Regulatory Pathway

مقدمه و ضرورت سند (صفحه ۳-۱) 6.7.1 ##

ماهیت حساس حوزه فعالیت .۱/۱

در تقاطع دو حوزه `nobatnou.ir` سیستم نوبت‌دهی آنلاین فعالیت می‌کند. ** (Health) **فناوری (تکنولوژی)** و **سلامت Digital) این جایگاه، آن را به یک **سرویس سلامت دیجیتال یا به طور خاص‌تر، یک **سرویس مدیریت **(Health Service - Patient Relationship Management) ارتباط با بیمار تبدیل می‌کند. حساسیت ذاتی این حوزه ناشی از موارد زیر **(PRM است:

* ماهیت داده‌های پردازشی:** داده‌های شخصی و حساس (شامل ** نام، شماره تماس، و در آینده احتمالاً اطلاعات اولیه پزشکی).

* ذینفعان متعدد و حساس:** بیماران (مصرف‌کنندگان نهایی با ** حقوق قانونی و انتظارات اخلاقی بالا)، پزشکان و مراکز درمانی (ذینفعان حرفه‌ای تحت نظارت نهادهای تخصصی)، و سیستم سلامت عمومی.

تأثیر بر تصمیم‌گیری‌های بهداشتی:** سیستم با ارائه اطلاعاتی ** *
مانند زمان تخمینی ویزیت، به طور غیرمستقیم در تصمیم بیمار برای
.مراجعه به پزشک تأثیر می‌گذارد

پیوند با زیرساخت سلامت:** قابلیت یکپارچه‌سازی آتی با ** *
.و شبکه‌های درمانی (EHR/EMR) سامانه‌های الکترونیک سلامت

هدف از تدوین مسیر انطباق رگولاتوری .۱/۲

این سند با این فرض کلیدی تدوین شده است: **"محصول بدون عبور از
موانع رگولاتوری مناسب، عملاً غیرقابل فروش در مقیاس گسترده و
:جذب سرمایه‌گذاری جدی است."** اهداف این سند عبارتند از

شناسایی جامع:** شناسایی کلیه قوانین، مقررات، استانداردها و ** *
.نهادهای ناظر مرتبط در ایران و در نگاهی فراتر، بازارهای منطقه‌ای

تدوین نقشه راه عملیاتی:** ارائه یک برنامه مرحله‌بندی‌شده، ** *
.واقع‌بینانه و مبتنی بر منابع، برای کسب مجوزها و انطباق‌های ضروری

تخمین هزینه و زمان:** ارائه برآورد شفاف از سرمایه و زمان ** *
.مورد نیاز برای عبور از این مسیر

مدیریت ریسک:** شناسایی ریسک‌های رگولاتوری و تعیین ** *
.راهکارهای کاهش آنها

شفاف‌سازی برای سرمایه‌گذار:** نشان‌دادن بلوغ فکری تیم ** *
بنیانگذار، درک عمیق از فضای کسب‌وکار و ارائه یک **"تکلیف واقعی

برای ورود به بازار (Realistic Go-to-Market Commitment)"**.

رویکرد کلی: تطبیق تدریجی و ریسک‌بنیان .۱/۳

رویکرد شرکت نه مقابله یا اجتناب، بلکه **"انطباق تدریجی (Phased Compliance)"** **"مدیریت فعال ریسک رگولاتوری"** و است. این مسیر از الزامات عمومی و کم‌هزینه‌تر آغاز و به سمت الزامات تخصصی و سنگین‌تر حرکت می‌کند، همگام با رشد شرکت و مقیاس خدمات.

6.7.۲ شناسایی نهادهای ناظر و حیطه نظارتی (صفحه ۷-۴)

مقررات گذاری بر سرویس نوبت نو می‌تواند از سوی چندین نهاد با اهداف متفاوت صورت پذیرد:

| نهاد ناظر / منبع قانون | حیطه نظارت / دغدغه اصلی | ارتباط با نوبت‌نو | سطح اولویت |

| ---------- | ---------- | ---------- | ---------- | ---------- |

وزارت بهداشت، درمان و آموزش پزشکی** و سازمان‌های تابعه ** | (مانند **مرکز مدیریت آمار و فناوری اطلاعات سلامت**) | سلامت دیجیتال، سامانه‌های اطلاعات سلامت، حریم خصوصی داده‌های سلامت، کیفیت خدمات سلامت. | **بالاترین اولویت.** نهاد اصلی حاکم بر محتوای سلامت‌محور سرویس. | فوری (Phase 1) |

سازمان نظام پزشکی جمهوری اسلامی ایران** | اخلاق حرفه‌ای ** | پزشکی، رابطه پزشک و بیمار، تبلیغات خدمات پزشکی، تعرفه‌ها. | **اولویت بالا.** ذینفعان اصلی (پزشکان) تحت نظر این سازمان هستند. قوانین آن بر تعامل پلتفرم با پزشکان حاکم است. | فوری (Phase 1) |

مرکز ملی فضای مجازی** و **پلیس فتا** | حاکمیت داده، امنیت ** | سایبری، فعالیت‌های برخط، جلوگیری از جرائم سایبری. | **اولویت بالا.** هر سرویس برخط با حجم داده شخصی، مشمول مقررات امنیت سایبری و حاکمیت داده می‌شود. | فوری (Phase 1) |

سازمان تنظیم مقررات و ارتباطات رادیویی** | ارسال پیامک ** | انبوه (برای یادآوری نوبت)، استفاده از پورت‌های پیامکی. | **اولویت متوسط.** برای ارسال اطلاع‌رسانی خودکار ضروری است. | میانی (Phase 2) |

اداره کل ثبت شرکتها و مالکیت صنعتی** | ثبت شرکت، ثبت برند ** | و علائم تجاری. | **اولویت پایه.** انجام شده/در حال انجام. | تکمیل | شده

مرکز توسعه تجارت الکترونیکی** (وابسته به وزارت صنعت) | ** | اعتماد و سلامت در تجارت الکترونیک، نشان‌های اعتماد الکترونیکی (اینماد). | **اولویت متوسط.** ایجاد اعتماد نزد کاربران عمومی. | | (Phase 2) میانی

شورای عالی انفورماتیک** (در صورت لزوم) | استانداردهای ** | فنی ملی در حوزه فناوری اطلاعات. | **اولویت آتی.** برای یکپارچه‌سازی با سیستم‌های دولتی ممکن است مطرح شود. | بلندمدت | (Phase 3)

HIPAAاتحادیه اروپا، GDPR :نمونه) مقررات بین‌المللی** | حریم خصوصی و امنیت داده‌های سلامت در سطح | **(آمریکا بین‌المللی. | **اولویت استراتژیک برای توسعه آینده.** بررسی به عنوان حتی در داخل. | چارچوب (Best Practice) چارچوب بهترین عمل | مرجع (همواره)

فازبندی مسیر انطباق (صفحه ۲۲-۸) 6.7.3 ##

فاز ۰: پایه‌های قانونی و انطباق حداقلی (۶ ماه گذشته و حال **حاضر)

* **هدف:** امکان راه‌اندازی و فعالیت پایلوت بدون ریسک حقوقی فوری.

* **اقدامات انجام‌شده/در حال انجام:**

1. **ثبت شرکت:** تکمیل شده.
2. **تدوین سیاست حریم خصوصی و شرایط استفاده:** بر اساس اصول GDPR (۶/۶) و قوانین داخلی، انجام شده.
3. **رعایت قانون تجارت الکترونیک:** درج اطلاعات شرکت، سیاست بازپرداخت در وب‌سایت.
4. **مشاوره حقوقی اولیه:** برای شناسایی چارچوب کلی.

* **خروجی:** **مجوز فعالیت غیرمستقیم** از طریق عدم مانع قانونی برای ارائه خدمات پایه.

فاز ۱: انطباق امنیتی، حریم خصوصی و پایه سلامت (ماه ۱ **تا ۱۲ پس از جذب سرمایه)

* **هدف:** رسمی‌سازی فعالیت، ایجاد اعتماد نزد پزشکان اولیه و آماده‌سازی برای رشد.

:اقدامات و مجوزهای موردنیاز *

#	اقدام / مجوز	نهاد صدورکننده	شرح و الزامات	زمان تخمینی	هزینه تخمینی (تومان)
۱/۱	اخذ "نشان اعتماد الکترونیک" (اینماد) – سطح یک یا دو**	مرکز توسعه تجارت الکترونیک	احراز هویت شرکت، شفافیت اطلاعات، داشتن سیاست‌های حریم خصوصی و بازپرداخت، امنیت نسبی سایت.	۳-۴ ماه	۵-۱۵ میلیون (متغیر)
۱/۲	ثبت سامانه در مرکز مدیریت آمار و فناوری اطلاعات سلامت وزارت بهداشت** (به عنوان یک "سرویس سلامت دیجیتال")	وزارت بهداشت	ارائه مستندات فنی، شرح خدمت، سیاست حریم خصوصی. بیشتر جنبه **اظهاری** دارد تا مجوزی. ضروری برای رسمیت بخشیدن و امکان همکاری آتی.	۲-۳ ماه	۲-۵ میلیون (هزینه‌های اداری و مشاوره)
۱/۳	انطباق با "آیین‌نامه حفاظت از داده‌های شخصی" (در صورت تصویب نهایی)**	مرکز ملی فضای مجازی / پلیس فتا	اجرای الزامات فنی و سازمانی حفاظت از داده (مطابق مستندات ۶/۲ و ۶/۶). ممکن است نیاز به **"اثبات انطباق"** داشته باشد.	۶ ماه (پیاده‌سازی)	۱۰-۳۰ میلیون (ارتقاء امنیت، ممیزی)

عقد تفاهم‌نامه یا رعایت "ضوابط تعامل با پزشکان"** | ** | ۱/۴ | سازمان نظام پزشکی (از طریق شعب استان) | رعایت مواردی مانند: عدم تعیین تعرفه توسط پلتفرم، عدم تبلیغات گمراه‌کننده، رعایت حریم رابطه پزشک-بیمار. اغلب نیاز به مذاکره و ارائه تعهدنامه دارد. | ۶-۳ | ماه | هزینه‌های اداری و مشاوره حقوقی تخصصی (۱۰-۵ میلیون)

اخذ مجوز ارسال پیامک انبوه (خدمات ارزش افزوده)** | ** | ۱/۵ | سازمان تنظیم مقررات (رگولاتوری) | برای ارسال یادآوری نوبت. نیاز به ثبت برند، ارائه شرح خدمت و همکاری با اپراتورهای دارای مجوز. | ۴-۲ ماه | هزینه‌های اشتراک سرویس با اپراتور (ماهانه) + هزینه‌های ثبت |

خروجی فاز ۱:** فعالیت با **پشتوانه رگولاتوری رسمی‌تر**، ** * امکان بازاریابی مطمئن‌تر به پزشکان، کاهش ریسک شکایت و توقف خدمات.

فاز ۲: انطباق پیشرفته و یکپارچه‌سازی (ماه ۱۳ تا ۲۴) ###

هدف:** تبدیل شدن به یک شریک معتبر برای کلینیک‌ها و ** * بیمارستان‌های بزرگ، توسعه ویژگی‌های پیشرفته و کاهش ریسک در مقیاس.

:اقدامات و مجوزهای موردنیاز *

اقدام / مجوز	نهاد صدورکننده	شرح و الزامات	زمان	#	تخمینی	هزینه تخمینی (تومان)
مثل) "اخذ "گواهی انطباق با استانداردهای امنیت اطلاعات**	۲٫۱	مؤسسه‌های صدور گواهی بین‌المللی/داخلی	اثبات	**(ISO 27001 قوی. **یک دارایی (ISMS) یک سیستم مدیریت امنیت اطلاعات ارزشمند برای جذب مشتریان سازمانی و سرمایه‌گذار.**	۹-۱۲ ماه	۱۵۰-۵۰ میلیون (مشاوره، پیاده‌سازی، ممیزی، صدور گواهی)
مانند) انطباق داوطلبانه با چارچوب‌های تخصصی سلامت**	۲٫۲	(اقدام داخلی)	حتی بدون -	**(به عنوان چارچوب مرجع HIPAA الزام قانونی در ایران، پیاده‌سازی کنترل‌های امنیتی و حریم خصوصی ، یک **مزیت رقابتی بزرگ و نشان‌دهنده تعهد فوق‌العاده** HIPAA است.	۶-۹ ماه	۸۰-۳۰ میلیون (مطالعه، پیاده‌سازی کنترل‌ها، آموزش)
کسب مجوز یا تفاهم‌نامه برای "یکپارچه‌سازی با **	۲٫۳	وزارت بهداشت / دانشگاه‌های علوم پزشکی / بیمارستان‌ها	برای ارتباط مستقیم با نوبت‌دهی داخلی بیمارستان. نیازمند **تست و تأیید فنی و امنیتی** توسط نهاد طرف	**"(HIS) سامانه‌های بیمارستانی		

قرارداد. بسیار پروژه‌محور است. | ۱۲-۶ ماه به ازای هر پروژه | بسیار | متغیر (۵۰۰-۱۰۰ میلیون بسته به پروژه)

عضویت در "انجمن سلامت دیجیتال ایران" یا نهادهای ** | ۲/۴ | مشابه** | انجمن‌های صنفی | شبکه‌سازی، تاثیرگذاری بر سیاست‌گذاری‌های آتی، تبادل دانش. | ۲-۱ ماه | هزینه‌های عضویت | سالانه (ناچیز)

خروجی فاز ۲:** موقعیت **رهبر بازار در بخش سلامت ** * دیجیتال ایران** از نظر اعتماد و انطباق، امکان عقد قراردادهای بزرگ ،. افزایش چشمگیر ارزش شرکتB2B

فاز ۳: آماده‌سازی برای توسعه بین‌المللی و مقررات آینده (ماه ** ### **۲۵ به بعد)

هدف:** ورود به بازارهای منطقه‌ای (مانند کشورهای عربی ** * .همسایه) و آمادگی برای سخت‌گیری احتمالی مقررات داخلی

:اقدامات *

مثلاً) **مطالعه دقیق مقررات سلامت دیجیتال بازار هدف** * .(در عربستان SFDAدر دبی، DHA

ISO 27799 اخذ گواهی‌های بین‌المللی معتبر** مانند** * .(امنیت اطلاعات در سلامت

* **طراحی معماری چنداجاره‌ای** (Multi-tenant) با قابلیت تطبیق محل ذخیره‌سازی داده** بر اساس قانون کشور میزبان.

* **همکاری با وکلای محلی** در بازار هدف**.

6.7.۴ استانداردهای فنی و امنیتی قابل اجرا (صفحه ۲۵-۲۳)

صرف نظر از مجوزهای اداری، رعایت استانداردهای فنی، سنگ بنای انطباق است.

استاندارد / چارچوب	حوزه	کاربرد برای نوبت‌نو	سطح بلوغ	هدف
ISO 27001:2022	مدیریت امنیت اطلاعات (ISMS)	استاندارد طلایی.** چارچوبی برای شناسایی، ارزیابی و مدیریت ** ریسک‌های امنیتی اطلاعات.	فاز ۲

| **NIST Cybersecurity Framework (CSF)** |
چارچوب امنیت سایبری | چارچوبی ساختاریافته (تشخیص، حفاظت، شناسایی، پاسخ، بازیابی) برای تقویت وضعیت امنیتی. | از فاز ۱ (به عنوان راهنما) |

| **OWASP Top 10** | امنیت برنامه‌های وب | کنترل‌های XSS، SQL تزریق) فنی برای جلوگیری از رایج‌ترین آسیب‌پذیری‌ها | فاز ۰ و ۱ (اجباری) | .(...و

| **HIPAA Security & Privacy Rules** (به عنوان Best Practice) | امنیت و حریم خصوصی داده سلامت در آمریکا | **مرجع عملیاتی عالی.** کنترل‌های فیزیکی، فنی و اداری دقیق برای محافظت از داده سلامت (PHI). | از فاز ۱ (تدریجی) تا فاز ۲ (کامل) |

| **وزارت بهداشت** سند "الزامات امنیتی سامانه‌های سلامت دیجیتال" (در صورت انتشار) | امنیت سامانه‌های سلامت داخلی | الزامات اجباری آینده. باید از هم‌اکنون رصد شود. | به محض انتشار |

6.7.۵ تحلیل ریسک‌های رگولاتوری و راهکارهای کاهش
**(صفحه ۲۸-۲۶)

ریسک	احتمال	تاثیر	راهکار کاهش (Mitigation)
تغییر ناگهانی یا سخت‌گیری مقررات داخلی** (مثلاً الزام اخذ ** مجوز سخت‌گیرانه برای تمام سرویس‌های سلامت دیجیتال)	متوسط	بالا (توقف موقت خدمات، هزینه انطباق فوری)	**فعالیت شبکه‌ای:** عضویت در انجمن‌ها، رصد مستمر اخبار وزارت بهداشت و مرکز ملی فضای مجازی. **طراحی چابک:** معماری نرم‌افزاری که امکان اعمال تغییرات امنیتی و منطقی را سریع فراهم کند.
اعلام غیرقانونی بودن مدل کسب‌وکار توسط یک نهاد** (مثلاً ** سازمان نظام پزشکی نسبت به دریافت هرگونه کارمزد از پزشکان معترض شود)	پایین	بسیار بالا (نابودی کسب‌وکار)	**شفافیت و مشاوره پیش‌دستانه:** ارائه مدل کسب‌وکار و دریافت نظر رسمی (حتی غیرالزام‌آور) از سازمان نظام پزشکی در فاز ۱. **تنوع درآمدی:** عدم وابستگی کامل به کارمزد از پزشکان (توسعه درآمد از تبلیغات هدفمند یا خدمات ارزش افزوده به بیماران).
رخداد یک حادثه امنیتی بزرگ (نقض داده)**	متوسط	بسیار ** بالا (جریمه‌های سنگین، از دست دادن کامل اعتماد، دعاوی قضایی)	**سرمایه‌گذاری پیشگیرانه در امنیت:** اجرای استانداردهای ISO 27001 و کنترل‌های OWASP از همان ابتدا. **اخذ بیمه سایبری

در فاز ۲ برای انتقال بخشی **:(Cyber Liability Insurance)
| .از ریسک مالی

عدم امکان یکپارچه‌سازی با سیستم‌های دولتی به دلیل ** |
محدود شدن رشد در بخش) استانداردهای انحصاری** | بالا | متوسط
و B2C تمرکز اولیه بر بازار** | (و بیمارستان‌های بزرگ B2G
های باز و استاندارد. مشارکت در API مطب‌های خصوصی.** توسعه
| .کمیته‌های تدوین استاندارد در بلندمدت

اخذ مجوزهای بین‌المللی برای صادرات خدمات، پرهزینه و ** |
زمان‌بر باشد** | بالا | متوسط (کند شدن سرعت توسعه بین‌المللی) |
انتخاب بازارهای هدف با مقررات شفاف‌تر و همسوتر (مثلاً امارات
| .پیش از اتحادیه اروپا). همکاری با شریک محلی در بازار هدف

برآورد منابع (هزینه و زمان) و نقشه راه گانت (صفحه ۶.۷.۶** ##
**۲۹-۳۰)

برآورد هزینه کل انطباق (فاز ۱ و ۲):** **۱۵۰ - ۳۰۰ میلیون ** *
تومان** (بدون احتساب هزینه‌های عملیاتی مستمر مثل بیمه سایبری یا
.ممیزی‌های دوره‌ای)

نیروی انسانی موردنیاز:** استخدام یا برون‌سپاری یک **مسئول ** *
**(Compliance & Security Officer) انطباق و امنیت
.نیمه‌وقت در فاز ۱ و تمام‌وقت در فاز ۲

:نقشه راه گانت (خلاصه) *

اخذ اینماد، ثبت در وزارت بهداشت، **:1403 Q1-Q2** *
.آغاز مذاکره با نظام پزشکی

پیاده‌سازی چارچوب امنیتی مبتنی بر **:1403 Q3-Q4** *
.، اخذ مجوز پیامکNIST/OWASP

، مطالعه و ISO 27001 آغاز پروژه اخذ **:1404** *
.به عنوان بهترین روش HIPAA پیاده‌سازی کنترل‌های

، آغاز اولین پروژه ISO 27001 تکمیل **:1405** *
.یکپارچه‌سازی با یک بیمارستان منتخب

جمع‌بندی و توصیه اجرایی (صفحه ۳۱) ۶.۷.۷ ##

مسیر رگولاتوری برای نوبت‌نو اگرچه چالشی است، اما **یک ضرورت
استراتژیک و در واقع یک "مزیت رقابتی قابل ساخت"** محسوب

می‌شود. در بازار آشفته سلامت دیجیتال ایران، شرکتی که زودتر و جدی‌تر این مسیر را بپیماید، به **تنها بازیگر معتبر و قابل اعتماد** برای پزشکان، بیمارستان‌ها و سرمایه‌گذاران تبدیل خواهد شد.

توصیه فوری برای جذب سرمایه:** برنامه فاز ۱ (به ویژه اخذ اینماد ** و ثبت در وزارت بهداشت) باید به عنوان **یکی از اهداف کلیدی دور اول سرمایه‌گذاری** تعریف شود و بودجه و (Milestones) زمان لازم برای آن در نظر گرفته شود. این نشان می‌دهد تیم بنیانگذار نه تنها به فناوری، بلکه به **پایداری و مقیاس‌پذیری قانونی کسب‌وکار** می‌اندیشد.

[امضای مدیرعامل و مسئول انطباق آینده]

[مهر شرکت]

تاریخ: ۲۰/۰۲/۱۴۰۳
