Aliance pro telemedicínu
a digitalizaci zdravotnictví
a sociálních služeb

V Praze 11. 11. 2025

Stanovisko ATDZ k bezpečnostním a provozním minimům standardů poskytování telemedicínských zdravotních služeb v České republice podle platných právních předpisů

I. Úvod

Toto stanovisko Aliance pro telemedicínu a digitalizaci zdravotnictví a sociálních služeb (dále jen „**ATDZ**“) je předkládáno s cílem vymezit minimální technické a obsahové standardy pro poskytování telemedicínských zdravotních služeb v České republice. Jeho hlavním účelem je zajistit, aby poskytování telemedicínských vyšetření probíhalo s ohledem na bezpečí pacientů, v požadované kvalitě a v souladu s právním řádem. Dokument vychází zejména z ustanovení § 11c zákona č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů (dále jen „zákon o zdravotních službách“) , zákona č. 325/2021 Sb. o elektronizaci zdravotnictví, ve znění pozdějších předpisů (dále jen „zákon o elektronizaci zdravotnictví“) prováděcích vyhlášek ministerstva zdravotnictví č. 30/2025 Sb., o telemedicínských zdravotních službách a č. 444/2024 Sb., o zdravotnické dokumentaci a z technického standardu telemedicínských zdravotních služeb podle zákona o elektronizaci zdravotnictví zveřejněného ve Věstníku Ministerstva zdravotnictví České republiky (dále jen „**MZČR**“) č. 4/2025.

Zvláštní důraz klademe na ochranu pacientů – jak v oblasti kybernetické bezpečnosti a ochrany osobních údajů, tak v klinické rovině prostřednictvím povinného vedení závěrečné zprávy a zavedení lékového záznamu, který zabrání nežádoucím lékovým interakcím. Stanovisko zároveň formuluje požadavky na interoperabilitu a technická opatření, která posílí důvěru pacientů i zdravotnických pracovníků v telemedicínské zdravotní služby.

Na Pankráci 322/26
140 00 Praha 4

tel.: 735 751 961

e-mail: info@atdz.cz
www.atdz.cz
IČ 11700751

II. Obecné technické a bezpečnostní požadavky

Zajištění bezpečnosti telemedicínských zdravotních služeb vyžaduje komplexní přístup zahrnující ochranu osobních údajů, kybernetickou bezpečnost i kontinuální správu technických řešení. Poskytovatelé telemedicínských zdravotních služeb (dále jen „TMZS“) jsou povinni pravidelně provádět analýzu rizik, realizovat penetrační testy a bezpečnostní audity, a tím průběžně ověřovat odolnost svých systémů vůči hrozbám. V souladu s požadavky Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dale jen “GDPR“) a zákona o kybernetické bezpečnosti *(Pozn. s účinností od 1. listopadu 2025 byl přijat nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti)* je nezbytné chránit integritu, důvěrnost a dostupnost zdravotnických dat. K tomu slouží zejména implementace pokročilých šifrovacích metod – povinné end-to-end šifrování komunikace, využití algoritmu AES-256 pro lokální ukládání dat a protokolu TLS verze 1.3 nebo vyšší při přenosu dat přes internet. Přístup k datům musí být chráněn vícefaktorovou autentizací (MFA) a řízen prostřednictvím modelu role-based access control (RBAC), který umožní přesně vymezit oprávnění jednotlivých uživatelů.

Další vrstvu ochrany představuje zabezpečení aplikačních rozhraní (API). Pro autorizaci přístupu je doporučeno využívat moderní protokoly typu OAuth 2.0 nebo OpenID Connect, které umožňují detailní kontrolu nad přístupem k datům a minimalizují riziko neoprávněného využití. Zároveň je třeba implementovat aplikační firewally, mechanismy pro omezení nadměrného počtu požadavků (Rate Limiting) a pravidelně provádět testy odolnosti proti útokům typu DoS/DDoS.

Správa a ochrana šifrovacích klíčů musí být realizována pomocí specializovaných bezpečnostních řešení (např. HSM, tokenů apod.) dle směrnice definované v regulaci eIDAS článku 30. pro kvalifikované prostředky, případně modulů integrovaných do zařízení (TPM, TEE, Secure Enclave), které umožňují izolované a bezpečné zpracování citlivých dat. Veškerý software i hardware využívaný pro telemedicínu musí být v aktivní podpoře výrobce nebo komunity; v případě ukončení podpory (EOL) je nutné jej neprodleně nahradit. V prostředích, kde je nezbytná vysoká dostupnost, je doporučeno testovat aktualizace nejprve v testovacím prostředí a aktivně sledovat databáze známých zranitelností, například CVE.

Specifickou oblastí je videokomunikace, která je v telemedicíně často využívána k diagnostice či konzultaci. Poskytovatel je povinen dodržovat Bezpečnostní standard pro videokonference vydaný NÚKIB a implementovat nástroje pro řízení šířky pásma a optimalizaci latence. Prioritizace provozu prostřednictvím QoS a průběžné monitorování výkonu sítě jsou klíčové pro udržení kvality poskytovaných služeb. Přenos obrazového a zvukového záznamu má být realizován prostřednictvím moderních kodeků (H.264, H.265, AV1) a zabezpečen šifrováním TLS 1.3. Ukládání záznamů a přenášených dat musí být chráněno šifrováním na úrovni ES-256, aby byla zachována jejich integrita a důvěrnost definována v regulaci eIDAS, která vymezuje soulad v rámci EU v oblasti kryptografie. Např. standard ETSI TS 119 312 specifikuje povolené kryptografické algoritmy a jejich parametry.

Pro zajištění univerzální dostupnosti a uživatelského komfortu je nezbytné, aby poskytovaná telemedicínská řešení byla nativně vyvinuta a dostupná pro všechny hlavní platformy, tedy iOS, Android, Windows a macOS. Současně musí být rozlišeno samostatné a zvlášť zabezpečené prostředí pro lékaře a pro pacienty, aby byla zajištěna odpovídající úroveň ochrany dat a funkčnost přizpůsobená specifickým potřebám jednotlivých uživatelských skupin. Všechna řešení musí být realizována jako nativní aplikace, nikoli pouze jako webové či hybridní nástroje, a jejich poskytovatelé musí disponovat relevantní certifikací dle mezinárodních standardů ISO, zejména ISO 13485 (řízení kvality zdravotnických prostředků), ISO/IEC 27001 (řízení informační bezpečnosti), ISO 16363 (důvěryhodné digitální úložiště) a ISO 20000-1 (systém managmentu služeb v IT). Úplný přehled všech vyžadovaných bezpečnostních certifikátů je uveden v příloze č. 1 tohoto stanoviska.

III. Interoperabilita a datová komunikace

Pro efektivní a bezpečné poskytování TMZS je nezbytné zajistit jejich plnou interoperabilitu s národními i evropskými systémy elektronického zdravotnictví, kterou definuje rámec Regulace (EU) 2024/1183 Evropského parlamentu a Rady ze dne 11. dubna 2024 - známého jako „Digitální peněženka“ eIDAS 2.0, kde rozšiřuje oblast užívání digitálních nástrojů, a to i ve zdravotnictví. Služby, které budou nově dostupné od roku 2026, musí zajistit interoperabilitu napříč EU a budou jimi například:

1.Přístup ke zdravotním datům a jejich výměna v rámci Evropského prostoru zdravotních dat

2. Průkaz dárce orgánů

3. Hlášení podezření na incident související se zdravotnickými prostředky

3. Případy užití v rámci národních a regionálních elektronických zdravotnických systémů

4. Digitální telemedicína

Telemedicínské technologie proto musí být schopny bezproblémové komunikace a výměny dat napříč různými platformami a zdravotnickými informačními systémy. ATDZ požaduje, aby byly povinně implementovány mezinárodní a národní standardy, zejména HL7 FHIR pro strukturovaná klinická data, DICOM pro obrazovou dokumentaci, evropský formát zdravotních záznamů EEHRxF a český standard DASTA.

Stejně důležitá je i možnost bezpečné výměny dat mezi pacienty, poskytovateli zdravotních služeb a dalšími oprávněnými subjekty. Přenos musí být realizován prostřednictvím šifrovaných komunikačních kanálů a vždy s důrazem na ochranu osobních údajů v souladu s GDPR. Interoperabilita tedy není pouze technickým požadavkem, ale i základní zárukou kontinuity péče, bezpečnosti pacienta a efektivního využití digitálních zdravotnických nástrojů.

IV. Obsahové požadavky na telemedicínské zdravotní služby

ATDZ zdůrazňuje, že samotné technické standardy nejsou dostatečné bez jasně stanovených obsahových náležitostí. Každé telemedicínské vyšetření proto musí být zakončeno vytvořením závěrečné zprávy, která se stane součástí zdravotnické dokumentace pacienta v souladu se zákonem o zdravotních službách a prováděcí vyhláškou o zdravotnické dokumentaci. Tato zpráva musí mít stejné právní a odborné náležitosti jako záznam z prezenčního vyšetření, a tedy zajistit kontinuitu péče a možnost jejího dalšího využití v klinické praxi.

Součástí zprávy musí být jednoznačná identifikace pacienta i zdravotnického pracovníka, který vyšetření provedl a to díky elektronické identifikaci klienta/zdravotní pracovníka dle Nařízení eIDAS (EU 910/2014) na požadované minimální úroveň eID:

- Podstatná (Substantial) kde ověření identity slouží nástroje např. Bankovní identita, OTP + heslo

Nebo

- Vysoká (High) Nejvyšší úroveň, kde je eObčanka, čipová karta s PIN, Biometrické ověření atd. a dále časové razítko eSEAL elektronická služba dle čl. 36 eIDAS ekvivalent razítka používaný právnickými osobami (firmami, úřady), sloužící k zaručení původu a integrity elektronického dokumentu tedy eReceptu apod. minimálně na úrovni Advanced nebo HIGH.

Od roku 1.1.2027 potom také služba důvěryhodné Archivace – dlouhodobé uchování důvěryhodnosti dokumentů specifikované v regulaci eIDAS 2.0. zajišťující ověřitelnost a chronologii záznamu, a rovněž záznam souhlasu či případných námitek pacienta v souladu s právní úpravou.

Tímto způsobem lze zajistit, aby telemedicínské služby nebyly vnímány pouze jako doplňková forma péče, ale jako plnohodnotná součást zdravotnického procesu, která odpovídá stejným nárokům na dokumentaci, bezpečnost a ochranu práv pacienta jako tradiční zdravotní služby.

V. Lékový záznam

ATDZ považuje za zásadní, aby součástí telemedicínských technologií byl také alespoň modul lékového záznamu. Tento prvek je klíčový pro zajištění bezpečnosti pacienta a prevenci nežádoucích účinků spojených s farmakoterapií. Modul musí umožňovat přehledné zobrazení všech předepsaných a vydaných léčiv pacienta. Díky tomu lze předcházet závažným zdravotním komplikacím a zvýšit bezpečnost poskytované péče v případech, kdy pacient nemusí být fyzicky přítomen u lékaře.

Propojení s centrálním systémem eRecept dle §81 a násl. zákona č. 378/2007 Sb., o léčivech, ve znění pozdějších předpisů a s lékovým záznamem vedeným podle §81d téhož zákona, je v tomto ohledu nezbytné. Telemedicínské technologie tak nebudou fungovat izolovaně, ale stanou se součástí komplexního systému elektronizace zdravotnictví, který umožní poskytovat péči na dálku se stejnou mírou bezpečnosti a odpovědnosti, jaká je vyžadována u prezenčních služeb.

Zařazení lékového záznamu mezi minimální standardy TMZS je podle ATDZ krokem, který posílí důvěru pacientů i zdravotnických pracovníků v telemedicínu a zajistí, že digitální nástroje nebudou pouze technickou inovací, ale skutečným prostředkem pro kvalitní a bezpečnou péči.

VI. Závěr

ATDZ plně podporuje rozvoj telemedicíny v České republice a vnímá ji jako důležitý nástroj moderní zdravotní péče. Aby však mohla telemedicína naplnit svůj potenciál, považujeme za nezbytné, aby byly jasně a závazně stanoveny minimální technické a obsahové standardy, které budou platit pro všechny poskytovatele TMZS i jejich technologické partnery.

ATDZ je připravena aktivně spolupracovat s Ministerstvem zdravotnictví ČR na dopracování detailních požadavků, metodických postupů i na jejich implementaci v praxi. Naším cílem je, aby telemedicína byla vnímána nejen jako technologická inovace, ale především jako spolehlivý, bezpečný a plnohodnotný způsob poskytování zdravotní péče, který chrání pacienty a posiluje důvěru ve zdravotnický systém.

Na Pankráci 322/26
140 00 Praha 4

tel.: 735 751 961

e-mail: info@atdz.cz
www.atdz.cz
IČ 11700751

Příloha č. 1 – Přehled vyžadovaných norem ISO pro telemedicínská řešení

Norma/Certifikace	Charakteristika	Význam pro telemedicínu
ISO/IEC 27001 – Řízení bezpečnosti informací	Mezinárodní standard pro nastavení, řízení a neustálé zlepšování systému řízení bezpečnosti informací.	Telemedicína pracuje s citlivými zdravotnickými daty pacientů, proto je zajištění ochrany proti únikům, kybernetickým útokům a neoprávněnému přístupu zásadní.
ISO/IEC 27701:2019 – Ochrana osobních údajů (PIMS)	Rozšíření ISO 27001 a 27002, zaměřené na ochranu osobních údajů a GDPR.	Pacienti musí mít jistotu, že jejich zdravotní data jsou chráněna v souladu s GDPR a další legislativou ochrany osobních údajů.
ISO/IEC 27799:2016 – Informační bezpečnost ve zdravotnictví	Standard, který aplikuje principy ISO 27001 přímo na zdravotnická data a procesy.	Poskytuje konkrétní metodiky, jak chránit elektronickou zdravotní dokumentaci, telemedicínské záznamy a diagnostická data.
ISO/IEC 16363:2012 – Důvěryhodné digitální repozitáře	Standard pro audit a certifikaci digitálních úložišť dat.	V telemedicíně je klíčové, aby archivovaná zdravotní data byla dlouhodobě dostupná, ověřitelná a důvěryhodná, např. pro budoucí léčbu nebo soudní účely.
ISO/IEC 37001:2016 – Protikorupční management systém	Mezinárodní standard zaměřený na prevenci korupce a etické řízení.	Ve zdravotnictví, kde probíhají tendry a velké veřejné zakázky, je transparentnost a protikorupční prostředí zásadní pro důvěru pacientů i partnerů.
ISO 13485:2016 – Kvalita zdravotnických prostředků	Standard pro systém managementu kvality výrobců a dodavatelů zdravotnických prostředků.	Telemedicínská aplikace je posuzována jako zdravotnický prostředek. Certifikace dokládá, že vývoj a provoz probíhají v souladu s nejvyššími normami kvality a bezpečnosti.
ISO 9001:2015 – Management kvality	Obecný standard pro řízení kvality napříč obory.	Ujišťuje pacienty i zdravotnická zařízení, že procesy v telemedicíně jsou systematicky řízeny a neustále zlepšovány.

ISO/IEC 20000-1:2018 – Řízení IT služeb (IT Systém Managment)	Standard pro poskytování a řízení IT služeb.	Telemedicína je postavená na IT službách, které musí být spolehlivé, dostupné a bezpečné, aby pacienti i lékaři měli jistotu nepřetržité funkčnosti.
ISO 22301:2019 – Řízení kontinuity činností (Business Continuity Management)	Standard pro nastavení a řízení kontinuity provozu v krizových situacích.	Zdravotnické služby musí být dostupné i při výpadku systémů, přírodních katastrofách nebo kybernetických útocích — život pacienta může záviset na okamžité dostupnosti služby.
eIDAS certifikace dle ISO/IEC 17065 – Důvěryhodné služby, kryptografické funkce a elektronická identita minimálně na úrovni Střední (Substential), doporučuje se úroveň HIGH (Vysoká), QSCD prostředky a důvěryhodné služby jako např. eSeal.	Evropský rámec pro poskytování důvěryhodných služeb (např. elektronický podpis, pečeť, časové razítko) certifikovaný akreditovanou autoritou dle ISO/IEC 17065.	Zajišťuje právní závaznost, důvěryhodnost a interoperabilitu elektronické identifikace a podpisů v celé EU, což je nezbytné pro právně platnou komunikaci v telemedicíně.