-medication, e-lab, e-reports) are funded via the statutory health-insurance and public budgets. Patients do not pay separately for these services.
- **Big Data Analytics**
  GDPR compliance: Large-scale analytics on health data must comply especially with legal basis for processing special-category data, purpose limitations, and safeguards for research/secondary use exceptions.
  Data governance and sharing: The EU Data Governance Act and national laws aim to facilitate the sharing and re-use of protected data, including some health data, under controlled conditions; Austrian telematics regimes on health and genetic data apply.
  De-identification and re-identification risk: Pseudonymisation/anonymisation strategies must be robust, given high re-identification risk with health big data, and are central to data protection impact assessments and ethics approvals for analytics projects.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Data protection: Key regulatory challenges include data controllership reconciling, data subject rights, blockchain immutability (e.g. right to erasure or correction) and ensuring confidentiality and access control.
  Health telematics: Where health data is transmitted within healthcare systems.
- **Natural Language Processing**
  MD qualification: NLP technologies generally do not qualify as MDs (e.g. dictation or transcription software) unless where NLP is specifically intended for a medical purpose (e.g. symptom analysis, clinical decision support, or diagnostic assistance).
  Where personal or health data is processed, data protection rules apply, including transparency and security requirements.

Medical advice: NLP-based tools must not replace the physician in giving medical advice; their outputs must be framed as decision support and used under professional responsibility.

3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?

Providers must: observe and navigate:

- Medical advice: only a treating physician, not the platform, must be presented as the medical service provider.
- Terms of use and user interfaces: should define responsibilities, professional independence of physicians and appropriate disclaimers.
- Prohibition of referral fees: platform business models must avoid per-patient referral fees, lead-based commissions or similar constructs; remuneration should be structured as neutral service fees (e.g. subscription/flat platform fees).
- Whether platform functionalities (e.g. decision support) could trigger MD requirements.
- GDPR and telematics: health data (special-category data) and state-of-the-art technical and organisational measures and roles (is controller, joint controller or processor).
- EU Digital Markets Act (Regulation (EU) 2022/1925): in case of gatekeeper-status, potential obligations on self-preferencing, data use and interoperability.
- Product liability, consumer protection and advertising restrictions.

Additionally, platforms intermediating between healthcare providers and patients may fall under the EU Platform-to-Business Regulation (Regulation (EU) 2019/1150), which requires transparent, fair terms and clear ranking and access rules for business users.

4 Data Use

4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The use of personal health data is primarily governed by the GDPR and the Austrian Data Protection Act. According to Art. 9 GDPR, genetic data, biometric data and data concerning health are categorised as special categories of personal data, the use of which is generally prohibited. The processing of the foregoing data is only permitted if one of the conditions of Art. 9 Para. 2 GDPR is met (e.g. consent of the data subject or processing is required to protect vital interests). The Austrian Data Protection Act does not stipulate additional obligations.

In addition to the general data protection framework, the Austrian Health Telematics Act stipulates rules for the processing of health data by healthcare providers and is the central legal framework for electronic health record systems. With the EHDS new rules for sharing, accessing and using health data will be established.

4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

Legal regulation of the use of personal health data is uniformly governed under national laws/European law.

4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?

According to Art. 9 Para. 2 GDPR, the processing of health data is permitted under specific conditions. These conditions do not address specific entities, but determine which purposes are accepted. Albeit, within the purposes, some entities are considered (e.g. associations with a non-profit aim, public health entities, research entities). For medical professionals, the Health Telematics Act is applicable in addition.

With regard to the nature of the data, the main element is whether the data are personal, thus relating to an identified or identifiable natural person or anonymised (then GDPR does not apply).

4.4 How do the regulations define the scope of personal health data use?

As the processing of health data is generally prohibited under the GDPR, the permitted scope of use is explicitly set out in Art. 9 Para. 2. Also, the Austrian Health Telematics Act lays down in detail which data may be used for what purpose, e.g. in Sec. 14.

4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?

A central aspect for contractual terms is the clear determination of the purpose of data processing and the roles of the different actors (data controller, data processor, data subject). Moreover, clarifying the retention of data, deletion of data, technical and organisational measures for secure processing, data transfers and data subjects' rights is essential.

4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

There are no regulations specifically addressing these aspects. However, the GDPR stipulates the principles of accuracy of data and the integrity of data, which also apply to health data. The Health Telematics Act additionally governs the integrity of electronic health data by stipulating the necessity of electronic signatures.

4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

There are various standards established by the Austrian Standards organisation, such as on health informatics.

5 Data Sharing

5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

The sharing of data is considered as a form of "processing"

such as the use of data. Therefore, for the sharing of data, the regulations of the GDPR and the Health Telematics Act apply. If data is shared for processing, the roles (controller and processor) and according obligations must be considered. If data is shared with a recipient that is located outside of the EU, this amounts to a transfer under the GDPR and must be in line with the strict requirements of Art. 44 *et seq.* GDPR. In addition, the EU Data Act must be considered.

5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?

The sharing of personal health data is uniformly governed under national laws/European law.

5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?

See question 4.3.

5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?

The GDPR stipulates strict rules for the sharing of data (as this is a form of processing and therefore requires a legal basis). In addition, the Health Telematics Act sets out in its Chapter 2 provisions specifically tailored to the electronic transfer of health data.

5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?

In Austria, federated models of healthcare data (HD) sharing are most prominently embodied in ELGA, which is designed as a decentralised/federated system where health data remain stored at the level of the original healthcare providers and are made accessible through a shared infrastructure rather than being centrally pooled. ELGA is essentially governed by the Health Telematics Act and the GDPR.

6 Intellectual Property

6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?

Under the Austrian Patent Act, an invention must be new, involve an inventive step, and be industrially applicable to be eligible for the awarding of a patent. Software as such is not patentable (explicitly excluded), unless it has a technical character or produces an additional technical effect. Hardware is patentable if it fulfils the requirements for a patent. Thus, DH technologies are patentable as hardware or as technical solutions, not as abstract data processing or medical decision-making alone.

6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?

The Austrian Copyright Act protects works that are original intellectual creations. It specifically governs the protection of computer software and databases, thus protecting the code, preparatory materials and databases. However, only works created by natural persons (not, e.g., AI) are protected.

6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?

The Austrian Act against Unfair Competition protects information that is secret, has commercial value due to its secrecy, and is subject to reasonable confidentiality measures, as a trade secret. This can be crucial if other intellectual property rights do not apply. However, the characteristics of a trade secret must be upheld to be protected.

6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?

The Austrian University Act stipulates that employed researchers must report inventions to the university, which can subsequently acquire patent rights to these inventions. With regards to copyrights, only the natural person generating the work is regarded as the originator and protected by copyrights, but rights of use can be granted to other parties such as academic institutions.

6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?

The protection for SaMD depends on the qualifications of the components. For hardware and software with technical contribution, patent law can apply. For source codes and databases, copyrights can apply. Information can be protected as a trade secret.

6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?

No. Only natural persons can be inventors.

6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?

There is no specialised statutory regime in Austria that provides for an automatic transfer of intellectual property rights to the state on the basis of funding. The allocation of these rights must be governed by contracts. It is common practice to grant certain rights or obligations on dissemination or open access.

6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?

Intellectual property rights are mainly shaped by the legal framework and less by precedential cases. A significant decision to mention was 4 Ob 119/20h issued by the Austrian Supreme Court on the aspects of "technicity" for protection under patent law.

7 Commercial Agreements

7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?

When structuring collaborations in DH, parties should:

- Define IP and ownership: clear contractual allocation of ownership to pre-existing and emerging IP, usage and commercialisation rights, licensing scope, exclusivity, and sublicensing rights.
- Allocate regulatory and liability responsibilities: Contractually assign MDR/IVDR roles and responsibilities for CE-marking, vigilance, post-market surveillance and telematics compliance, clarify liabilities, insurance and corrective measure responsibility.
- Define governance and exit: regulate decision-making processes, joint steering, audits, governance structures, information sharing, exit scenarios, and the handling of regulatory-driven changes to ensure long-term scalability and compliance.

7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?

- Compliance and roles under MDR/GDPR.
- Ensure business transparency and written documentation.
- Ensure healthcare compliance with ABC rules (MD laws, criminal law), professional conduct rules and industry codes (for MDs and drugs).

7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?

- Address roles (controller, joint controller, processor).
- Regulate security, data minimisation, governance and confidentiality.
- Assess whether data can be anonymised, as this limits the data protection requirements and allows re-use and commercialisation.
- Address IP ownership in trained models, restrictions on downstream use, and regulatory compliance (e.g. MDR, AI Act).
- Regulate liability allocation and audit rights.

7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?

- Ensure AI Act compliance (e.g. AI literacy, prohibited practices, transparency, high-risk AI).
- Ensure MDR alignment (risk classification, conformity assessment, technical documentation, risk management, transparency).
- Clarify who may use and own AI-generated code, text, images or clinical content, and whether and how such output may be reused, commercialised or used for further training.
- Identify and address third-party IP risks and allocate warranties, indemnities and due-diligence obligations accordingly.
- Prohibit or tightly control input of identifiable patient data into general-purpose AI systems unless a solid GDPR legal basis, telematic compliance and appropriate DPAs are in place (including location of processing and sub-processor chains).
- Define confidentiality, security and data-use limits for providers of foundation models (e.g. patient/customer data training).
- Regulate product liability and transparency (human supervision).

8 Artificial Intelligence and Machine Learning

8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?

Austria has not yet established a centralised regulatory body for AI/ML frameworks enforcement. Consequently, competences are distributed among various authorities, such as: the AI Service Desk at the RTR; the governmental AI Advisory Board; DSB; and AGES.

8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.

The primary regulatory framework is the EU AI Act. At present, there is no supplementary national legislation in Austria dedicated to AI. However, the deployment of such technologies remains subject to existing cross-sectoral regimes, specifically the GDPR and the Health Telematics Act for the secure electronic processing of health data.

8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?

Under Austrian law, rights are only granted to human originators. Improvements generated autonomously by AI either remain unprotected or are attributed to the human who designed the system, depending on circumstances.

8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

As HD is a special category of personal data (Art. 9 GDPR), HD licensing is significantly more restricted and compliance-heavy than general AI data licensing.

8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

Currently, only the AI Act itself differentiates: if an AI system serves to generate text, images etc., transparency obligations apply (e.g. the output must be marked as generated by AI). In addition, there are specific rules for general purpose AI (GPAI), i.e. an AI model trained with a large amount of data using self-supervision, capable of performing a wide range of distinct tasks. Providers of GPAI must comply with stricter requirements (e.g. notification of the EC, technical documentation, copyright protection policy).

When health data is used in AI applications, high-risk AI rules apply, as Annex I of the AI Act classifies MDs as high-risk AI.

8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?

Generative AI and GPAI are subject to a more stringent regulatory regime under the EU AI Act due to the risks associated with synthetic outputs that are indistinguishable from human-generated content and the possibility of using these applications for various purposes.

8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.

In Austria, the issue of AI/ML models trained on data without appropriate rights is addressed through a combination of copyright rules, GDPR and the EU AI Act. The central legal mechanism is the Text-and-Data-Mining exception, which stipulates that models may be trained on data, if the holder of the according rights has not explicitly refused. With regard to personal data, the processing must comply with the GDPR.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health solutions?

Austria regulates DH liability through general liability rules rather than a sector-specific regime. For AI/ML, the same basic rules apply, but forthcoming EU product-liability and AI rules will increase expectations on risk management, transparency and documentation.

- Contractual and tort liability (for damages caused culpably and unlawfully in the healthcare context, including pain and suffering, but excluding punitive damages).
- Strict Product liability (2026 will bring liability rules for standalone apps and AI models as well as presumptions of defect and document disclosure obligation).
- Regulatory, criminal and professional consequences (for instance fines or recalls).

9.2 What cross-border considerations are there?

- Applicable law and jurisdiction mainly follow EU rules, unless contractually agreed upon.
- Physicians outside Austria providing telemedical services to patients located in Austria must comply with Austrian professional licensing requirements unless the freedom to provide services applies (if services are provided on a temporary and occasional basis, Sec. 37 ÄrzteG).
- Consumer protection rules may also be relevant, as healthcare services are typically provided on the basis of contracts concluded by patients acting as consumers.

9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?

Such risks can be mitigated through a combination of legal, technical, and organisational measures, namely a robust regulatory and quality compliance, allocation of responsibility and governance.

- Ensure AI/ML-enabled solutions comply with MD/IVD laws (risk management, clinical evaluation, post-market surveillance, etc.), with clear allocation of roles.
- Implement documented quality-management and risk-management systems that explicitly address AI/ML lifecycle risks.
- Ensure clear allocation of responsibilities (vendor, integrators, providers, deployers) and governance around models and updates.
- Ensure data protection, security and transparency.

9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?

- GDPR: A misuse of HD constitutes a breach of GDPR, which allows the data subject to exercise its rights and claim damages under tort law or contract law. In addition, administrative fines can be awarded.
- Manufacturer and vendor liability: AI/ML developers and vendors can be liable under contract and tort principles, and/or product liability (e.g., security defects, model leaks).

In practice, managing the liability risk requires careful allocation and documentation of roles (controller/processor, manufacturer/user), lawful data sourcing and training, strong technical and organisational safeguards, and clear internal policies on how AI/ML outputs are used in clinical and commercial workflows.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

- Data protection and telematics compliance (strong encryption, access controls, logging and secure transmission; location of processing and transfer to third countries, especially regarding ELGA/eHealth infrastructure integration).
- MD qualification and shared responsibility (manufacturer, cloud provider and healthcare role, e.g. regarding configuration and update responsibilities, incident response).

10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?

- Regulatory perimeter and business-model fit: Check if the solution is a MD/IVD, whether activities/services fall under medical services (reserved for physicians) or engage in prohibited patient referrals and/or comply with health data rules.
- Reimbursement: Assessed whether reimbursement is legally possible to avoid market entry barriers.
- Healthcare compliance (ABC) rules *vis-à-vis* HCPs/HCOs and implement compliance culture/structures.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?

- Perform in-depth regulatory, healthcare law and data-protection due diligence.
- Ensure EU-wide regulatory scalability.
- For AI/ML-based products regarding compliance with model development, training data, update processes and documentation rules and EU AI/product-liability requirements.
- Check reimbursement status and eHealth pathways (ELGA integration, possible future DiGA/DiPA-type schemes, individual contracts with payors) and dependence on specific HCPs/HCOs for assessing scale potential.

10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?

- Medical advice is reserved to licensed physicians thereby limiting task-shifting and automation or direct-to-patient models.
- Infrastructure constraints: Fragmented IT infrastructure and varying digital maturity across providers and regions can slow down integration of new tools with hospital information systems and ELGA.
- Literacy gaps: digital literacy of the aging patient population and/or HCPs.
- *Ad hoc* reimbursement: currently no structured framework, but standardised process to be established 2026.

10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?

Adoption and processes are primarily governed by regulatory frameworks rather than by independent certification bodies.

Consultations on these matters typically involve the Austrian Medical Chamber, the Umbrella Association of Social Insurances or special health associations. Endorsements or guidelines from such professional associations and scientific societies can be influential in clinical practice and may be consulted in legislative, court or policy processes, especially for defining "state-of-the-art" care.

10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?

A standardised national reimbursement process will be codified by 2026/2027 – DiGAs will be reimbursable if clinical evidence of positive care effects is provided.

Presently, for digital tools, reimbursement, on an occasional basis, requires the solution to be classified as a medical aid or reimbursement is specifically agreed upon by the developer with social insurance carriers. Still, formal evaluation and registration requirements are expected to increase as Austria develops a framework for evidence-based digital therapeutic applications under the Digital Austria agenda.

10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?

Due diligence gaps often arise from the complex framework, namely the intersection of regulatory, data protection, and technical issues. Legal, technical, and clinical aspects are frequently analysed in isolation but require a multidisciplinary approach. Also, interoperability with eHealth systems and data fragmentation and insufficient documentation or validation can be an issue.

10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.

- Trade licences and facility permits.
- The 2026 alignment of ELGA with the EHDS regarding cross-border portability and secondary use data (data altruism).
- DiGAs: standardised national reimbursement process planned.
- High-risk AI: AI Regulatory Sandbox, allowing DH startups to test AI-driven solutions in a "safe harbour" environment with regulatory guidance from the BASG.
- Mandatory digitalisation for physicians (medical data storage).
- Stricter product liability (AI/software defects, evidence standards).

Dr. Daniel Larcher is a partner at ATLAS Attorneys at Law and was admitted to the Bar in 2010. He specialises in commercial law and public commercial law with a focus on healthcare, regulatory and contracts. Daniel is the author of numerous publications in his areas of expertise and gives lectures, workshops, and training courses on these topics.

ATLAS Attorneys at Law
Nibelungengasse 13/1
1010 Vienna
Austria

Tel: +43 1 925 97 66
Email: d.larcher@atlas-law.at
LinkedIn: www.linkedin.com/in/daniel-larcher-43808698

Dr. Mariella Rieder, LL.M., is a Senior Legal Counsel at Prewave GmbH, an Austrian company providing AI-driven software for supply-chain monitoring. Mariella has passed the Austrian Bar exam, worked for an international law firm, the European Commission, as well as the Austrian Ministry of Justices, and currently specialises in AI Law, Data Protection Law and IT Law.

Prewave GmbH
Rothschildplatz 4 / Austria Campus 4, 3rd Floor
1020 Vienna
Austria

Tel: +43 1 30 50 743
Email: mariella.rieder@prewave.ai
LinkedIn: www.linkedin.com/in/mariella-rieder