



كلية الطب
والصيدلة - مراكش
FACULTÉ DE MÉDECINE
ET DE PHARMACIE - MARRAKECH

Année 2026

Thèse N°87

Digitalisation des données médicales: entre éthique et sécurité

THÈSE

PRÉSENTÉE ET SOUTENUE PUBLIQUEMENT LE : 06/02/2026

PAR

Mlle.Lamyae BOUSSIRI

Née le 16/02/2000 À Béni Mellal

POUR L'OBTENTION DU DOCTORAT EN MÉDECINE

MOTS-CLÉS :

Digitalisation – Données médicales – Éthique – Cybersécurité – Loi 09-08

JURY

Mr. **M. ZYANI**

Professeur de Médecine Interne

PRESIDENT

Mr. **A. RAISSI**

Professeur d' Hématologie clinique

RAPPOTEUR

Mr. **Y. QAMOUSS**

Professeur d' Anesthésie Réanimation

Mr. **I. ESSÂDI**

Professeur d'Oncologie médicale

JUGES

يُؤْتِي الْحِكْمَةَ مَنْ يَشَاءُ وَمَنْ يُؤْتَ الْحِكْمَةَ فَقَدْ أُوتِيَ خَيْرًا كَثِيرًا



سورة المائدة : الآية ٢٦٩

« Dieu accorde la sagesse à qui Il veut, et celui à qui la sagesse est
accordée a certes reçu un immense bien. »

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ الرَّحْمَنِ الرَّحِيمِ

مَالِكِ يَوْمِ الدِّينِ إِيَّاكَ نَعْبُدُ وَإِيَّاكَ

نَسْتَعِينُ اهْدِنَا الصِّرَاطَ الْمُسْتَقِيمَ

صِرَاطَ الَّذِينَ أَنْعَمْتَ عَلَيْهِمْ غَيْرِ

الْمَغْضُوبِ عَلَيْهِمْ وَلَا الضَّالِّينَ

سُورَةُ الْفَاتِحَةِ

وَقَدْ كَلَّمَكَ



Serment d'Hippocrate

Au moment d'être admis à devenir membre de la profession médicale, je m'engage solennellement à consacrer ma vie au service de l'humanité.

*Je traiterai mes maîtres avec le respect et la reconnaissance
qui leur sont dus.*

Je pratiquerai ma profession avec conscience et dignité. La santé de mes malades sera mon premier but.

*Je ne trahirai pas les secrets qui me seront confiés.
Je maintiendrai par tous les moyens en mon pouvoir l'honneur et les nobles traditions de la profession médicale.*

Les médecins seront mes frères.

Aucune considération de religion, de nationalité, de race, aucune considération politique et sociale, ne s'interposera entre mon devoir et mon patient.

Je maintiendrai strictement le respect de la vie humaine dès sa conception. Même sous la menace, je n'userai pas mes connaissances médicales d'une façon contraire aux lois de l'humanité.

Je m'y engage librement et sur mon honneur.

Déclaration Genève, 1948





LISTE DES PROFESSEURS



UNIVERSITE CADI AYYAD
FACULTE DE MEDECINE ET DE PHARMACIE
MARRAKECH

Doyens Honoraires

: Pr. Badie Azzaman MEHADJI

: Pr. Abdelhaq ALAOUI YAZIDI

: Pr. Mohammed BOUSKRAOUI

ADMINISTRATION

Doyen

: Pr. Said ZOUHAIR

Vice doyen de la Recherche et la Coopération

: Pr. Mohamed AMINE

Vice doyen des Affaires Pédagogiques

: Pr. Redouane EL FEZZAZI

Vice doyen Chargé de la Pharmacie

: Pr. Oualid ZIRAOUI

Secrétaire Générale

: Mr. Azzeddine EL HOUDAIGUI

LISTE NOMINATIVE DU PERSONNEL ENSEIGNANTS CHERCHEURS PERMANANT

N°	Nom et Prénom	Cadre	Spécialités
01	ZOUHAIR Said (Doyen)	P.E.S	Microbiologie
02	CHOULLI Mohamed Khaled	P.E.S	Neuro pharmacologie
03	BOUSKRAOUI Mohammed	P.E.S	Pédiatrie
04	KHATOURI Ali	P.E.S	Cardiologie
05	NIAMANE Radouane	P.E.S	Rhumatologie
06	AIT BENALI Said	P.E.S	Neurochirurgie
07	KRATI Khadija	P.E.S	Gastro-entérologie
08	SOUMMANI Abderraouf	P.E.S	Gynécologie-obstétrique
09	RAJI Abdelaziz	P.E.S	Oto-rhino-laryngologie
10	SARF Ismail	P.E.S	Urologie
11	MOUTAOUAKIL Abdeljalil	P.E.S	Ophtalmologie
12	AMAL Said	P.E.S	Dermatologie
13	ESSAADOUNI Lamiaa	P.E.S	Médecine interne
14	MANSOURI Nadia	P.E.S	Stomatologie et chirurgie maxillo faciale
15	MOUTAJ Redouane	P.E.S	Parasitologie

16	AMMAR Haddou	P.E.S	Oto-rhino-laryngologie
17	CHAKOUR Mohammed	P.E.S	Hématologie biologique
18	EL FEZZAZI Redouane	P.E.S	Chirurgie pédiatrique
19	YOUNOUS Said	P.E.S	Anesthésie-réanimation
20	BENELKHAIAT BENOMAR Ridouan	P.E.S	Chirurgie générale
21	ASMOUKI Hamid	P.E.S	Gynécologie-obstétrique
22	BOUMZEBRA Drissi	P.E.S	Chirurgie Cardio-vasculaire
23	CHELLAK Saliha	P.E.S	Biochimie-chimie
24	LOUZI Abdelouahed	P.E.S	Chirurgie-générale
25	AIT-SAB Imane	P.E.S	Pédiatrie
26	GHANNANE Houssine	P.E.S	Neurochirurgie
27	OULAD SAIAD Mohamed	P.E.S	Chirurgie pédiatrique
28	DAHAMI Zakaria	P.E.S	Urologie
29	EL HATTAOUI Mustapha	P.E.S	Cardiologie
30	AMINE Mohamed	P.E.S	Epidémiologie clinique
31	EL ADIB Ahmed Rhassane	P.E.S	Anesthésie-réanimation
32	ELFIKRI Abdelghani	P.E.S	Radiologie
33	ARSALANE Lamiae	P.E.S	Microbiologie-virologie
34	KAMILI El Ouafi El Aouni	P.E.S	Chirurgie pédiatrique
35	MAOULAININE Fadl mrabih rabou	P.E.S	Pédiatrie (Néonatalogie)
36	MATRANE Aboubakr	P.E.S	Médecine nucléaire
37	ADMOU Brahim	P.E.S	Immunologie
38	CHERIF IDRISSE EL GANOUNI Najat	P.E.S	Radiologie
39	MANOUDI Fatiha	P.E.S	Psychiatrie
40	BOURROUS Monir	P.E.S	Pédiatrie
41	TASSI Noura	P.E.S	Maladies infectieuses
42	NEJMI Hicham	P.E.S	Anesthésie-réanimation
43	LAOUAD Inass	P.E.S	Néphrologie
44	FOURAJI Karima	P.E.S	Chirurgie
45	BOUKHIRA Abderrahman	P.E.S	Biochimie-chimie
46	KHALLOUKI Mohammed	P.E.S	Anesthésie-réanimation
47	BSISS Mohammed Aziz	P.E.S	Biophysique
48	EL OMRANI Abdelhamid	P.E.S	Radiothérapie

49	SORAA Nabila	P.E.S	Microbiologie–virologie
50	KHOUCHANI Mouna	P.E.S	Radiothérapie
51	JALAL Hicham	P.E.S	Radiologie
52	EL ANSARI Nawal	P.E.S	Endocrinologie et maladies métaboliques
53	AMRO Lamyae	P.E.S	Pneumo–phtisiologie
54	OUALI IDRISSE Mariem	P.E.S	Radiologie
55	ZAHLANE Mouna	P.E.S	Médecine interne
56	BENJILALI Laila	P.E.S	Médecine interne
57	NARJIS Youssef	P.E.S	Chirurgie générale
58	RABBANI Khalid	P.E.S	Chirurgie générale
59	SAMLANI Zouhour	P.E.S	Gastro–entérologie
60	LAGHMARI Mehdi	P.E.S	Neurochirurgie
61	ABOUSSAIR Nisrine	P.E.S	Génétique
62	BENCHAMKHA Yassine	P.E.S	Chirurgie réparatrice et plastique
63	CHAFIK Rachid	P.E.S	Traumato–orthopédie
64	ABKARI Imad	P.E.S	Traumato–orthopédie
65	EL BOUIHI Mohamed	P.E.S	Stomatologie et chirurgie maxillo faciale
66	LAKMICHI Mohamed Amine	P.E.S	Urologie
67	AGHOUTANE El Mouhtadi	P.E.S	Chirurgie pédiatrique
68	HOCAR Ouafa	P.E.S	Dermatologie
69	EL KARIMI Saloua	P.E.S	Cardiologie
70	EL BOUCHTI Imane	P.E.S	Rhumatologie
71	QAMOUISS Youssef	P.E.S	Anésthésie réanimation
72	ZYANI Mohammad	P.E.S	Médecine interne
73	QACIF Hassan	P.E.S	Médecine interne
74	BEN DRISS Laila	P.E.S	Cardiologie
75	MOUFID Kamal	P.E.S	Urologie
76	EL BARNI Rachid	P.E.S	Chirurgie générale
77	KRIET Mohamed	P.E.S	Ophtalmologie
78	BOUCHENTOUF Rachid	P.E.S	Pneumo–phtisiologie
79	ABOUCHADI Abdeljalil	P.E.S	Stomatologie et chirurgie maxillo faciale
80	BASRAOUI Dounia	P.E.S	Radiologie
81	RAIS Hanane	P.E.S	Anatomie Pathologique

82	BELKHOU Ahlam	P.E.S	Rhumatologie
83	ZAOUI Sanaa	P.E.S	Pharmacologie
84	MSOUGAR Yassine	P.E.S	Chirurgie thoracique
85	EL MGHARI TABIB Ghizlane	P.E.S	Endocrinologie et maladies métaboliques
86	DRAISS Ghizlane	P.E.S	Pédiatrie
87	EL IDRISSE SLITINE Nadia	P.E.S	Pédiatrie
88	RADA Noureddine	P.E.S	Pédiatrie
89	BOURRAHOUAT Aicha	P.E.S	Pédiatrie
90	MOUAFFAK Youssef	P.E.S	Anesthésie-réanimation
91	ZIADI Amra	P.E.S	Anesthésie-réanimation
92	ANIBA Khalid	P.E.S	Neurochirurgie
93	TAZI Mohamed Illias	P.E.S	Hématologie clinique
94	ROCHDI Youssef	P.E.S	Oto-rhino-laryngologie
95	FADILI Wafaa	P.E.S	Néphrologie
96	ADALI Imane	P.E.S	Psychiatrie
97	ZAHLANE Kawtar	P.E.S	Microbiologie- virologie
98	LOUHAB Nisrine	P.E.S	Neurologie
99	HAROU Karam	P.E.S	Gynécologie-obstétrique
100	BOUKHANNI Lahcen	P.E.S	Gynécologie-obstétrique
101	FAKHIR Bouchra	P.E.S	Gynécologie-obstétrique
102	BENHIMA Mohamed Amine	P.E.S	Traumatologie-orthopédie
103	HACHIMI Abdelhamid	P.E.S	Réanimation médicale
104	EL KHAYARI Mina	P.E.S	Réanimation médicale
105	AISSAOUI Younes	P.E.S	Anesthésie-réanimation
106	BAIZRI Hicham	P.E.S	Endocrinologie et maladies métaboliques
107	ATMANE El Mehdi	P.E.S	Radiologie
108	EL AMRANI Moulay Driss	P.E.S	Anatomie
109	BELBARAKA Rhizlane	P.E.S	Oncologie médicale
110	ALJ Soumaya	P.E.S	Radiologie
111	OUBAHA Sofia	P.E.S	Physiologie
112	EL HAOUATI Rachid	P.E.S	Chirurgie Cardio-vasculaire
113	BENALI Abdeslam	P.E.S	Psychiatrie
114	MLIHA TOUATI Mohammed	P.E.S	Oto-rhino-laryngologie

115	MARGAD Omar	P.E.S	Traumatologie–orthopédie
116	KADDOURI Said	P.E.S	Médecine interne
117	ZEMRAOUI Nadir	P.E.S	Néphrologie
118	EL KHADER Ahmed	P.E.S	Chirurgie générale
119	DAROUASSI Youssef	P.E.S	Oto–rhino–laryngologie
120	BENJELLOUN HARZIMI Amine	P.E.S	Pneumo–phtisiologie
121	FAKHRI Anass	P.E.S	Histologie–embyologie cytogénétique
122	SALAMA Tarik	P.E.S	Chirurgie pédiatrique
123	CHRAA Mohamed	P.E.S	Physiologie
124	ZARROUKI Youssef	P.E.S	Anesthésie–réanimation
125	AIT BATAHAR Salma	P.E.S	Pneumo–phtisiologie
126	ADARMOUCH Latifa	P.E.S	Médecine communautaire (médecine préventive, santé publique et hygiène)
127	BELBACHIR Anass	P.E.S	Anatomie pathologique
128	HAZMIRI Fatima Ezzahra	P.E.S	Histologie–embyologie cytogénétique
129	EL KAMOUNI Youssef	P.E.S	Microbiologie–virologie
130	EL MEZOUARI El Mostafa	P.E.S	Parasitologie mycologie
131	SERGHINI Issam	P.E.S	Anesthésie–réanimation
132	ABIR Badreddine	P.E.S	Stomatologie et chirurgie maxillo faciale
133	GHAZI Mirieme	P.E.S	Rhumatologie
134	ZIDANE Moulay Abdelfettah	P.E.S	Chirurgie thoracique
135	LAHKIM Mohammed	P.E.S	Chirurgie générale
136	MOUHSINE Abdelilah	P.E.S	Radiologie
137	TOURABI Khalid	P.E.S	Chirurgie réparatrice et plastique
138	ARABI Hafid	P.E.S	Médecine physique et réadaptation fonctionnelle
139	BELHADJ Ayoub	P.E.S	Anesthésie–réanimation
140	BOUZERDA Abdelmajid	P.E.S	Cardiologie
141	ABDELFETTAH Youness	P.E.S	Rééducation et réhabilitation fonctionnelle
142	REBAHI Houssam	P.E.S	Anesthésie–réanimation
143	BENNAOUI Fatiha	P.E.S	Pédiatrie
144	ZOUIZRA Zahira	P.E.S	Chirurgie Cardio–vasculaire

145	SEBBANI Majda	P.E.S	Médecine Communautaire (Médecine préventive, santé publique et hygiène)
146	FENANE Hicham	Pr Ag	Chirurgie thoracique
147	ABDOU Abdessamad	P.E.S	Chirurgie Cardio-vasculaire
148	HAMMOUNE Nabil	P.E.S	Radiologie
149	ESSADI Ismail	P.E.S	Oncologie médicale
150	ALJALIL Abdelfattah	P.E.S	Oto-rhino-laryngologie
151	LAFFINTI Mahmoud Amine	P.E.S	Psychiatrie
152	RHARRASSI Issam	P.E.S	Anatomie-pathologique
153	ASSERRAJI Mohammed	P.E.S	Néphrologie
154	JANAH Hicham	P.E.S	Pneumo-phthisiologie
155	NASSIM SABAH Taoufik	P.E.S	Chirurgie réparatrice et plastique
156	ELBAZ Meriem	P.E.S	Pédiatrie
157	SEDDIKI Rachid	P.E.S	Anesthésie-réanimation
158	BELGHMAIDI Sarah	Pr Ag	Ophtalmologie
159	GEBRATI Lhoucine	MC Hab	Chimie
160	FDIL Naima	MC Hab	Chimie de coordination bio-organique
161	LOQMAN Souad	MC Hab	Microbiologie et Toxicologie
162	BAALLAL Hassan	Pr Ag	Neurochirurgie
163	BELFQUIH Hatim	Pr Ag	Neurochirurgie
164	AKKA Rachid	Pr Ag	Gastro-entérologie
165	BABA Hicham	Pr Ag	Chirurgie générale
166	MAOUJOUD Omar	Pr Ag	Néphrologie
167	SIRBOU Rachid	Pr Ag	Médecine d'urgence et de catastrophe
168	DAMI Abdallah	Pr Ag	Médecine Légale
169	AZIZ Zakaria	Pr Ag	Stomatologie et chirurgie maxillo faciale
170	ELOUARDI Youssef	Pr Ag	Anesthésie-réanimation
171	LAHLIMI Fatima Ezzahra	Pr Ag	Hématologie clinique
172	NASSIH Houda	Pr Ag	Pédiatrie
173	LAHMINI Widad	Pr Ag	Pédiatrie
174	BENANTAR Lamia	Pr Ag	Neurochirurgie
175	EL FADLI Mohammed	Pr Ag	Oncologie médicale
176	AIT ERRAMI Adil	Pr Ag	Gastro-entérologie

177	CHETTATI Mariam	Pr Ag	Néphrologie
178	BOUTAKIOUTE Badr	Pr Ag	Radiologie
179	SAYAGH Sanae	Pr Ag	Hématologie
180	EL FAKIRI Karima	Pr Ag	Pédiatrie
181	EL FILALI Oualid	Pr Ag	Chirurgie Vasculaire périphérique
182	EL- AKHIRI Mohammed	Pr Ag	Oto-rhino-laryngologie
183	HAJJI Fouad	Pr Ag	Urologie
184	JALLAL Hamid	Pr Ag	Cardiologie
185	ZBITOU Mohamed Anas	Pr Ag	Cardiologie
186	RAISSI Abderrahim	Pr Ag	Hématologie clinique
187	EL HAKKOUNI Awatif	Pr Ag	Parasitologie mycologie
188	ACHKOUN Abdessalam	Pr Ag	Anatomie
189	DARFAOUI Mouna	Pr Ag	Radiothérapie
190	EL-QADIRY Rabiyy	Pr Ag	Pédiatrie
191	ELJAMILI Mohammed	Pr Ag	Cardiologie
192	HAMRI Asma	Pr Ag	Chirurgie Générale
193	ELATIQI Oumkeltoum	Pr Ag	Chirurgie réparatrice et plastique
194	BENZALIM Meriam	Pr Ag	Radiologie
195	ABOULMAKARIM Siham	Pr Ag	Biochimie
196	LAMRANI HANCHI Asmae	Pr Ag	Microbiologie-virologie
197	HAJHOUI Farouk	Pr Ag	Neurochirurgie
198	EL KHASSOUI Amine	Pr Ag	Chirurgie pédiatrique
199	CHAHBI Zakaria	Pr Ag	Maladies infectieuses
200	MEFTAH Azzelarab	Pr Ag	Endocrinologie et maladies métaboliques
201	BELLASRI Salah	Pr Ag	Radiologie
202	ATMANI Nouredine	Pr Ag	Chirurgie Cardio-vasculaire
203	AABBASSI Bouchra	Pr Ag	Pédopsychiatrie
204	DOUIREK Fouzia	Pr Ag	Anesthésie-réanimation
205	SAHRAOUI Houssam Eddine	Pr Ag	Anesthésie-réanimation
206	RHEZALI Manal	Pr Ag	Anesthésie-réanimation
207	ABALLA Najoua	Pr Ag	Chirurgie pédiatrique
208	MOUGUI Ahmed	Pr Ag	Rhumatologie
209	ZOUITA Btissam	Pr Ag	Radiologie

210	HAZIME Raja	Pr Ag	Immunologie
211	SALLAHI Hicham	Pr Ag	Traumatologie–orthopédie
212	BENCHAFAI Ilias	Pr Ag	Oto–rhino–laryngologie
213	EL JADI Hamza	Pr Ag	Endocrinologie et maladies métaboliques
214	AZAMI Mohamed Amine	Pr Ag	Anatomie pathologique
215	FASSI FIHRI Mohamed jawad	Pr Ag	Chirurgie générale
216	AMINE Abdellah	Pr Ag	Cardiologie
217	CHETOUI Abdelkhalek	Pr Ag	Cardiologie
218	ROUKHSI Redouane	Pr Ag	Radiologie
219	ARROB Adil	Pr Ag	Chirurgie réparatrice et plastique
220	MOULINE Souhail	Pr Ag	Microbiologie–virologie
221	AZIZI Mounia	Pr Ag	Néphrologie
222	BOUHAMIDI Ahmed	Pr Ag	Dermatologie
223	YANISSE Siham	Pr Ag	Pharmacie galénique
224	KHALLIKANE Said	Pr Ag	Anesthésie–réanimation
225	ZIRAOUI Oualid	Pr Ag	Chimie thérapeutique
226	IDALENE Malika	Pr Ag	Maladies infectieuses
227	LACHHAB Zineb	Pr Ag	Pharmacognosie
228	ABOUDOURIB Maryem	Pr Ag	Dermatologie
229	AHBALA Tariq	Pr Ag	Chirurgie générale
230	EL AOUAME Amal	Pr Ag	Orthodontie et orthopédie dento–faciale
231	WARDA Karima	MCHab	Microbiologie
232	SBAI Asma	MCHab	Informatique
233	ABISSY Meriem	MC	Microbiologie
234	SLIOUI Badr	MC	Radiologie
235	CHEGGOUR Mouna	MC	Biochimie
236	BELARBI Marouane	MC	Néphrologie
237	EL AMIRI My Ahmed	MC	Chimie de Coordination bio–organnique
238	LALAOUI Abdessamad	MC	Pédiatrie
239	ESSAFTI Meryem	MC	Anesthésie–réanimation
240	RACHIDI Hind	MC	Anatomie pathologique
241	FIKRI Oussama	MC	Pneumo–phtisiologie
242	EL HAMDAOUI Omar	MC	Toxicologie

243	EL HAJJAMI Ayoub	MC	Radiologie
244	BOUMEDIANE El Mehdi	MC	Traumato-orthopédie
245	RAFI Sana	MC	Endocrinologie et maladies métaboliques
246	JEBRANE Ilham	MC	Pharmacologie
247	LAKHDAR Youssef	MC	Oto-rhino-laryngologie
248	LGHABI Majida	MC	Médecine du Travail
249	AIT LHAJ El Houssaine	MC	Ophtalmologie
250	RAMRAOUI Mohammed-Es-said	MC	Chirurgie générale
251	EL MOUHAFID Faisal	MC	Chirurgie générale
252	AHMANNNA Hussein-choukri	MC	Radiologie
253	AIT M'BAREK Yassine	MC	Neurochirurgie
254	ELMASRIOUI Joumana	MC	Physiologie
255	FOURA Salma	MC	Chirurgie pédiatrique
256	LASRI Najat	MC	Hématologie clinique
257	BOUKTIB Youssef	MC	Radiologie
258	MOUROUTH Hanane	MC	Anesthésie-réanimation
259	BOUZID Fatima zahrae	MC	Génétique
260	MRHAR Soumia	MC	Pédiatrie
261	QUIDDI Wafa	MC	Hématologie
262	BEN HOUMICH Taoufik	MC	Microbiologie-virologie
263	FETOUI Imane	MC	Pédiatrie
264	FATH EL KHIR Yassine	MC	Traumato-orthopédie
265	NASSIRI Mohamed	MC	Traumato-orthopédie
266	AIT-DRISS Wiam	MC	Maladies infectieuses
267	AIT YAHYA Abdelkarim	MC	Cardiologie
268	DIANI Abdelwahed	MC	Radiologie
269	AIT BELAID Wafae	MC	Chirurgie générale
270	ZTATI Mohamed	MC	Cardiologie
271	HAMOUCHE Nabil	MC	Néphrologie
272	ELMARDOULI Mouhcine	MC	Chirurgie Cardio-vasculaire
273	BENNIS Lamiae	MC	Anesthésie-réanimation
274	BENDAOUD Layla	MC	Dermatologie
275	HABBAB Adil	MC	Chirurgie générale

276	CHATAR Achraf	MC	Urologie
277	OUMGHAR Nezha	MC	Biophysique
278	HOUMAID Hanane	MC	Gynécologie-obstétrique
279	YOUSFI Jaouad	MC	Gériatrie
280	NACIR Oussama	MC	Gastro-entérologie
281	BABACHEIKH Safia	MC	Gynécologie-obstétrique
282	ABDOURAFIQ Hasna	MC	Anatomie
283	TAMOUR Hicham	MC	Anatomie
284	IRAQI HOUSSAINI Kawtar	MC	Gynécologie-obstétrique
285	EL FAHIRI Fatima Zahrae	MC	Psychiatrie
286	BOUKIND Samira	MC	Anatomie
287	LOUKHNATI Mehdi	MC	Hématologie clinique
288	ZAHROU Farid	MC	Neurochirurgie
289	MAAROUFI Fathillah Elkarim	MC	Chirurgie générale
290	EL MOUSSAOUI Soufiane	MC	Pédiatrie
291	BARKICHE Samir	MC	Radiothérapie
292	ABI EL AALA Khalid	MC	Pédiatrie
293	AFANI Leila	MC	Oncologie médicale
294	EL MOULOUA Ahmed	MC	Chirurgie pédiatrique
295	LAGRINE Mariam	MC	Pédiatrie
296	DAFIR Kenza	MC	Génétique
297	CHERKAOUI RHAZOUANI Oussama	MC	Neurologie
298	ABAINOU Lahoussaine	MC	Endocrinologie et maladies métaboliques
299	BENCHANNA Rachid	MC	Pneumo-phtisiologie
300	EL GUAZZAR Ahmed (Militaire)	MC	Chirurgie générale
301	OULGHOUL Omar	MC	Oto-rhino-laryngologie
302	AMOCH Abdelaziz	MC	Urologie
303	ZAHLAN Safaa	MC	Neurologie
304	EL MAHFOUDI Aziz	MC	Gynécologie-obstétrique
305	CHEHBOUNI Mohamed	MC	Oto-rhino-laryngologie
306	LAIRANI Fatima ezzahra	MC	Gastro-entérologie
307	SAADI Khadija	MC	Pédiatrie
308	TITOU Hicham	MC	Dermatologie

309	EL GHOUL Naoufal	MC	Traumato-orthopédie
310	BAHI Mohammed	MC	Anesthésie-réanimation
311	RAITEB Mohammed	MC	Maladies infectieuses
312	DREF Maria	MC	Anatomie pathologique
313	ENNACIRI Zainab	MC	Psychiatrie
314	BOUSSAIDANE Mohammed	MC	Traumato-orthopédie
315	JENDOUI Omar	MC	Urologie
316	MANSOURI Maria	MC	Génétique
317	ERRIFAIY Hayate	MC	Anesthésie-réanimation
318	BOUKOUB Naila	MC	Anesthésie-réanimation
319	OUACHAOU Jamal	MC	Anesthésie-réanimation
320	EL FARGANI Rania	MC	Maladies infectieuses
321	IJIM Mohamed	MC	Pneumo-phtisiologie
322	AKANOUR Adil	MC	Psychiatrie
323	ELHANAFI Fatima Ezzohra	MC	Pédiatrie
324	MERBOUH Manal	MC	Anesthésie-réanimation
325	BOUROUMANE Mohamed Rida	MC	Anatomie
326	IJDDA Sara	MC	Endocrinologie et maladies métaboliques
327	GHARBI Khalid	MC	Gastro-entérologie
328	ATBIB Yassine	MC	Pharmacie clinique
329	MOURAFIQ Omar	MC	Traumato-orthopédie
330	ZAIZI Abderrahim	MC	Traumato-orthopédie
331	HENDY Iliass	MC	Cardiologie
332	HATTAB Mohamed Salah Koussay	MC	Stomatologie et chirurgie maxillo faciale
333	DEBBAGH Fayrouz	MC	Microbiologie-virologie
334	OUASSIL Sara	MC	Radiologie
335	KOUYED Aicha	MC	Pédopsychiatrie
336	DRIOUICH Aicha	MC	Anesthésie-réanimation
337	TOURAIF Mariem	MC	Chirurgie pédiatrique
338	BENNAOUI Yassine	MC	Stomatologie et chirurgie maxillo faciale
339	SABIR Es-said	MC	Chimie bio organique clinique
340	LAATITIOUI Sana	MC	Radiothérapie

341	IBBA Mouhsin	MC	Chirurgie thoracique
342	SAADOUNE Mohamed	MC	Radiothérapie
343	TLEMCANI Younes	MC	Ophtalmologie
344	SOLEH Abdelwahed	MC	Traumato-orthopédie
345	OUALHADJ Hamza	MC	Immunologie
346	BERGHALOUT Mohamed	MC	Psychiatrie
347	EL BARAKA Soumaya	MC	Chimie analytique-bromatologie
348	KARROUMI Saadia	MC	Psychiatrie
349	EL-OUAKHOUMI Amal	MC	Médecine interne
350	AJMANI Fatima	MC	Médecine légale
351	ZOUITEN Othmane	MC	Oncologie médicale
352	MENJEL Imane	MC	Pédiatrie
353	BOUCHKARA Wafae	MC	Gynécologie-obstétrique
354	ASSEM Oualid	MC	Pédiatrie
355	ELHANAFI Asma	MC	Médecine physique et réadaptation fonctionnelle
356	ABDELKHALKI Mohamed Hicham	MC	Gynécologie-obstétrique
357	ELKASSEH Mostapha	MC	Traumato-orthopédie
358	EL OUAZZANI Meryem	MC	Anatomie pathologique
359	HABBAB Mohamed	MC	Traumato-orthopédie
360	KHAMLIJ Aimad Ahmed	MC	Anesthésie-réanimation
361	EL KHADRAOUI Halima	MC	Histologie-embryologie-cyto-génétique
362	ELKHETTAB Fatimazahra	MC	Anesthésie-réanimation
363	SIDAYNE Mohammed	MC	Anesthésie-réanimation
364	ZAKARIA Yasmina	MC	Neurologie
365	BOUKAIDI Yassine	MC	Chirurgie Cardio-vasculaire
366	NABIL Mehdi	MC	Anesthésie-réanimation
367	KAAKOUA Mohamed	MC	Oncologie médicale
368	FIQHI Mohammed Kamal	MC	Stomatologie et chirurgie maxillo faciale
369	BEN ELHEND Salah	MC	Radiologie
370	KHERRAB Anass	MC	Rhumatologie
371	AWATI El Mehdi	MC	Hématologie

372	HAOUANE Mohamed Amine	MC	Anatomie pathologique
373	BOUABBADI Salah eddine	MC	Ophtalmologie
374	MOUNIR Reda	MC	Chirurgie Cardio-vasculaire
375	AHCHOUCH Siham	MC	Hématologie clinique
376	AZRIOUIL Ouhb	MC	Traumato-orthopédie
377	CHALOUAH Badr	MC	Traumato-orthopédie
378	EL BEJJAJ latimad	MC	Anatomie pathologique
379	BABA Zineb	MC	Rhumatologie
380	OUSSAYEH Imane	MC	Anesthésie-réanimation

LISTE ARRETEE LE 08/10/2025



الحمد لله الذي بنعمته تتم الصالحات، وبفضله تنزل الرحمات، وبحكمته
تُدرَك الغايات.

وما كنتُ لأنال ما أنا فيه، أو أبلغ ما بلغت، لولا فضله سبحانه وتعالى
أولاً وآخرًا، ظاهرًا وباطنًا.

له الحمد على ما علّمني وما ألهمني، وما وفقني إليه
من علمٍ وعملٍ في سبيله.

أسأله جلّ في علاه أن يجعل هذا العمل خالصًا لوجهه الكريم، نافعًا
لعباده، وأن يعينني على الإخلاص في مهنتي،

لأكون وسيلة من وسائل رحمته بعباده،

شكرًا له واعترافًا بفضله العظيم.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
قَالَ رَسُولُ اللَّهِ ﷺ

« مَنْ لَا يَشْكُرِ النَّاسَ لَا يَشْكُرِ اللَّهَ »

*La gratitude, c'est le secret de la vie. Celui qui ne sait pas remercier ne sait pas aimer. » **Albert Schweitzer***



*À toutes celles et ceux qui ont semé dans mon cœur la force de
persévérer et le courage de rêver,
À ceux qui ont éclairé mes jours de leur bienveillance et apaisé mes
doutes par leurs mots,
Je veux dire merci, du plus profond de l'âme.
Cette thèse est le fruit d'un effort personnel, mais surtout d'un amour
collectif, de gestes simples et d'un soutien sincère.
C'est avec reconnaissance et tendresse que
Je dédie cette thèse ...*



Tout d'abord à Allah,

اللهم لك الحمد حمداً كثيراً طيباً مباركاً فيه عدد خلقك ورضى نفسك ووزنة
معرضك ومداد كلماتك اللهم لك الحمد ولك الشكر حتى ترضى ولك الحمد
ولك الشكر عند الرضى ولك الحمد ولك الشكر دائماً وأبداً على نعمتك

*Au bon Dieu tout puissant, qui m'a inspiré, qui m'a guidé dans le bon
chemin, je vous dois ce que je suis devenu louanges et remerciements
pour votre clémence et miséricorde « Qu'il nous couvre de sa
bénédiction ». AMEN!*

No journey is taken alone, and mine has been shaped by the love, patience, and unwavering belief of truly remarkable people. I am profoundly grateful for every hand that supported me and every heart that stood beside me. To honor them, I would like to express my deepest appreciation to both the family I was born into and the family I found along the way.

To my dear parents,

No words could ever capture the depth of the love, devotion, and respect I have always felt for you. Nothing in this world can compare to the endless sacrifices you made, day and night, to ensure my education and well-being. This work stands as a humble reflection of your selfless dedication. You have always been my strength and my refuge; you were, you are, and you will forever be the most precious part of my life. My gratitude knows no bounds, and my heart overflows with appreciation. I pray that Allah blesses you with good health and grants me the grace to one day honor and repay even a fraction of what you have given me.

To the woman who gave me everything, my guiding light, my forever inspiration, my precious mother AYYOUBI NAJAT

my unwavering source of strength, love, and reassurance, thank you for believing in me long before I ever learned to believe in myself.

You have been my greatest cheerleader in every season, my safest place to speak freely about anything and everything, and the gentle, loving voice that reminds me to care for myself when I forget to do so. Your presence has been my anchor in moments of doubt, and your wisdom has guided me through choices both big and small.

Your prayers carried me through challenges I could not always put into words, and your constant faith in me gave me the courage to keep moving forward, even when the path felt heavy or uncertain. Every step of this journey has been made possible by your love, your sacrifices, and your quiet strength.

Thank you for your continuous and unparalleled love, encouragement, and support. Thank you for being my earliest role model of hard work and dedication, and for inspiring me to grow without limits.

This thesis is, first and foremost, dedicated to you. I hope that through this achievement, I have made you proud—even a fraction as proud as I have always been to be your child.

To the man who shaped my life ; my precious father BOUSSIRI
HASSAN

whose love is expressed not through many words, but through countless acts of care and sacrifice. Even when you did not say it aloud, I always felt how deeply you believed in me. Thank you for every effort you made to make my path smoother, for every late night spent worrying, and for every moment you pushed me to stand strong on my own.

Your guidance taught me resilience, your actions taught me responsibility, and your presence taught me that love can be steady and powerful even in silence. I hope this accomplishment brings you pride, just as your strength and dedication have always inspired me.

To my precious sisters, my constant support and forever best friends, may Allah protect you, bless you abundantly, and grant you joy, fulfillment, and peace in every step of your lives.

To my sister CHAYMAE BOUSSIRI

whose quiet nature speaks louder than words ever could. You care with a softness that is steady and sincere ; in the way you notice everything, support silently, and love without seeking attention. You may not always express your feelings openly, but your presence has been a constant reassurance in my life.

Thank you for your love, for the thoughtful gestures that reveal how deeply you care, and for always being there in the background, ready to step in when it matters most. I admire the strength you carry quietly and the kindness you offer so effortlessly. You are a gift in our lives, and I hope you always know how appreciated and deeply loved you are.

To my sister ZINEB BOUSSIRI « Zina »

younger in years, but so much bigger in heart. You have been my confidante, my constant supporter, and the one who can make me laugh even when I am the punchline of the joke. You stood by me through every high and low with a loyalty that words can barely describe. Watching you grow and blossom into the remarkable, strong-willed, and beautifully stubborn person you are today has been one of the greatest privileges of my life.

I am endlessly proud of you ; proud of your courage, your strength, and that bright personality that fills every room you walk into. As long as I exist, you will always have a sister who loves you fiercely, protects you, cheers for you, and celebrates every victory that comes your way. You are not just my sibling; you are my built-in best friend and my forever companion. I thank Allah every day for the blessing of calling you my sister.

To my beloved friend, Binomtii HOUDA CHAHRAOUI

my partner through every chaotic shift and every unexpected laugh. I will never stop reminding you of how beautiful you are ; not only in appearance, but in the kindness, sincerity, and light that radiate from your heart. Together, we have shared successes that made us proud and challenges that made us stronger. Every car ride, every conversation, every shift, and every obstacle we faced side by side has become a cherished memory simply because you were there.

Through it all, you carried yourself with patience and grace, always finding a way to move forward with a smile. You consistently choose to see the good in people first, and that is one of the many reasons your presence is such a gift. I am deeply grateful that we grew through everything together, supporting one another, encouraging one another, and laughing our way through it all. Thank you for being exactly who you are: beautifully genuine, quietly strong, and effortlessly wonderful.

May life always return to you the joy, kindness, and light you so generously give, and may your path be filled with laughter, love, and peace.

To Chaïmaa Bouskout « biscuit »

your hugs have always been the warmest and safest place to land, a quiet refuge when words were not enough. You have a heart overflowing with love, and I am endlessly grateful that a part of it has been shared with me. You have cared for me deeply and supported me through every moment, both the loud ones and the quiet ones.

You love so openly, listen so genuinely, and show your care not only through words but through actions that speak volumes.. Your wisdom, honesty, and kindness are gifts I treasure more than I can fully express. I am profoundly grateful that we walked this journey together, side by side. Watching you grow into the elegant, kind-hearted woman you are today fills me with pride and happiness.

From the bottom of my heart, I wish you every success, every joy, and every beautiful thing life has to offer—because you truly deserve all of it and more.

To Rime Bounouar

Your presence brings peace wherever you go. You are the definition of beauty and brilliance : elegant, determined, and wonderfully unbothered by anything that does not deserve your energy. I will always admire the way you focus on solutions rather than problems, approaching every situation with clarity, maturity, and quiet strength. You understand deeply, care genuinely, and have a rare gift for lifting others up with an ease that feels natural and sincere.

Your optimism carries a quiet light that has lifted my spirit in moments of doubt.

Those who do not have you in their lives are truly missing out on someone exceptional. Sharing this journey with you - through every high and every low - has made it richer, lighter, and infinitely more meaningful. Thank you for your calm presence, your steady support, and for simply being the remarkable person you are.

May life reward your wisdom, grace, and kindness with peace, fulfillment, and endless reasons to smile.

To Farah Bounaouara, our Daisy

a woman of incredible strength and an even more incredible heart. This journey hasn't been the easiest for you, yet you always carried a smile, not only for yourself, but for all of us. It is no surprise that you are loved by so many; you give without measure, love deeply, and brighten every space you enter. Sharing a flat with you was never just about living together, but about collecting memories I will treasure forever. listening to your stories, and learning through your laughter and passion. I will always hold close our laughter, our tears, our late-night talks, your wonderfully chaotic recipes, you singing Elissa's songs, and your animated explanations of your favorite series (but definitely not sbouzi) . Every story you share carries a piece of your beautiful journey, and I will forever listen to them with the same admiration. You have made every one of us proud, and I know your beloved father is looking at you with immense pride as well. You will always be our favorite Tunisian, and I hope life treats you with the same kindness, strength, and joy that you so generously give to others.

I hope you find time to be happy and not just strong.

To Ines Chenani

the one with the stunning presence and an energy that lights up every room she walks into. From the very beginning, your joy has been contagious, carried most beautifully in one of the loveliest laughs I have ever known—the kind that instantly lifts spirits and makes everything feel lighter. Wherever there is fun, excitement, or a good plan, you somehow find yourself at the heart of it, radiating happiness, confidence, and a spark that makes life feel fuller and more alive. Yet beyond the joy and the sparkle, what truly defines you is how deeply you care for the people you love, always attentive, always making sure everyone around you feels included, comfortable, and happy. I will forever cherish our sleep-ins, our shared meals, our spontaneous clothes-shopping adventures, and all the laughter woven into those simple moments. Those memories may seem small, but they hold so much warmth and meaning for me. Thank you for being such a bright, joyful, and genuine part of my journey ; life has always felt richer, lighter, and more beautiful with you in it.

May life always surround you with happiness, love, and beautiful opportunities, and may your light continue to shine just as brightly wherever you go.

To Ossama Bouremah

Thank you for being a constant source of wisdom, calm, and light. Your honesty and quiet clarity have always been a steady anchor for me.

Your words have carried me in ways that you may never fully know.

Through your kind gestures, your genuine care, and your steady presence, you have shown what true friendship means. You meet both ease and difficulty with the same quiet composure, never complaining, always leading with patience and perspective.

You have a rare ability to see the bright side of things, to give without expecting anything in return, and to say exactly what needs to be said at exactly the right moment. We often joke that you are lucky, but the truth is that we are the lucky ones, truly blessed to have you in our lives. I am deeply proud of the man you have become, profoundly grateful for your friendship, and I sincerely wish you a life filled with fulfillment, peace, and everything your heart deserves.

To Ikram Nada Messaho,

my highschool bestie, even though distance now stands between us, my love and appreciation for you have never changed. I will always love you to the moon and back. You believed in me long before this journey truly began, back when I first said I wanted to become a doctor, and that belief meant more than you know. I cherish every memory we created walking to and from school, our endless conversations, our shared dreams, and the laughter that made everything feel possible. You have one of the purest hearts, full of kindness and sincerity. We may not talk every day, but whenever we do, you somehow make my day lighter, brighter, and filled with comfort. Thank you for being a constant in my life, even from afar.

May life always surround you with happiness, love, and beautiful opportunities, and may your light continue to shine just as brightly wherever you go.

To ilías chekrouni

Since high school, you have carried the same kind, calm, and loving heart. Your nonchalant energy has always made things feel lighter and easier. You have a subtle way of caring—quiet, steady, and sincere—that speaks more through presence than words. And while you may often be asleep, on the rare occasions you are not, I know I can always count on you. I am truly grateful for our friendship, and I sincerely hope that life treats you with the same kindness and generosity you so naturally give to others.

To Soufiane Chekairi

you have always known how to make us laugh with your dark humor, especially when we needed it most. I've truly enjoyed every debate, every conversation where we challenged each other's thoughts and perspectives. But it was through the hard times that I got to see who you really are : reliable, kind, and far more caring than you ever admit. Thank you for showing up and for being a steady presence when life got difficult. I genuinely wish you all the happiness this world has to offer ; because you deserve good things, even if your jokes sometimes suggest otherwise.

To Abdelbasset Chalabi

we may not have started off on the right foot, but getting to know the real you has been one of the best surprises of this journey. With time, I discovered your humorous, kind-hearted soul, and I am so grateful that I did. I hold countless memories of you making us laugh until we cried — your singing, your impressions, and your comedic timing deserve their own award. Those moments will forever be golden memories that I'll keep close to my heart. Thank you for being exactly who you are : a friend who always knows how to turn any ordinary moment into an unforgettable one.

To my former flatmates,

To Laila hajji « our Layaalii »

a soul defined by kindness and a heart of rare purity. You are brave in ways that inspire me, and beautiful in ways that go far beyond what is seen. Traveling with you was never just about destinations, but about sharing moments, laughter, and discovering joy in every part of the journey. You stood by me through both the light and the heavy days, offering presence, warmth, and understanding without ever needing to be asked. Your support has been a constant comfort, and your friendship a quiet strength. I am endlessly grateful for you and for the place you hold in my life.

I pray that life meets you with the same kindness you so effortlessly give, that your path is filled with peace, courage, and happiness, and that you are always surrounded by the love you deserve.

To Amale Soudani

the voice that always knows how to find me when I need it most. You have an incredible way of saying exactly the right words, reminding me that after every hardship, something good is waiting to unfold. I admire your willingness to always try, to learn, and to step into the unknown with courage and curiosity. Your words have lifted me more times than you know, and your honesty and care never go unnoticed. You bring clarity, reassurance, and light, and for that, I am deeply thankful.

I pray that your journey is filled with growth, clarity, and joy, that every effort you make is rewarded, and that life continues to return to you the light you so generously give to others.

To Raouane El fadili "Rai"

a roommate who quickly became so much more than that. These years felt easier because you were part of them. We shared simple moments that turned into memories: meals after long days, spontaneous late-night dances, quiet stress before exams, and the joy of celebrating our successes together. We cried when things felt overwhelming, laughed at our mistakes, and found comfort in doing it all side by side. Sharing a space with you meant sharing life, and I will always carry these moments with gratitude.

I pray that your days ahead are filled with ease, laughter, and success, that life surprises you with goodness, and that you always find warmth and happiness wherever you go.

To Imane amchaarou, Abir Taib, Nouhayla Ellaili

eight years ago, our paths crossed. Time passed, places changed, yet our closeness remained, growing stronger with every shared memory. You are beautiful in your own ways, kind at heart, endlessly funny, and simply a joy to be around. We have lived so many moments together, experiences that shaped us and stories that still make us laugh until our sides hurt. Being with you is always fun in the truest sense : effortless, loud, and full of life. I pray that our bond continues to defy time and distance, that your lives are filled with happiness, love, and success, and that we keep creating memories together for many years to come.

To Rachid Benchekroune

though we met only recently, your kindness, reliability, and infectious energy have left a lasting impression. It has been a pleasure getting to know someone so genuine and dependable. I wish you continued success, happiness and fulfillment in all that lies ahead.



REMERCIEMENTS



À NOTRE MAÎTRE MOHAMMED ZYANI, PRÉSIDENT DU JURY,

*Nous tenons à vous exprimer, Professeur Zyani,
notre profonde
gratitude pour l'honneur que vous nous faites en acceptant de
présider
le jury de cette thèse. Votre présence confère à ce travail une valeur
particulière, empreinte de rigueur scientifique et de reconnaissance
académique.*

*Nous vous remercions très sincèrement pour l'attention que vous
avez
bien voulu accorder à ce travail, ainsi que pour la bienveillance, la
disponibilité et l'exigence intellectuelle qui caractérisent votre
engagement envers la formation médicale.
Veuillez agréer, Professeur, l'expression de notre très haute
considération et de notre profond respect.*

**A NOTRE CHER MAÎTRE ET DIRECTEUR DE THÈSE, PR
ABDERRAHIM RAÏSSI,**

*Je tiens à exprimer, Professeur Raïssi, ma profonde reconnaissance
pour avoir accepté de diriger ce travail et pour l'accompagnement
précieux que vous m'avez accordé tout au long de cette thèse.*

*Votre disponibilité constante, votre bienveillance et la confiance que
vous m'avez témoignée ont été déterminantes et témoignent de
grandes qualités humaines, pour lesquelles je vous serai toujours
reconnaissante.*

*Votre exigence intellectuelle, la rigueur de vos orientations et la
pertinence de vos conseils ont largement contribué à la qualité
scientifique de ce travail et ont profondément enrichi ma réflexion.*

*Veuillez trouver ici l'expression de ma reconnaissance la plus sincère
et la plus durable, que je conserverai bien au-delà de l'aboutissement
de cette thèse.*

*À NOTRE CHER MAÎTRE ET membre de jury PROFESSEUR
YOUSSEF QAMOÛSS*

C'est pour moi un grand honneur que vous ayez accepté de siéger au sein de ce jury honorifique.

Je suis particulièrement touchée par la bienveillance avec laquelle vous avez accepté d'évaluer ce travail.

Votre parcours professionnel exemplaire, vos compétences reconnues, ainsi que vos qualités humaines font de vous un professeur éminent, qui suscite en moi admiration et profond respect.

Permettez-moi, Cher Maître, de vous adresser l'expression de ma sincère gratitude et de mon profond respect.

*À NOTRE CHER MAÎTRE ET membre de jury PROFESSEUR
ISMAIL ESSÂDI*

Nous vous remercions vivement, Professeur Essâdi, d'avoir accepté avec chaleur de nous honorer de votre présence au sein de ce jury.

Vous

incarnez des qualités remarquables ; votre humilité professionnelle, ainsi que vos compétences professionnelles et humaines, constituent pour

nous un modèle à suivre dans l'exercice de notre profession.

Veuillez trouver, à travers ce travail, l'expression de notre gratitude sincère, de notre très haute considération et de notre profond respect.



LISTE DES ABRÉVIATIONS



LISTE DES ABRÉVIATIONS

CERT	Computer Emergency Response Team
CHU	Centre Hospitalier Universitaire
CNDP	Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel
CSIRT	Computer Security Incident Response Team
DPI	Dossier Patient Informatisé
DPP	Dossier Patient Partagé
ECISO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity (Agence de l'Union européenne pour la cybersécurité)
FMPM	Faculté de Médecine et de Pharmacie de Marrakech
IoMT	Internet of Medical Things (Internet des objets médicaux)
IT	Information Technology (Technologies de l'information)
MENA	Middle East and North Africa (Moyen-Orient et Afrique du Nord)
NASSS	Non-adoption, Abandonment, Scale-up, Spread and Sustainability
OMS	Organisation Mondiale de la Santé
PIH	Plateforme d'Information Hospitalière
RGPD	Règlement Général sur la Protection des Données
SIH	Système d'Information Hospitalier
UE	Union Européenne
UTAUT	Unified Theory of Acceptance and Use of Technology



Liste des figures



Liste des figures

Figure 1	Répartition des répondants selon le sexe
Figure 2	Répartition des répondants selon la tranche d'âge
Figure 3	Répartition des répondants selon la profession
Figure 4	Répartition selon l'établissement
Figure 5	Répartition selon le secteur
Figure 6	Répartition selon le service
Figure 7	Répartition selon l'ancienneté
Figure 8	Niveau d'aisance informatique
Figure 9	Formation des répondants
Figure 10	Organisation des dossiers patients
Figure 11	Supports d'accès aux données numériques
Figure 12	Accès au système d'information par identifiant personnel
Figure 13	Existence et connaissance des procédures
Figure 14	Perceptions globales de la digitalisation des données médicales
Figure 15	Perceptions éthiques liées à la digitalisation des données de santé
Figure 16	Axe cybersécurité : pratiques et perceptions des professionnels
Figure 17	Analyse comparative des bénéfices perçus de la digitalisation des données médicales selon les professionnels de santé et la littérature internationale
Figure 18	Contraintes et risques perçus liés à la digitalisation des données médicales, comparaison entre notre étude et la littérature internationale
Figure 19	Modèle intégré de gouvernance éthique et sécurisée des données de santé



Liste des tableaux



Liste des tableaux

Tableau 1	Perceptions globales de la digitalisation des données médicales
Tableau 2	Perceptions éthiques liées à la digitalisation des données de santé
Tableau 3	Axe cybersécurité : pratiques et perceptions des professionnels
Tableau 4	Principaux points de convergence entre la loi marocaine n°09-08, le RGPD et la HIPAA
Tableau 5	Principaux points de divergence entre la loi marocaine n°09-08, le RGPD et la HIPAA
Tableau 6	Synthèse des études sur le décalage entre aisance informatique et compétences normatives en santé numérique
Tableau 7	Bénéfices perçus de la digitalisation des données médicales selon les professionnels de santé, comparés aux données de la littérature internationale
Tableau 8	Contraintes et risques perçus liés à la digitalisation des données médicales
Tableau 9	Comparaison des pratiques numériques à risque observées dans notre étude et dans la littérature internationale
Tableau 10	Recommandations opérationnelles pour une e-santé conforme et sécurisée



PLAN



INTRODUCTION	1
MATERIELS ET METHODES	5
I. Type d'étude :	6
II. Population d'étude :	6
1. Population cible	6
2. Critères d'inclusion	6
3. Critères d'exclusion	6
III. Période d'étude :	6
IV. Outil de collecte des données :	7
V. Structure du questionnaire ;	7
VI. Taille de l'échantillon :	7
VII. Recueil et traitement des données :	8
VIII. Considérations éthiques :	8
RÉSULTATS	9
I. Données sociodémographiques :	10
1. Répartition selon le sexe ;	10
2. Répartition selon la tranche d'âge :	10
3. Répartition selon la profession :	11
4. Répartition selon l'établissement d'exercice	12
5. Répartition selon le secteur d'activité :	13
6. Répartition selon le service d'affectation	14
7. Ancienneté professionnelle :	15
8. Niveau d'aisance avec l'outil informatique	15
9. Formation préalable dans des domaines spécifiques	16
II. Organisation des systèmes d'informations et outils	17
1. Mode de gestion des dossiers patients	17
2. Supports utilisés pour accéder aux données numériques	18
3. Modalités d'authentification et d'accès au système d'information	19
4. Existence de règlements ou procédures écrites concernant l'utilisation des données médicales numériques :	20
III. Perceptions globales de la digitalisation :	20
IV. Perceptions éthiques liées à la digitalisation des données de santé :	23
V. Axe cybersécurité	26
DISCUSSION	30
A. Fondements et contexte de la digitalisation des données médicales :	31
I. Contexte général et définitions :	31
1. Définition de la donnée médicale :	31
2. Évolution de la digitalisation dans les systèmes de santé	31
3. Technologies associées à la digitalisation	32
II. Cadre légal et institutionnel marocain	33
1. La loi n°09-08 et ses implications dans le domaine de la santé	33
2. Rôle institutionnel de la CNDP	33
3. Réglementations internationales comparées	34

III. Concepts clés : éthique, sécurité et confiance	36
1. Éthique et secret médical à l'ère du numérique	36
2. Sécurité des systèmes d'information en santé :	36
3. Perception du risque et culture de sécurité chez les médecins :	37
B. Interprétation des résultats à la lumière de la littérature	38
I. Analyse critique des résultats sociodémographiques	38
1. Profil sociodémographique et adoption des technologies numériques	38
2. Aisance informatique perçue versus compétences normatives :	39
3. Statut professionnel et perceptions des technologies numériques	41
4. Rôle de la formation et du contexte organisationnel	42
II. Adoption et usage des systèmes d'information hospitaliers	44
1. Un niveau d'adoption intermédiaire : la persistance de modèles hybrides	44
2. Impact perçu des SIH sur la continuité et la coordination des soins	45
3. Contraintes institutionnelles et disparités public-privé	48
4. Fragmentation régionale et limites de l'intégration nationale	49
5. Charge administrative et paradoxes de l'adoption des systèmes d'information hospitaliers	50
III. Cybersécurité en santé au Maroc : responsabilité individuelle et gouvernance institutionnelle :	54
IV. Perceptions éthiques et respect du secret médical	56
1. Continuité des soins versus confidentialité : une tension éthique structurelle	56
2. Pratiques numériques à risque et fragilisation du secret médical	57
3. Cadre juridique marocain et exigences de conformité éthique	59
4. Consentement éclairé et autonomie du patient à l'ère numérique	59
5. Droits du patient, contrôle des données et confiance numérique	61
6. Pratiques numériques à risque : analyse comparative avec la littérature	62
V. Dimension cybersécurité et risques organisationnels	65
1. Perception du risque cyber chez les professionnels de santé	66
2. Vulnérabilités techniques et pratiques numériques à risque	67
3. Faibles organisationnelles et déficit de gouvernance	68
4. Illustrations internationales des impacts cliniques et organisationnels	69
5. Vers une gouvernance intégrée du risque cyber en santé	70
VI. Mise en perspective avec la stratégie nationale de e-Santé	70
1. Ambition stratégique nationale et enjeux de maturité opérationnelle	71
2. Le Dossier Patient Partagé: pilier stratégique et conditions de faisabilité	71
3. Temporalité de la transformation numérique et charge organisationnelle	72
4. Confiance numérique du patient : condition clé de réussite de la stratégie e-Santé	72
5. Une tension structurante entre ambition stratégique et réalité de terrain	73
6. Implications pour la stratégie nationale	73
VII. Forces, limites et perspectives de l'étude	73
1. Forces de l'étude	74
2. Limites de l'étude	76
3. Implications et Perspectives :	77

C. Recommandations :	77
1. Recommandations au niveau des établissements de santé	78
2. Recommandations pédagogiques et de formation	78
3. Recommandations réglementaires et institutionnelles	79
4. Recommandations relatives à l'information et à l'implication du patient	79
CONCLUSION	82
RESUME	85
ANNEXES	91
BIBLIOGRAPHIE	103



INTRODUCTION



La digitalisation des données médicales constitue un axe majeur de transformation des systèmes de santé. Elle vise à améliorer l'efficacité des soins, la coordination entre les professionnels et l'accès à l'information médicale. Toutefois, la sensibilité des données de santé impose des exigences élevées en matière de confidentialité, de sécurité et d'éthique (1). Le développement des systèmes d'information hospitaliers (SIH), du Dossier Patient Informatisé (DPI), de la télémédecine et de l'Internet of Medical Things (IoMT) modifie profondément les pratiques médicales et l'organisation des établissements de santé (2,3).

Au Maroc, cette évolution s'inscrit dans un contexte de réformes structurelles du secteur de la santé, notamment la généralisation de la couverture médicale et la mise en œuvre d'une stratégie nationale de digitalisation. La transition du dossier médical papier vers le dossier numérique constitue une étape clé de cette modernisation, mais elle s'accompagne de défis organisationnels, techniques, juridiques et humains. La gestion des accès aux données, leur traçabilité, le respect du secret médical, la cybersécurité et la protection de la vie privée figurent parmi les principales préoccupations des professionnels de santé (4).

Sur le plan juridique, la loi marocaine n°09-08 relative à la protection des données à caractère personnel constitue le cadre réglementaire de référence. Elle encadre la collecte, le traitement et la sécurisation des données personnelles, sous le contrôle de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) (5). Toutefois, plusieurs travaux ont mis en évidence une connaissance insuffisante de cette législation par les professionnels de santé, limitant son application effective au sein des établissements de soins (6).

Par ailleurs, la digitalisation des données de santé soulève des enjeux éthiques majeurs. Le secret médical, fondement de la relation de confiance entre le patient et le médecin, est mis à l'épreuve dans un environnement numérique marqué par la circulation rapide de l'information. Des dilemmes émergent entre confidentialité et continuité des soins, sécurité et accessibilité des données, ainsi qu'entre utilité clinique et respect du consentement du patient (7). L'utilisation secondaire des données de santé à des fins de recherche,

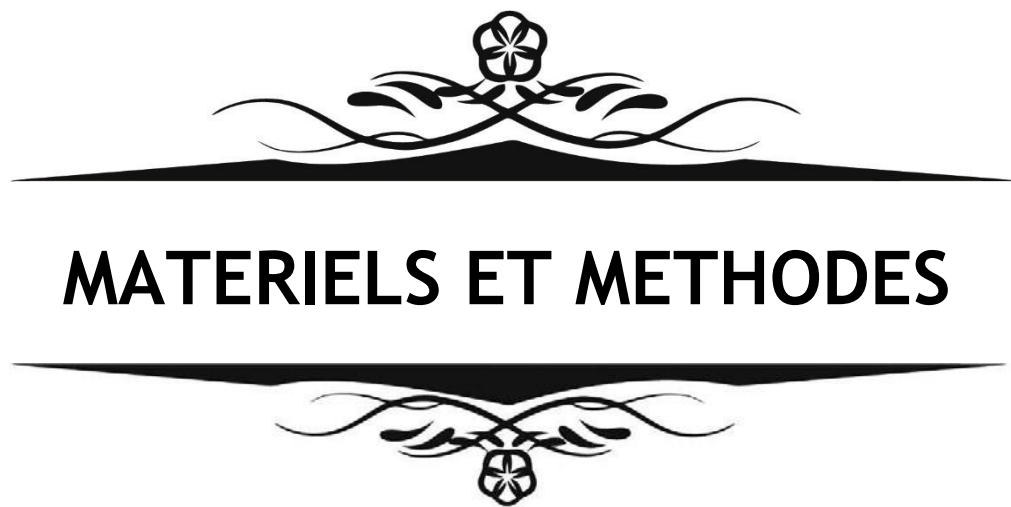
d'épidémiologie ou commerciales soulève également des interrogations éthiques importantes (8).

1. Objectif général :

Évaluer les perceptions, les connaissances et les pratiques des médecins de Marrakech et région concernant la digitalisation des données médicales, en analysant les enjeux éthiques, organisationnels et sécuritaires associés.

2. Objectifs spécifiques :

- Décrire le degré de digitalisation des établissements de santé à travers l'utilisation des systèmes d'information, des dossiers médicaux informatisés et des outils numériques.
- Analyser les perceptions des médecins concernant les bénéfices et les risques liés à la digitalisation, notamment en matière de qualité des soins, de confidentialité et de sécurité.
- Évaluer les pratiques individuelles des médecins en matière de protection des données, incluant l'usage des mots de passe, des messageries, des supports numériques et la gestion des accès.
- Explorer les attitudes éthiques face au secret médical, à l'accès aux dossiers, aux situations de partage d'information et à l'utilisation secondaire des données.
- Mesurer le niveau de connaissance du cadre légal marocain, en particulier la loi n°09-08 et les missions de la CNDP.
- Identifier les faiblesses, les risques et les besoins exprimés par les médecins en matière de cybersécurité et de formation.
- Proposer des recommandations pour renforcer la digitalisation éthique et sécurisée au sein des établissements de santé marocains.



I. Type d'étude :

Il s'agit d'une étude quantitative, descriptive et transversale, menée par enquête auprès de médecins exerçant au niveau de la région de Marrakech.

II. Population d'étude :

1. Population cible

La population cible était constituée de médecins en exercice ou en formation, exerçant dans la ville de Marrakech ou les provinces limitrophes, incluant :

- Internes des hôpitaux relevant de la FMPPM
- Résidents en formation
- Médecins généralistes du secteur public et privé
- Médecins spécialistes du secteur public et privé
- Professeurs de médecine et de chirurgie

2. Critères d'inclusion

- Médecins en exercice ou en formation appartenant aux catégories citées ci-dessus
- Acceptant volontairement de répondre au questionnaire
- Ayant complété l'intégralité du questionnaire

3. Critères d'exclusion

- Formulaires incomplets ou non validés
- Participants exerçant en dehors de la région ciblée

III. Période d'étude :

La collecte des données s'est déroulée sur une période de trois mois, allant d'octobre à décembre 2025.

IV. Outil de collecte des données :

Le recueil des données a été réalisé à l'aide d'un questionnaire élaboré spécifiquement en fonction des objectifs de la recherche (annexe 1). Sa conception s'est appuyée sur la littérature nationale et internationale relative à la digitalisation des données médicales, les principes d'éthique en santé, les recommandations en cybersécurité ainsi que le cadre législatif marocain, notamment la loi n°09-08 relative à la protection des données à caractère personnel.

Le questionnaire comprenait des questions fermées, des questions à choix multiples ainsi que des échelles de Likert, utilisées afin d'évaluer le degré d'accord des participants vis-à-vis des différentes affirmations proposées. L'ensemble des items était organisé en plusieurs sections thématiques. Le questionnaire a été administré en ligne via la plateforme Google Forms, et diffusé à travers des canaux professionnels (groupes d'internes, réseaux institutionnels, associations médicales), garantissant l'anonymat des participants et facilitant l'exportation des données pour l'analyse.

V. Structure du questionnaire :

- A. Profil des participants
- B. Organisation du système d'information
- C. Perceptions globales de la digitalisation
- D. Aspects éthiques
- E. Pratiques individuelles de cybersécurité
- F. Culture de sécurité
- G. Connaissances du cadre légal
- H. Situations pratiques

VI. Taille de l'échantillon :

Un total de 380 questionnaires exploitables a été collecté et inclus dans l'analyse.

VII. Recueil et traitement des données :

Les réponses ont été recueillies automatiquement via la plateforme Google Forms, puis exportées sous format tableur (Excel) afin d'être analysées de manière quantitative. Les résultats ont été présentés sous forme de tableaux et de graphiques.

VIII. Considérations éthiques :

La participation à l'étude était libre, éclairée et anonyme. Les objectifs de l'étude, le caractère volontaire de la participation ainsi que la confidentialité des réponses ont été clairement mentionnés dans l'introduction du questionnaire. Cette étude respecte les principes fondamentaux de l'éthique médicale et de la protection des données personnelles.



L'analyse porte sur un effectif total de 380 professionnels de santé ayant répondu au questionnaire. Les résultats sont exprimés en effectifs absolus et en pourcentages, calculés sur la base de l'effectif total pour chaque variable.

VI. Données sociodémographiques :

1. Répartition selon le sexe :

Parmi les participants, 59,5 % étaient de sexe masculin (n = 226) et 40,5 % de sexe féminin (n = 154). (figure 1)

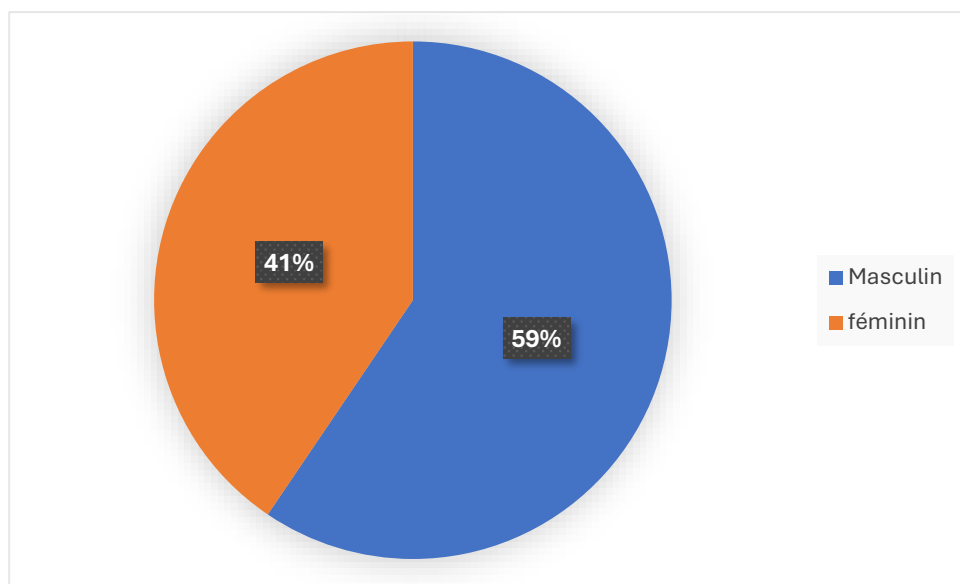


FIGURE 1 : REPARTITION DES REpondANTS SELON LE SEXE

2. Répartition selon la tranche d'âge :

La répartition des participants par tranche d'âge montre une prédominance des médecins de moins de 30 ans (38,9 %). Les tranches d'âge de 30 à 39 ans et de 40 à 49 ans représentent respectivement 31 % et 20,8 % de l'échantillon, tandis que les médecins âgés de plus de 50 ans sont les moins représentés (9,2 %). (figure 2)

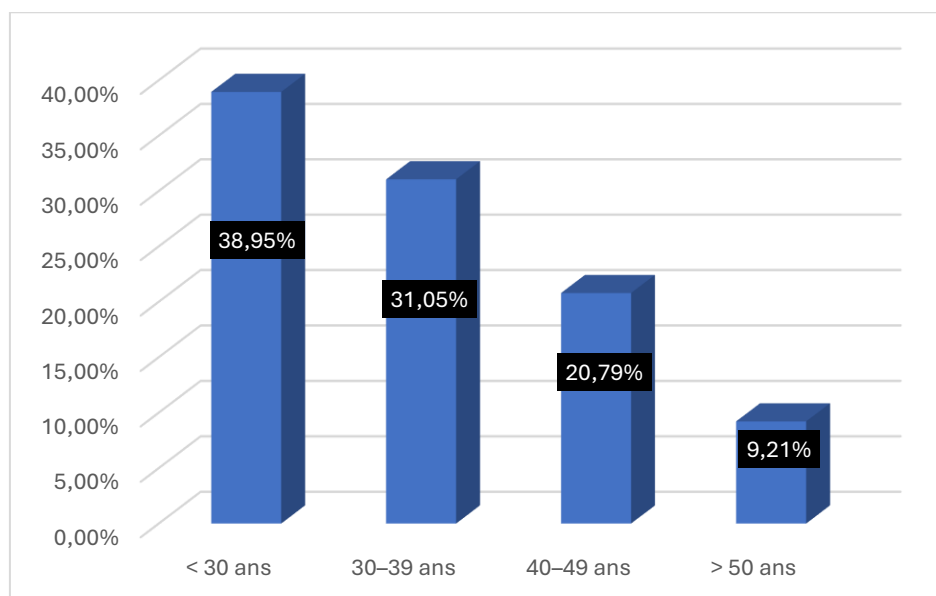


FIGURE 2 : REPARTITION DES REpondANTS SELON LA TRANCHE D'AGE

3. Répartition selon la profession :

Concernant le statut professionnel, les médecins spécialistes constituent le groupe le plus représenté (31,3% ; n=119), suivis des résidents (23,7% ; n=90), des internes (16,6%; n=63), des médecins généralistes (15,8%; n=60) et des professeurs (12,6%; n=48). (figure 3)

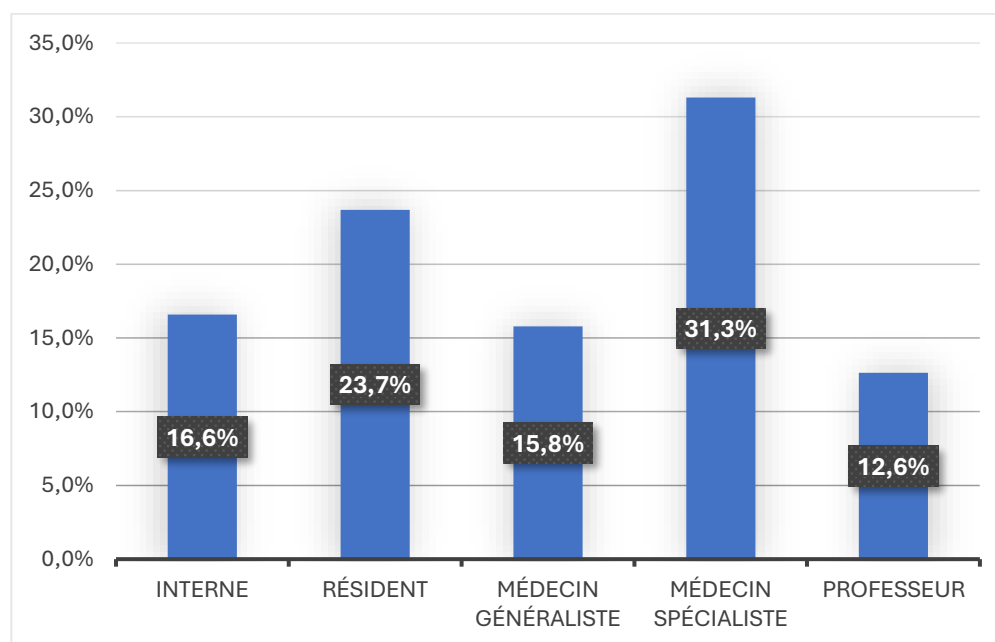


Figure 3 : Répartition des répondants selon la profession

4. Répartition selon l'établissement d'exercice

La répartition selon le type d'établissement montre une prédominance du Centre Hospitalier Universitaire, où exercent 46,1 % des médecins (n = 175). Les hôpitaux militaires représentent 22,1 % des participants (n = 84), suivis des cabinets libéraux (13,2 % ; n = 50) et des centres de santé urbains (11,3 % ; n = 43). Les centres de santé ruraux ou dispensaires ainsi que les autres structures regroupent 7,3 % de l'effectif total. (figure 4)

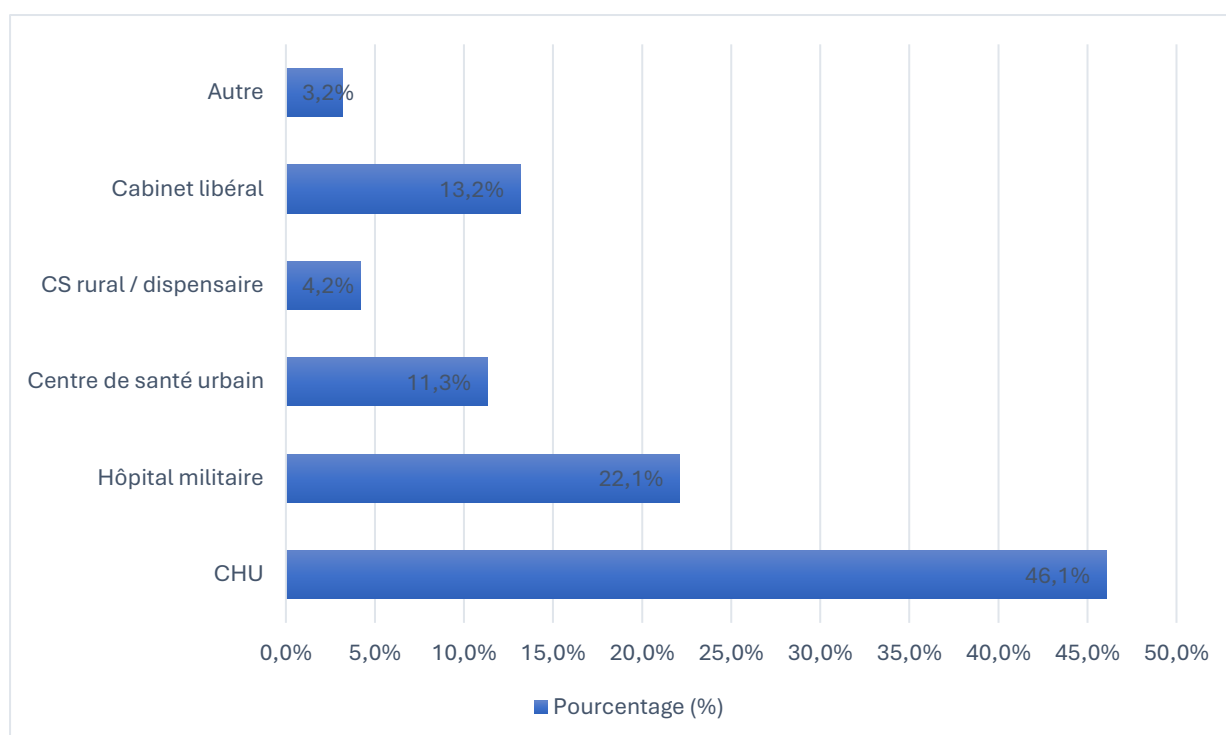


FIGURE 4 : REPARTITION SELON L'ETABLISSEMENT

5. Répartition selon le secteur d'activité :

La répartition des médecins selon le secteur d'exercice montre une prédominance du secteur public, qui regroupe 86,3 % des participants ($n = 328$). Les médecins exerçant dans le secteur privé représentent 13,7 % de l'effectif total ($n = 52$). (figure 5)

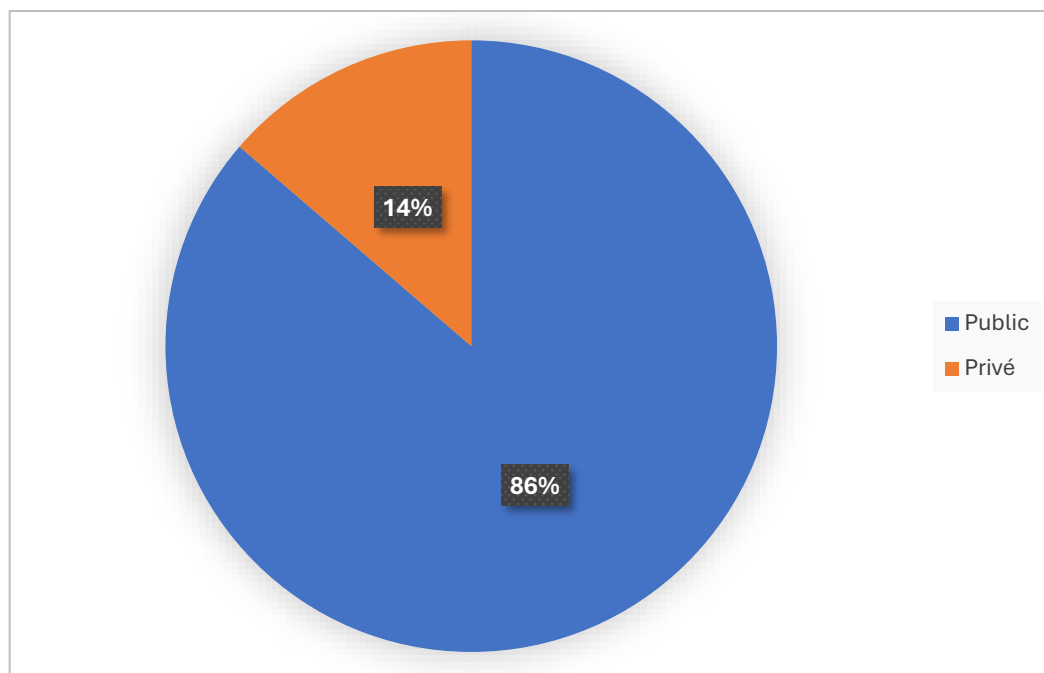


FIGURE 5 : REPARTITION SELON LE SECTEUR

6. Répartition selon le service d'affectation

La répartition des médecins selon le service d'exercice montre une prédominance des services médicaux, qui regroupent 31,6 % des participants (n = 120). Les services chirurgicaux représentent 21,8 % de l'effectif (n = 83), suivis par la médecine générale, qui concerne 15,8 % des répondants (n = 60).

Les urgences-réanimation représentent 7,4% des participants (n=28). Les services de gynécologie, pédiatrie et les laboratoires regroupent chacun 5,3% des répondants (n=20). Tandis que la psychiatrie est la moins représentée avec 3,7 % (n = 14). (figure 6)

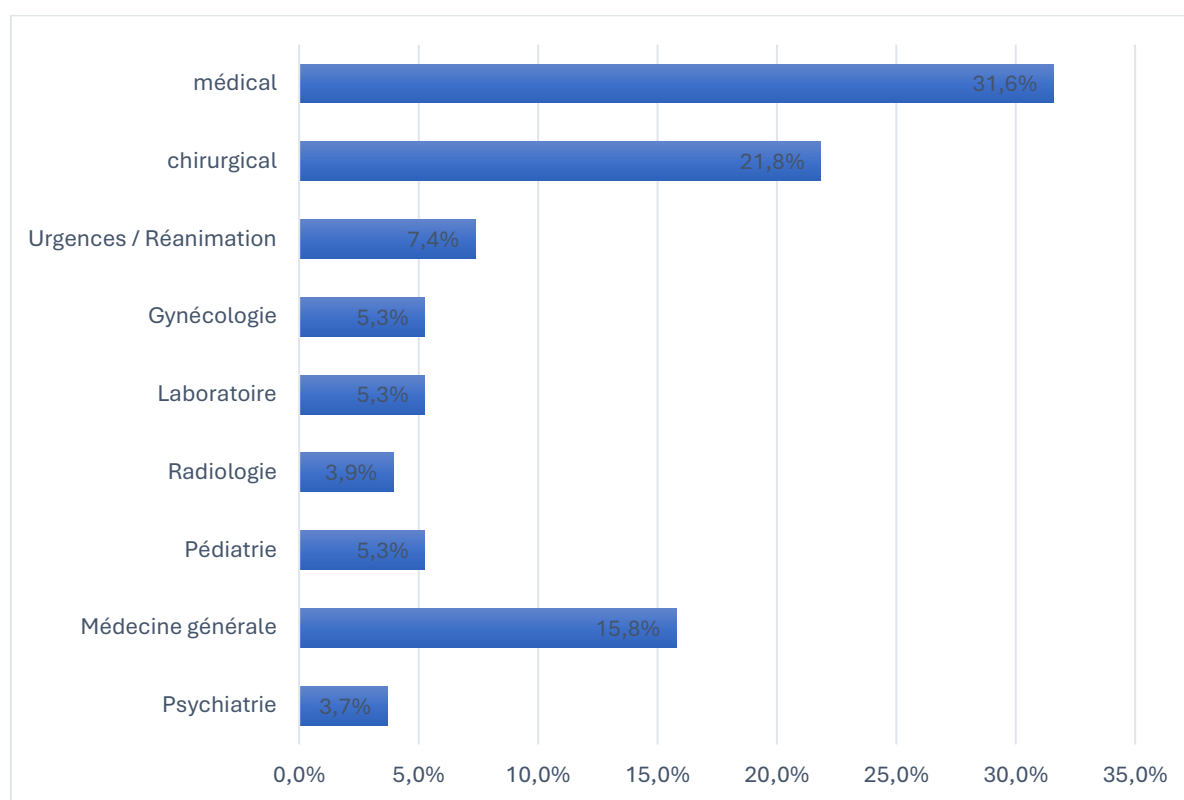


FIGURE 6 : REPARTITION SELON LE SERVICE

7. Ancienneté professionnelle :

La répartition des médecins selon l'ancienneté professionnelle montre que les praticiens ayant moins de 5 ans d'exercice représentent 33,7 % de l'effectif total (n = 128). Les médecins ayant une ancienneté comprise entre 11 et 20 ans constituent 27,4 % des participants (n = 104), tandis que ceux ayant entre 6 et 10 ans d'ancienneté représentent 22,9 % (n = 87). Les médecins justifiant de plus de 20 ans d'ancienneté sont les moins nombreux, avec une proportion de 16,1 % (n = 61). (figure 7)

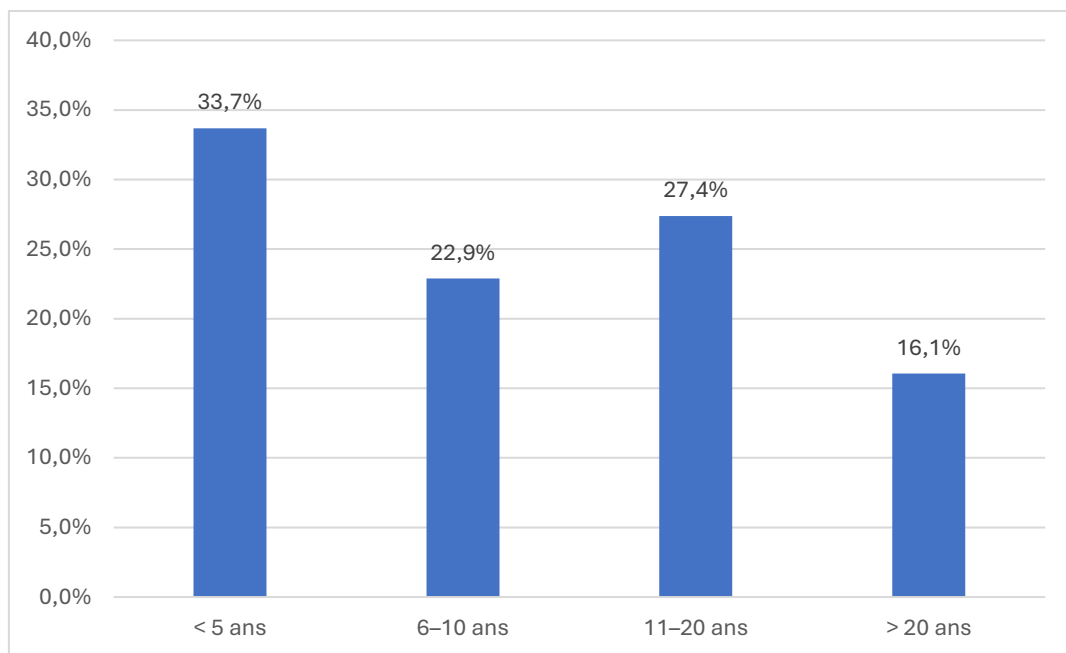


FIGURE 7 : REPARTITION SELON L'ANCIENNETE

8. Niveau d'aisance avec l'outil informatique

L'analyse du niveau d'aisance informatique des répondants montre que la majorité des médecins déclarent un niveau moyen, représentant 51,9 % de l'effectif (n = 197). Les niveaux élevé et très élevé concernent respectivement 22,7 % (n = 86) et 7,6 % (n = 29) des participants. En revanche, une proportion plus limitée des répondants rapporte un niveau faible ou très faible en informatique, avec 12,6 % (n = 48) et 5,2 % (n = 20). (figure 8)

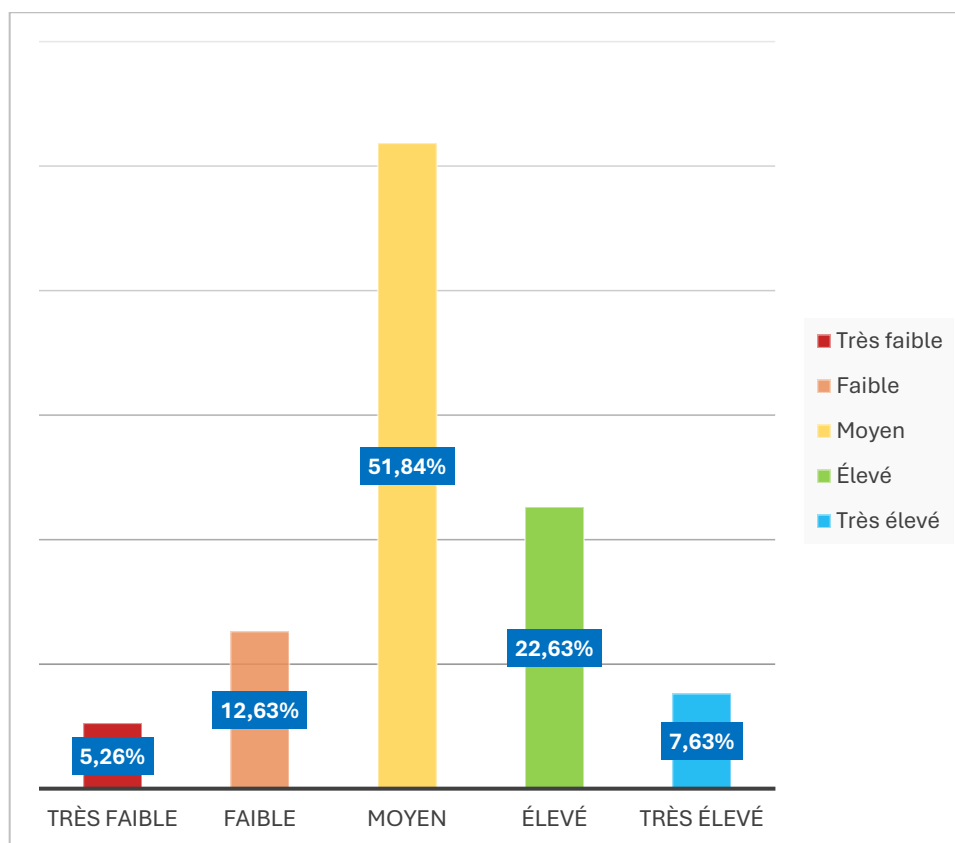


FIGURE 8 : NIVEAU D'AISSANCE INFORMATIQUE

9. Formation préalable dans des domaines spécifiques

Parmi les 380 médecins interrogés, 320 (84,2 %) déclarent avoir bénéficié d'une formation en éthique médicale, tandis que 60 (15,7 %) indiquent ne pas avoir reçu de formation ou ne pas s'en souvenir.

Concernant la protection des données personnelles, seuls 18 répondants (4,7 %) rapportent avoir suivi une formation spécifique, alors que 362 (95,2 %) déclarent ne pas avoir été formés ou ne pas être informés.

La cybersécurité est le domaine le moins couvert par la formation médicale, avec seulement 12 répondants (3,1 %) ayant reçu une formation, contre 368 (96,9 %) n'ayant bénéficié d'aucune formation ou ne s'en souvenant pas. (figure 9)

Au total, si la majorité des répondants a bénéficié d'une formation en éthique médicale, les formations en protection des données et en cybersécurité restent très peu répandues.

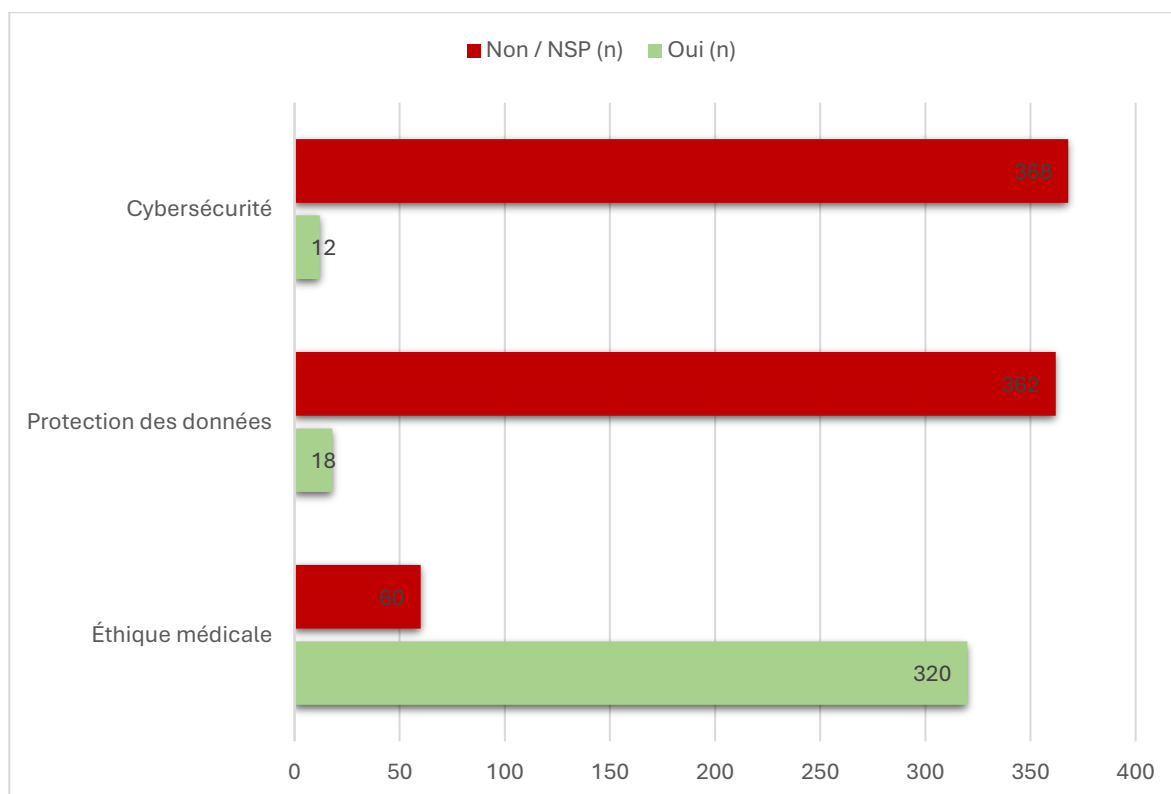


FIGURE 9 : FORMATION DES RÉPONDANTS

VII. Organisation des systèmes d'informations et outils

1. Mode de gestion des dossiers patients

La majorité des répondants (54,6 %) rapporte une gestion des dossiers majoritairement papier avec un recours limité aux outils informatiques. Seuls 7,6 % déclarent travailler dans un environnement entièrement informatisé, tandis que 16,8 % utilisent exclusivement le support papier. (figure 10)

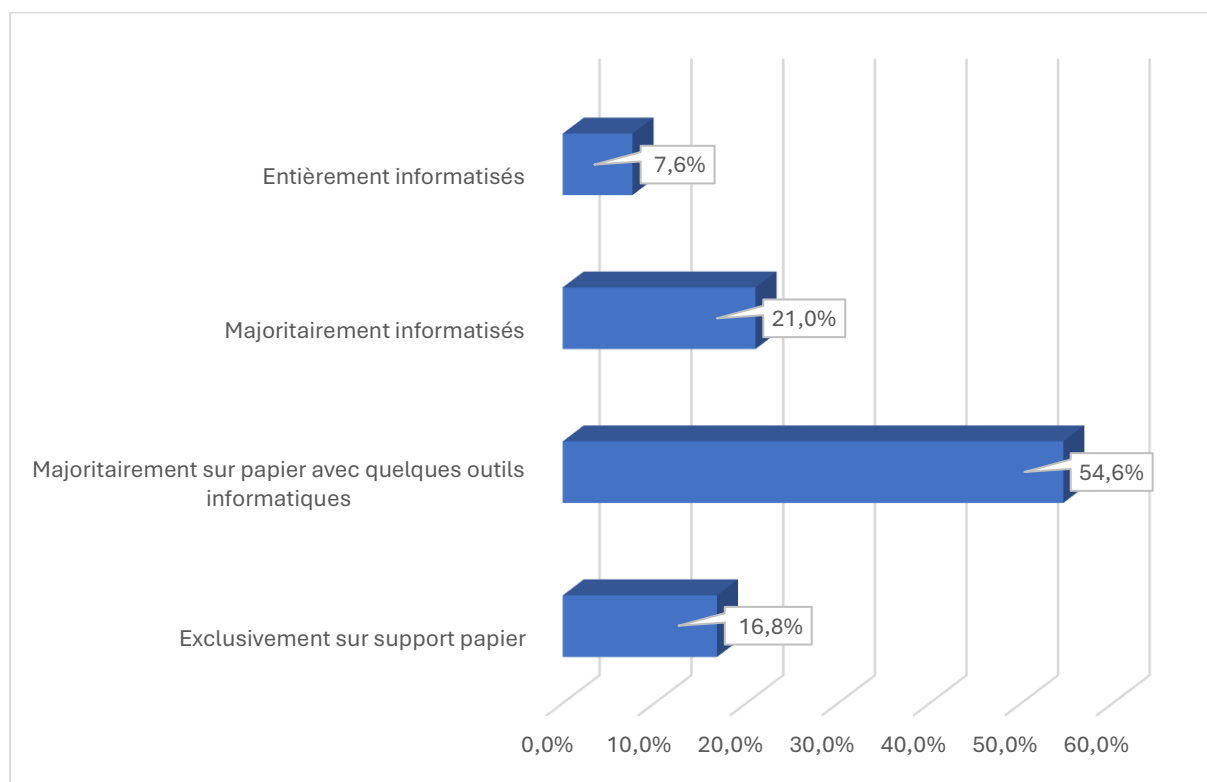


Figure 10 : Organisation des dossiers patients

2. Supports utilisés pour accéder aux données numériques

L'ordinateur mis à disposition par l'établissement est utilisé par 190 répondants, soit 50,0 % de l'effectif total. L'utilisation d'ordinateurs personnels concerne 80 professionnels (21,1 %), tandis que 60 répondants (15,8 %) déclarent utiliser un smartphone. L'option « non applicable » a été rapportée par 49 participants, correspondant à 12,9 % de l'effectif total. (figure 11)

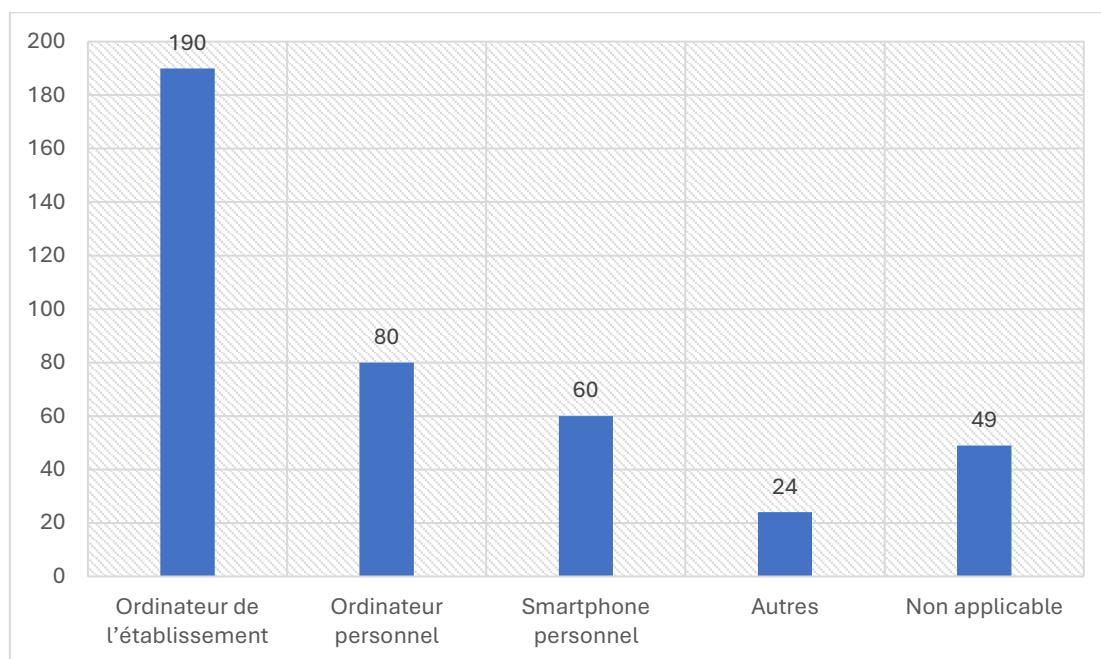


FIGURE 11 : SUPPORTS D'ACCES AUX DONNEES NUMERIQUES

3. Modalités d'authentification et d'accès au système d'information

Moins d'un quart des répondants (23,7 %) disposent d'un identifiant et mot de passe personnels. En revanche, l'utilisation d'identifiants partagés est fréquente (45,8 %), et 17,6 % des professionnels déclarent utiliser les identifiants d'un collègue.(figure 12)

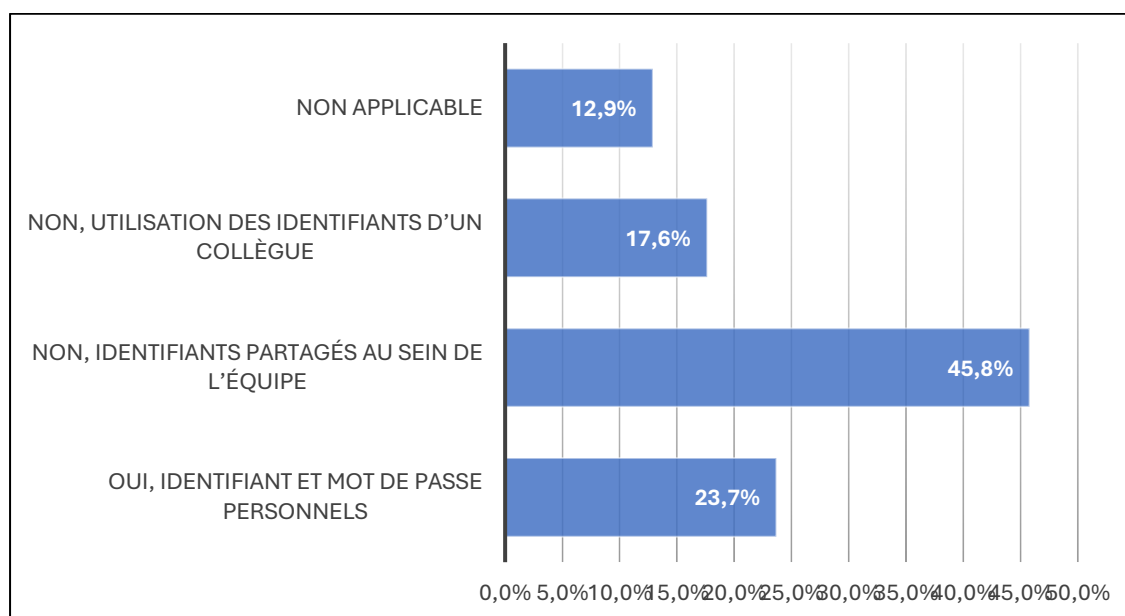


Figure 12 : Accès au système d'information par identifiant personnel

4. Existence de règlements ou procédures écrites concernant l'utilisation des données médicales numériques :

Plus de la moitié des répondants (54,0 %) déclarent ne pas connaître l'existence d'un règlement ou d'une procédure écrite concernant l'utilisation des données médicales numériques. Seuls 25 % affirment connaître effectivement ces procédures.(figure 13)

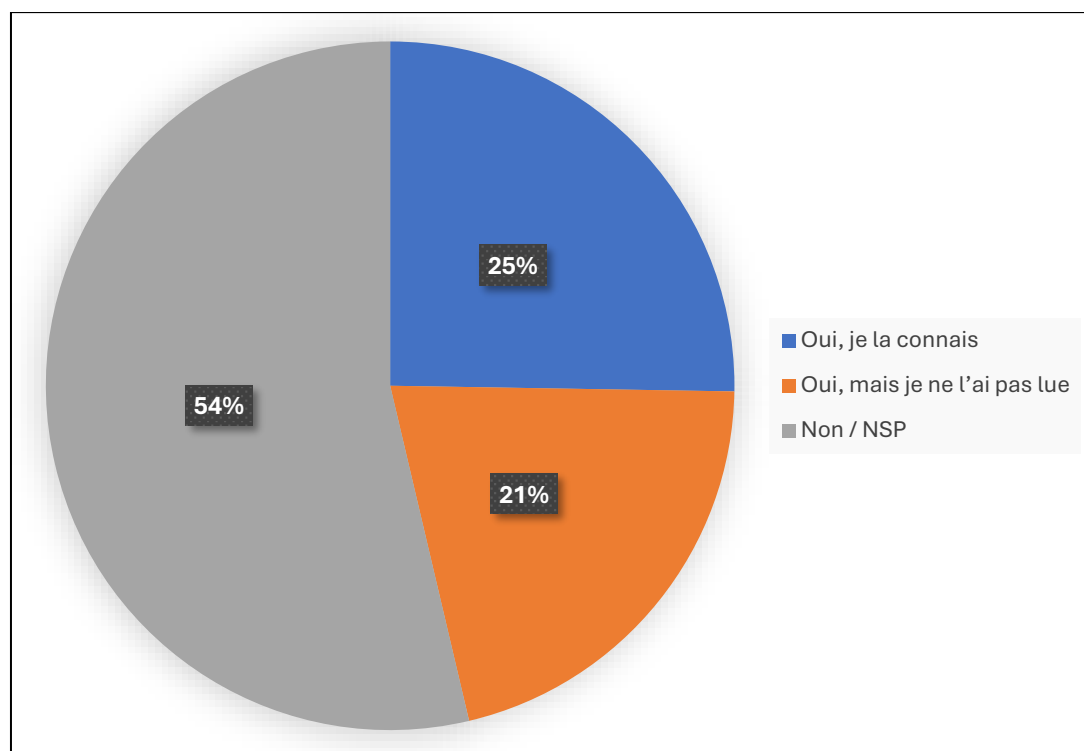


FIGURE 13 : EXISTENCE ET CONNAISSANCE DES PROCEDURES

VIII. Perceptions globales de la digitalisation :

Parmi les répondants, 76,6 % des médecins expriment un accord ou un fort accord avec l'affirmation selon laquelle l'informatisation du dossier patient améliore la qualité et la continuité des soins (scores 4 et 5). Les dossiers médicaux électroniques sont perçus comme améliorant la sécurité clinique par 68,7 % des participants et comme facilitant la coordination des soins par 75,9 % des répondants. Concernant la charge administrative, 35,0 % des médecins déclarent être en accord ou en fort accord avec l'affirmation selon laquelle l'informatisation augmente la charge administrative, tandis que 23,7 % adoptent une position intermédiaire et 41,2 % expriment un désaccord ou un fort désaccord.

Par ailleurs, 64,0 % des médecins déclarent être en accord ou en fort accord avec le fait que la numérisation facilite l'accès non autorisé à des informations sensibles, et 71,8 % estiment qu'elle augmente le risque de fuites massives de données. De plus, 58,5 % des participants expriment un accord ou un fort accord avec l'affirmation selon laquelle l'accès informatisé favorise des consultations injustifiées des dossiers médicaux.

S'agissant de l'équilibre entre bénéfices et risques de la digitalisation dans le contexte marocain, 64,7 % des médecins déclarent être en accord ou en fort accord avec le fait que les bénéfices l'emportent sur les risques, tandis que 19,3 % expriment un désaccord ou un fort désaccord et 16,2 % adoptent une position intermédiaire. La traçabilité des accès aux dossiers médicaux recueille 27,5 % d'accord ou de fort accord, 35,1 % de réponses intermédiaires et 37,5 % de désaccord ou de fort désaccord. Du point de vue des patients, 68,7 % des médecins expriment un accord ou un fort accord avec l'affirmation selon laquelle les patients sont insuffisamment informés sur l'utilisation de leurs données de santé, et 68,8 % estiment que les patients devraient pouvoir limiter l'accès à certaines informations sensibles contenues dans leur dossier médical. Enfin, 22,7 % des médecins déclarent être en accord ou en fort accord avec le fait d'avoir confiance dans la sécurité informatique des systèmes de leur établissement, tandis que 31,3 % adoptent une position intermédiaire et 46,0 % expriment un désaccord ou un fort désaccord. (tableau1)(figure 14)

TABLEAU 1 : PERCEPTIONS GLOBALES DE LA DIGITALISATION DES DONNEES MEDICALES

(Échelle de Likert : 1 = Pas du tout d'accord ; 5 = Tout à fait d'accord ; N = 380)

Item évalué	1 n	2 n	3 n	4 n	5 n
L'informatisation du dossier patient améliore la qualité et la continuité des soins	10	18	60	102	190
L'informatisation augmente la charge administrative	76	81	90	94	39
Les DME améliorent la sécurité clinique	18	29	72	114	147
Les DME facilitent la coordination des soins	25	14	52	76	213
La numérisation facilite l'accès non autorisé à des infos sensibles	16	38	84	133	109
Les bénéfices > risques (contexte marocain)	24	50	61	133	112
Les systèmes permettent une traçabilité des accès	40	102	134	78	26
La digitalisation augmente le risque de fuite massive	12	27	68	150	123
L'accès informatisé favorise des consultations injustifiées	24	56	78	133	89
Les patients sont insuffisamment informés	13	23	82	157	105
Les patients devraient pouvoir limiter l'accès à des infos sensibles	9	28	82	170	91
Confiance dans la sécurité informatique de l'établissement	60	115	119	61	25

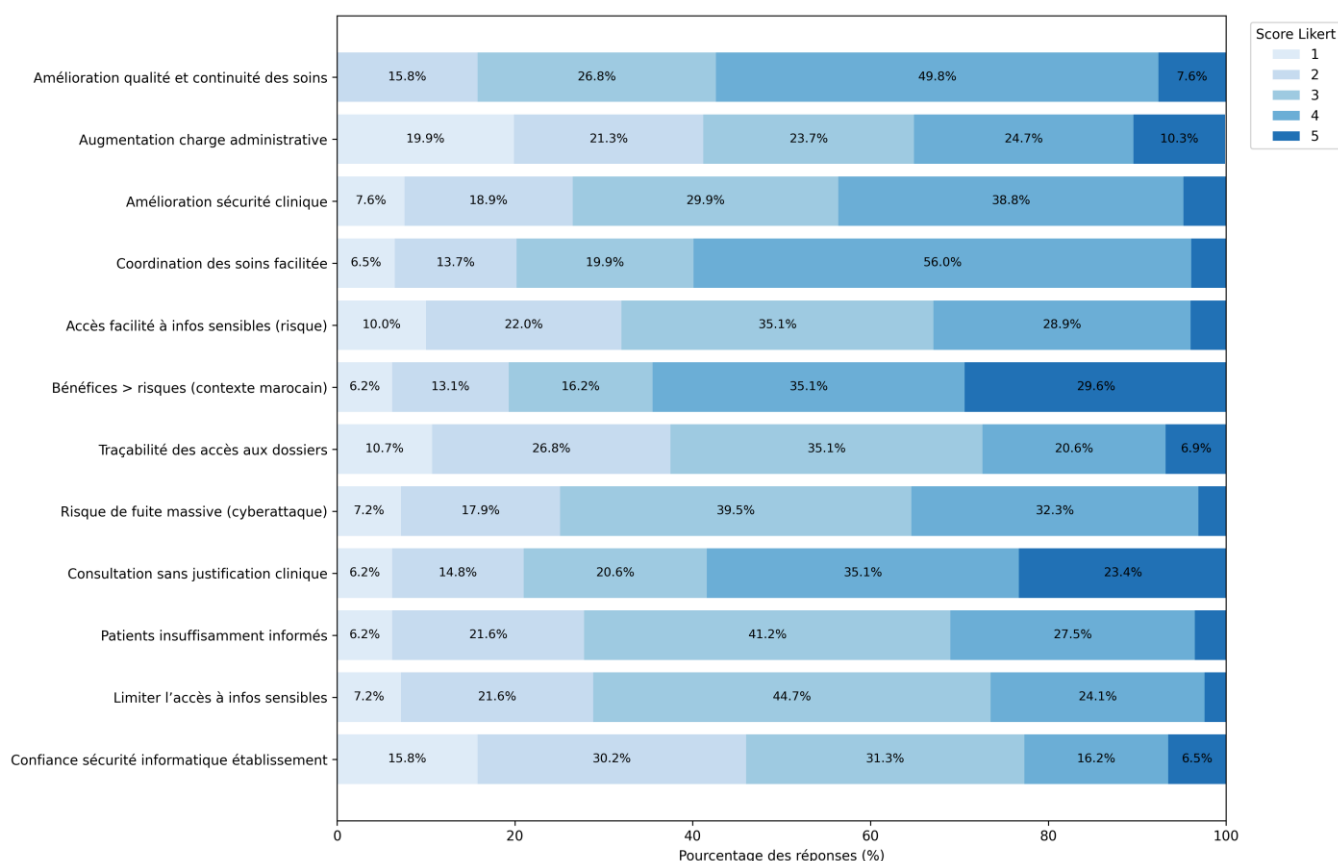


FIGURE 14 : PERCEPTIONS GLOBALES DE LA DIGITALISATION DES DONNEES MEDICALES

IX. Perceptions éthiques liées à la digitalisation des données de santé :

Concernant le respect du secret médical, 81,4 % des médecins se déclarent en accord ou en fort accord avec son caractère prioritaire, y compris face aux demandes administratives émanant d'organismes tiers.

Cependant, un conflit entre la nécessité de partager l'information pour assurer la continuité des soins et le respect strict de la confidentialité est rapporté par une proportion importante des répondants. En effet, 52,9 % des médecins expriment un accord ou un fort accord avec l'existence de ce dilemme, tandis que 29,6 % adoptent une position intermédiaire.

Concernant l'organisation institutionnelle, 20,6 % des médecins estiment que les droits d'accès sont clairement définis dans leur établissement, alors que 50,2 % expriment un désaccord ou un fort désaccord.

Par ailleurs, 47,7 % des répondants reconnaissent discuter de cas cliniques dans des lieux ou devant des personnes non autorisées, et 34,0 % jugent acceptable, dans certaines situations urgentes, l'envoi d'informations médicales identifiantes via des messageries non sécurisées.

S'agissant de l'information des patients, seuls 23,0 % des médecins estiment que les patients sont informés que leurs données sont conservées dans des systèmes numériques, tandis que 46,7 % expriment un désaccord ou un fort désaccord. De même, 52,2 % considèrent que l'utilisation des données à des fins de recherche ou de registres épidémiologiques est expliquée aux patients et que leur consentement est recherché lorsque nécessaire.

En revanche, 69,0 % des médecins en accord ou en fort accord sur la nécessité d'une pseudonymisation minimale et idéalement d'une anonymisation des données transmises à des tiers. Par ailleurs, 73,6 % estiment que l'utilisation des données de santé à des fins commerciales est problématique, même lorsqu'elles sont pseudonymisées.

Enfin, 21,4 % des médecins déclarent se sentir suffisamment formés sur le plan éthique pour prendre des décisions concernant l'utilisation des données de leurs patients, tandis que 51,5 % expriment un désaccord ou un fort désaccord. (tableau 2)(figure 15)

TABEAU 2 : PERCEPTIONS ETHIQUES LIEES A LA DIGITALISATION DES DONNEES DE SANTE

(Échelle de Likert : 1 = Pas du tout d'accord ; 5 = Tout à fait d'accord ; N = 380)

Item évalué	1	2	3	4	5
Le respect du secret médical reste prioritaire, même face aux demandes administratives (assureurs, CNSS, autorités, etc.)	8	16	47	154	155
Je ressens un conflit entre la nécessité de partager l'information pour la continuité des soins et le respect strict de la confidentialité du patient	18	50	112	133	67
Dans mon établissement, il est clairement défini qui a le droit d'accéder à quelles parties du dossier médical	54	137	110	59	20
Il m'arrive de discuter de cas cliniques (diagnostic, détails) dans des lieux ou devant des personnes non autorisées	37	70	94	115	64
Il est acceptable, dans certaines situations urgentes, d'envoyer des informations médicales identifiantes via WhatsApp ou autre messagerie non sécurisée	68	82	101	93	36
Les patients sont informés que leurs données sont conservées dans des systèmes numériques	61	116	114	63	26
Les données utilisées pour la recherche devraient être au minimum pseudonymisées et idéalement anonymisées lorsqu'elles sont transmises à des tiers	14	25	78	163	100
L'utilisation de données de santé à des fins commerciales (industries, assurances, plateformes privées) est problématique, même si les données sont pseudonymisées	9	29	63	149	130
Je me sens suffisamment formé(e) sur le plan éthique pour prendre des décisions concernant l'utilisation des données de mes patients	71	125	103	56	25
L'utilisation des données des patients pour la recherche ou les registres épidémiologiques est clairement expliquée aux patients et leur consentement est recherché lorsqu'il est nécessaire	35	47	100	120	78

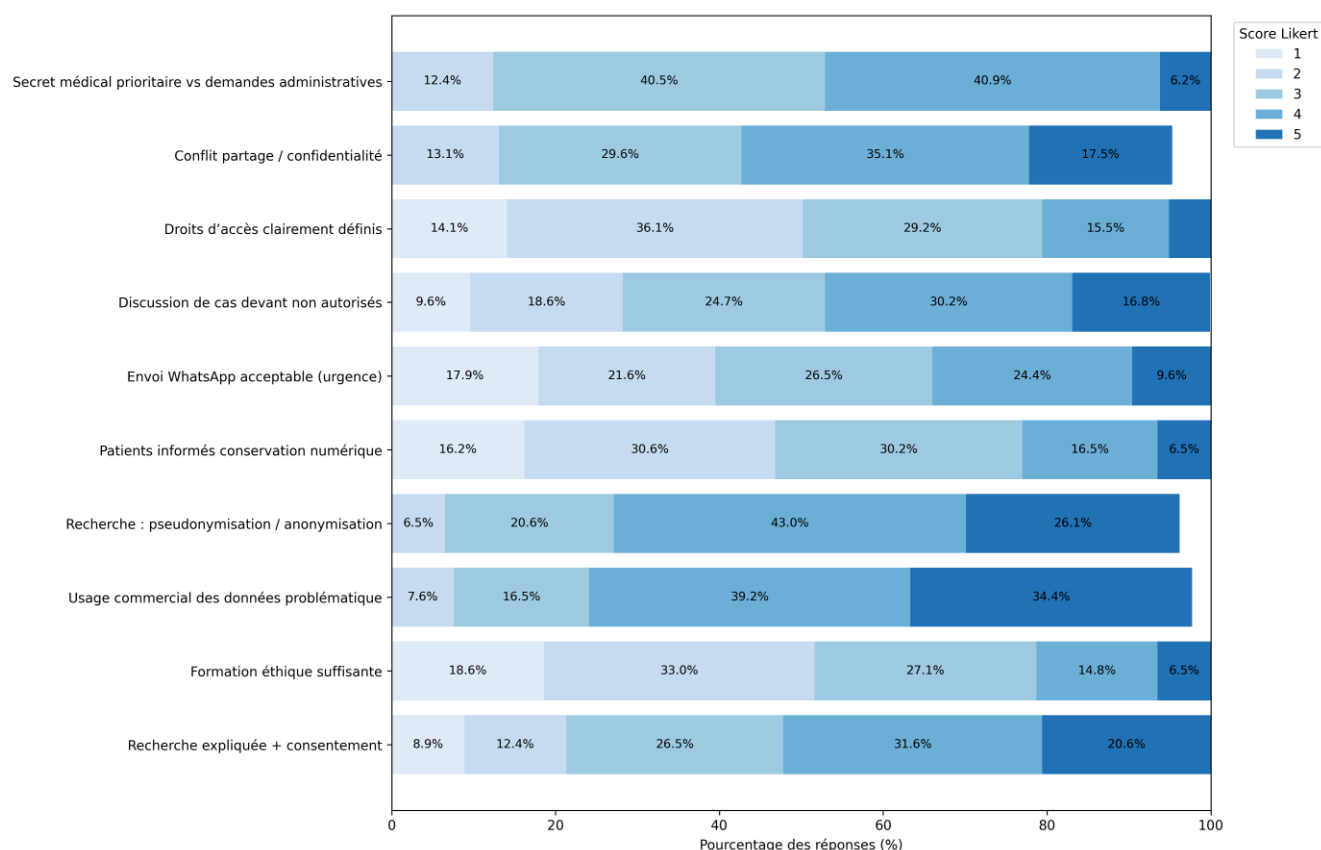


FIGURE 15 : PERCEPTIONS ETHIQUES LIEES A LA DIGITALISATION DES DONNEES DE SANTE

X. Axe cybersécurité

Concernant la sécurisation des postes de travail, 39,7 % des répondants déclarent être en accord ou en fort accord avec le fait de verrouiller leur session ou leur poste dès qu'ils s'absentent, tandis que 25,3 % adoptent une position intermédiaire et 35,0 % expriment un désaccord ou un fort désaccord.

La modification régulière des mots de passe est rapportée par 16,1 % des médecins (accord ou fort accord), alors que 23,4 % adoptent une position intermédiaire et 60,5 % expriment un désaccord ou un fort désaccord.

L'utilisation de mots de passe forts et différents selon les systèmes concerne 17,4 % des répondants, 27,6 % se positionnant de manière intermédiaire et 55,0 % exprimant un désaccord ou un fort désaccord.

La communication des identifiants à un collègue est déclarée par 45,8 % des médecins (accord ou fort accord), tandis que 23,7 % expriment un désaccord ou un fort désaccord et 30,5 % adoptent une position intermédiaire.

L'utilisation du même mot de passe pour des usages professionnels et personnels est rapportée par 32,9 % des répondants, 31,6 % se situant en position intermédiaire et 35,5 % exprimant un désaccord ou un fort désaccord.

Le transfert de données médicales vers des supports personnels est déclaré par 32,1 % des médecins, 27,9 % adoptant une position intermédiaire et 40,0 % exprimant un désaccord ou un fort désaccord.

Le stockage de documents patients sur des supports non sécurisés concerne 27,6 % des répondants, tandis que 26,1 % adoptent une position intermédiaire et 46,3 % expriment un désaccord ou un fort désaccord.

S'agissant de la vigilance face aux emails suspects de type phishing, 42,1 % des médecins déclarent être en accord ou en fort accord avec cette affirmation, 36,6 % adoptent une position intermédiaire et 21,3 % expriment un désaccord ou un fort désaccord.

La connaissance des circuits de signalement des incidents de cybersécurité est rapportée par 19,9 % des répondants, alors que 32,3 % adoptent une position intermédiaire et 47,8 % expriment un désaccord ou un fort désaccord.

Concernant la responsabilité de la cybersécurité, 46,8 % des médecins expriment un accord ou un fort accord avec l'affirmation selon laquelle celle-ci relève principalement des services informatiques, 30,5 % adoptent une position intermédiaire et 22,6 % expriment un désaccord ou un fort désaccord.

Enfin, 52,9 % des répondants déclarent être en accord ou en fort accord avec l'affirmation selon laquelle une violation de données aurait un impact grave sur la confiance des patients, tandis que 24,5 % adoptent une position intermédiaire et 22,6 % expriment un désaccord ou un fort désaccord. (tableau 3)(figure 16)

TABLEAU 3 : AXE CYBERSECURITE : PRATIQUES ET PERCEPTIONS DES PROFESSIONNELS

(Échelle de Likert : 1 = Pas du tout d'accord ; 5 = Tout à fait d'accord ; N = 380)

Item évalué	1 n	2 n	3 n	4 n	5 n
Je verrouille ma session ou mon poste de travail dès que je m'absente	38	95	96	100	51
Je modifie régulièrement mes mots de passe	94	136	89	44	17
J'utilise des mots de passe forts et différents selon les systèmes	107	125	80	46	22
Il m'est arrivé de communiquer mon mot de passe/identifiants à un(e) collègue	40	76	90	98	76
J'utilise parfois le même mot de passe pour le travail et le personnel	47	86	120	82	43
Je transfère des données médicales vers des supports personnels	57	95	106	77	45
Je suis attentif(ve) aux emails suspects (phishing)	34	80	106	99	61
Je stocke des documents patients sur des supports non sécurisés	80	96	99	63	42
Je sais à qui signaler un incident de cybersécurité	98	112	94	50	26
La cybersécurité relève surtout des services informatiques	25	61	116	113	65
Une violation de données aurait un impact grave sur la confiance	56	30	93	116	85

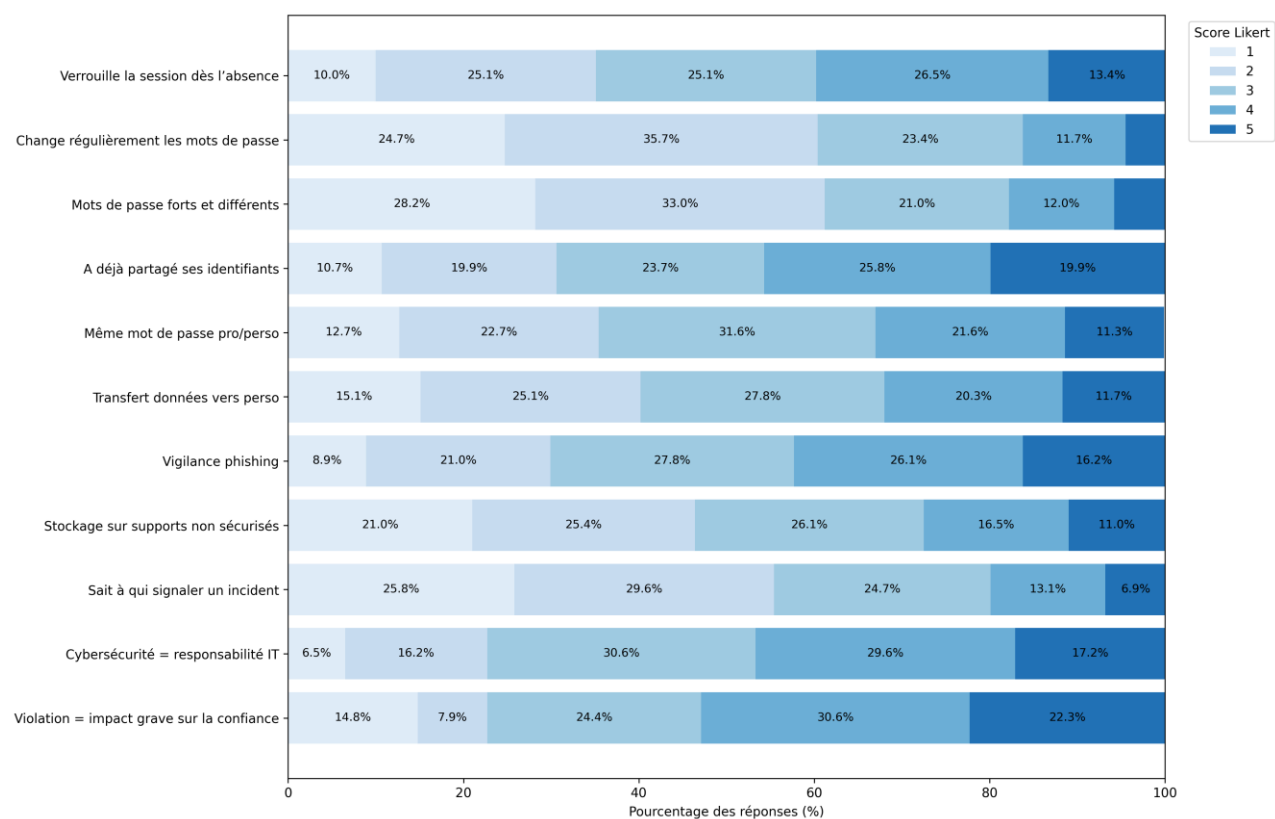


FIGURE 16 : AXE CYBERSECURITE : PRATIQUES ET PERCEPTIONS DES PROFESSIONNELS



A. Fondements et contexte de la digitalisation des données médicales :

I. Contexte général et définitions :

1. Définition de la donnée médicale :

Les données médicales regroupent l'ensemble des informations relatives à l'identification d'un patient, à son état de santé, à son parcours de soins ainsi qu'aux actes médicaux réalisés. Elles incluent :

- **les données administratives** (identité, adresse, couverture médicale),
- **les données sensibles** (antécédents médicaux, diagnostics, traitements, données génétiques),
- **les données biométriques** (empreintes, imagerie, paramètres physiologiques).

Au Maroc, la loi n°09-08 définit les données à caractère personnel comme toute information permettant d'identifier, directement ou indirectement, une personne physique. Les données médicales y occupent une place particulière en raison de leur sensibilité et des obligations renforcées qui s'y appliquent en matière de protection, de confidentialité et de sécurité (5).

La digitalisation des données médicales implique le respect de certains principes fondamentaux :

- **La confidentialité**, qui garantit qu'aucune personne non autorisée n'accède aux informations médicales.
- **Le secret médical**, obligation déontologique et légale protégeant les informations confiées au médecin dans l'exercice de sa fonction.(7)
- **La traçabilité**, qui permet de savoir qui a consulté quel dossier, quand et pour quelle finalité, contribuant à la transparence et à la sécurisation des accès (2).

2. Évolution de la digitalisation dans les systèmes de santé

La transformation numérique des systèmes de santé s'est opérée de manière progressive. Initialement centrée sur des dossiers papier, la gestion de l'information médicale

a évolué vers le dossier patient informatisé (DPI), facilitant l'accès aux données, la coordination des soins et la continuité de la prise en charge. (2)

Cette transformation s'est accompagnée du développement de nouveaux outils numériques, tels que les SIH, intégrant des données administratives, médicales et logistiques, ainsi que les dispositifs de télémédecine, dont l'usage s'est considérablement accru au cours des dernières années.

Au Maroc, la digitalisation du secteur de la santé constitue une priorité stratégique nationale, portée par une volonté d'harmonisation des systèmes d'information et de préparation au déploiement d'un dossier patient unique à l'échelle nationale. Toutefois, cette transformation demeure marquée par des disparités importantes entre régions, établissements et secteurs d'activité, en particulier entre le secteur public et le secteur privé (9).

3. Technologies associées à la digitalisation

La digitalisation des données médicales repose sur un écosystème technologique complexe. Les systèmes d'information hospitaliers constituent l'ossature de la gestion numérique des données, tandis que les dispositifs de cybersécurité regroupent l'ensemble des mesures techniques et organisationnelles destinées à protéger les systèmes contre les cybermenaces. Par ailleurs, l'Internet of Medical Things permet la collecte continue de données physiologiques à partir de dispositifs médicaux connectés, ouvrant de nouvelles perspectives en matière de suivi des patients et de personnalisation des soins (4).

Si ces technologies offrent des opportunités majeures pour l'amélioration de la qualité et de la sécurité des soins, elles exposent également les établissements de santé à des risques accrus, notamment les cyberattaques, les failles de sécurité, la perte ou l'altération des données et les accès non autorisés, souvent liés au facteur humain (4,6).

II. Cadre légal et institutionnel marocain

1. La loi n°09-08 et ses implications dans le domaine de la santé

La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue le cadre juridique de référence au Maroc. Promulguée le 18 février 2009 par le Dahir n°1-09-15 et publiée au Bulletin Officiel le 5 mars 2009, elle a instauré un dispositif réglementaire visant à encadrer la collecte, le traitement et la protection des données personnelles (5).

Cette loi repose sur plusieurs principes fondamentaux, notamment :

- **le consentement**, selon lequel la personne concernée doit être informée et donner son accord au traitement de ses données ;
- **la finalité**, imposant que les données soient collectées pour un objectif précis, explicite et légitime ;
- **la proportionnalité**, limitant la collecte aux seules données strictement nécessaires au traitement ;
- **la sécurité**, obligeant le responsable du traitement à mettre en œuvre des mesures techniques et organisationnelles appropriées afin de protéger les données contre l'accès non autorisé, la perte, l'altération ou le détournement (1,5).

Dans le domaine de la santé, ces exigences s'appliquent avec une rigueur particulière en raison de la sensibilité des données médicales. Les établissements de santé sont ainsi tenus de déclarer ou de solliciter une autorisation préalable auprès de la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel pour tout traitement numérique impliquant des données médicales, conformément aux dispositions de la loi n°09-08 (5).

2. Rôle institutionnel de la CNDP

La CNDP est l'autorité nationale chargée de veiller à l'application de la loi n°09-08. Ses missions incluent :

- l'examen des demandes d'autorisation,
- le contrôle du respect de la loi,

- la sensibilisation des institutions,
- l'émission de recommandations.

Dans le secteur de la santé, la CNDP joue un rôle central pour assurer la conformité des systèmes d'information hospitaliers, des plateformes de télémédecine et des échanges de données avec des partenaires externes.

Toutefois, plusieurs travaux soulignent un niveau de connaissance encore insuffisant de ses missions parmi les professionnels de santé marocains, limitant l'effectivité du cadre légal dans les pratiques quotidiennes (6,7).

3. Réglementations internationales comparées :

À l'échelle internationale, plusieurs cadres réglementaires ont influencé les politiques de protection des données :

- **Le RGPD (Règlement Général sur la Protection des Données)** en Europe, reconnu pour sa rigueur en matière de consentement, de minimisation des données et de droits des personnes.
- **La HIPAA (Health Insurance Portability and Accountability Act)** aux États-Unis, centrée sur la sécurisation des informations médicales et la responsabilité institutionnelle.

Malgré des différences contextuelles et juridiques, ces cadres présentent plusieurs points de convergence notables avec la loi marocaine n°09-08. Ils reposent tous sur le principe fondamental du respect de la vie privée et de la confidentialité des données personnelles, en imposant aux responsables de traitement des obligations strictes en matière de sécurité, d'intégrité et de traçabilité des informations. Le consentement de la personne concernée constitue également un socle commun, bien que ses modalités varient selon le cadre juridique. Par ailleurs, les données de santé sont unanimement reconnues comme des données sensibles nécessitant un niveau de protection renforcé. Enfin, ces réglementations consacrent le principe de responsabilité des institutions traitant les données, lesquelles peuvent faire l'objet de

contrôles et de sanctions en cas de non-conformité, traduisant une volonté commune de prévenir les usages abusifs et les atteintes aux droits des patients (10-12).

Les **tableaux 4 et 5** présentent respectivement les **points de convergence** et les **points de divergence** entre la loi marocaine n°09-08, le RGPD et la HIPAA.

Tableau 4 : principaux Points de convergence entre la loi marocaine n°09-08, le RGPD et la HIPAA

Principe commun	Loi n°09-08 / CNDP (Maroc)	RGPD (Union européenne)	HIPAA (États-Unis)
Données de santé considérées comme sensibles	Protection renforcée prévue	Catégorie spéciale de données	Informations médicales protégées (PHI)
Finalité du traitement	Finalité légitime exigée	Finalité déterminée et explicite	Usage limité aux soins et à la gestion médicale
Minimisation des données	Principe implicite	Principe fondamental	Limitation aux données nécessaires
Sécurité et confidentialité	Mesures techniques et organisationnelles	Obligation de sécurité renforcée	Safeguards administratives, physiques et techniques
Consentement de la personne	Généralement requis	Libre, spécifique et révocable	Généralement requis
Responsabilité des organismes	Responsabilité juridique du responsable	Principe de responsabilisation (accountability)	Responsabilité institutionnelle

Tableau 5 : principaux points de divergence entre la loi marocaine n°09-08, le RGPD et la HIPAA

Critère de comparaison	Loi n°09-08 / CNDP (Maroc)	RGPD (UE)	HIPAA (États-Unis)
Champ d'application	Toutes les données personnelles	Toutes les données personnelles	Données de santé uniquement
Étendue des droits des patients	Accès, rectification, opposition	Droits plus étendus (effacement, portabilité, limitation)	Accès et rectification principalement
Droit à l'effacement	Non prévu	Droit central	Non prévu
Notification des violations de données	Non systématique	Obligatoire sous 72 heures	Obligatoire selon la gravité
Sévérité des sanctions	Amendes limitées	Très élevées (jusqu'à 4 % du CA mondial)	Amendes graduées et sanctions pénales

III. Concepts clés : éthique, sécurité et confiance

1. Éthique et secret médical à l'ère du numérique

Le passage au numérique ne remet pas en cause le principe du secret médical, mais en complexifie l'application. L'élargissement du nombre d'utilisateurs des systèmes d'information, la rapidité de circulation des données et le recours à des outils de communication non sécurisés augmentent les risques de violation de la confidentialité. L'éthique médicale impose dès lors un usage responsable, proportionné et justifié de l'information médicale, dans le respect des principes fondamentaux de bienfaisance, de non-malfaisance et d'autonomie (1,7).

2. Sécurité des systèmes d'information en santé :

La cybersécurité constitue aujourd'hui un enjeu majeur pour les établissements de santé, qui figurent parmi les cibles privilégiées des cyberattaques en raison de la valeur

stratégique des données médicales et de la vulnérabilité de certaines infrastructures. Les incidents observés sont liés à la fois à des **failles techniques** et à des **comportements humains inadaptés**, ces derniers étant reconnus comme l'une des principales sources de vulnérabilité des systèmes d'information (4,6).

3. Perception du risque et culture de sécurité chez les médecins :

La réussite de la transformation numérique dépend largement de l'adhésion des professionnels de santé. Une culture de la sécurité insuffisamment développée, un manque de formation et une méconnaissance des obligations légales et éthiques peuvent compromettre la protection des données médicales et altérer la confiance des patients (6,7).

En définitive, ce cadre juridique et déontologique, bien que robuste sur le plan normatif, met en lumière une tension persistante entre l'exigence de protection des données de santé et les contraintes concrètes de l'exercice médical contemporain. La digitalisation, en multipliant les acteurs, les supports et les usages de l'information médicale, transforme le secret professionnel d'une obligation essentiellement individuelle en un enjeu organisationnel et systémique. Cette évolution interroge la capacité des structures de soins à accompagner efficacement les professionnels dans l'appropriation opérationnelle des règles juridiques et éthiques, sans entraver la continuité et la qualité des soins. Ainsi, la question centrale n'est plus seulement celle de l'existence d'un cadre légal adéquat, mais celle de son intégration effective dans les pratiques quotidiennes, à travers des dispositifs de gouvernance, de formation et de responsabilisation adaptés. C'est dans cet espace de tension entre norme et pratique que s'inscrit l'analyse des résultats de la présente étude.

B. Interprétation des résultats à la lumière de la littérature

I. Analyse critique des résultats sociodémographiques

1. Profil sociodémographique et adoption des technologies numériques

L'analyse du profil sociodémographique de notre échantillon met en évidence une population majoritairement jeune et en début de carrière. En effet, près de 70 % des médecins interrogés ont moins de 40 ans, dont 38,9 % ont moins de 30 ans, traduisant une nette prédominance des jeunes médecins au sein de l'échantillon. Ceci est confirmé par l'ancienneté professionnelle, puisque 33,7 % des répondants déclarent une expérience inférieure à cinq ans et 56,6 % exercent depuis moins de dix ans. Cette distribution traduit donc une population de médecins relativement jeunes, engagés dans une phase active de formation ou de l'installation professionnelle : un facteur non négligeable pour expliquer les perceptions et les pratiques en matière de numérique en santé.

Ce profil est comparable à celui rapporté dans la littérature, notamment par **Gagnon et al.**, qui décrivent une surreprésentation des professionnels de santé jeunes ou en cours de formation parmi les utilisateurs des systèmes d'information hospitaliers, en particulier dans les établissements universitaires. Ces auteurs soulignent que les médecins en début de carrière représentent un groupe central dans la dynamique d'adoption des technologies numériques en santé, en raison de leur forte implication dans l'activité clinique quotidienne et de leur exposition précoce aux environnements hospitaliers informatisés (13).

- Cette observation rejoint également les travaux de **Venkatesh et al.**, développés dans le cadre du modèle UTAUT appliqué aux systèmes d'information en santé, ainsi que ceux de **Yusof et al.**, qui mettent en évidence l'influence significative de l'âge et du niveau de formation académique sur l'acceptabilité et l'utilisation des systèmes d'information hospitaliers. Selon ces auteurs, les professionnels plus jeunes et mieux formés présentent généralement une perception plus favorable de l'utilité clinique des outils

numériques et une moindre résistance à leur adoption. Toutefois, ces travaux soulignent également que cette acceptabilité élevée, associée au profil sociodémographique et professionnel, ne garantit pas une appropriation complète des exigences en matière de sécurité, de confidentialité et de maîtrise du cadre juridique, en particulier en ce qui concerne la protection des données médicales sensibles (14,15).

Sur le plan professionnel et institutionnel, notre échantillon est largement dominé par le secteur public, qui regroupe 86,3 % des répondants, avec une prédominance du Centre Hospitalier Universitaire (46,1 %). Cette répartition reflète l'organisation du système de santé marocain, dans laquelle les structures hospitalières publiques et universitaires concentrent l'essentiel des médecins en formation et des jeunes praticiens. Des observations similaires ont été rapportées par **Holden et Karsh**, qui montrent que les contextes hospitaliers et hospitalo-universitaires constituent des environnements privilégiés pour l'implantation et l'utilisation des technologies numériques en santé, en raison de la complexité des parcours de soins et de la nécessité d'une coordination accrue entre les professionnels (16).

2. Aisance informatique perçue versus compétences normatives :

Dans notre étude, l'aisance informatique perçue apparaît globalement satisfaisante, puisque 82,1 % des médecins interrogés déclarent un niveau intermédiaire à élevé dans l'utilisation des outils informatiques, dont 30,3 % rapportent une aisance élevée ou très élevée. Cette familiarité avec les technologies numériques est cohérente avec le profil sociodémographique de la population étudiée, majoritairement jeune et en début de carrière. Toutefois, cette aisance auto-déclarée contraste nettement avec le faible niveau de compétences spécifiques en matière de protection des données médicales et de cybersécurité.

Ce constat rejoint les travaux de **Norman et Skinner**, qui distinguent la littératie numérique fonctionnelle, centrée sur l'utilisation des outils informatiques, de la littératie informationnelle et normative, intégrant la compréhension des dimensions juridiques, éthiques et organisationnelles propres aux technologies numériques en santé. Selon ces

auteurs, une proportion importante de professionnels de santé présente une aisance technique apparente sans disposer des compétences nécessaires pour appréhender les enjeux de confidentialité et de protection des données, une situation comparable à celle observée dans notre étude (17).

De manière concordante, **McGonigle et Mastrian** soulignent que, malgré l'adoption croissante des systèmes d'information en santé, les connaissances relatives à la sécurité des données et aux obligations réglementaires demeurent insuffisantes chez une large proportion de professionnels. Dans notre contexte, cette insuffisance se traduit par l'absence de formation structurée et par une méconnaissance des principes fondamentaux de cybersécurité, exposant potentiellement les établissements de santé à des vulnérabilités organisationnelles et éthiques accrues (18).

Cette discordance entre une aisance informatique largement déclarée et un déficit de compétences spécifiques s'inscrit dans ce que **Tikanmäki et al.** décrivent comme une *illusion de compétence numérique*. Selon ces auteurs, la familiarité avec les outils numériques est fréquemment assimilée, à tort, à une compétence professionnelle globale, alors qu'elle ne recouvre pas nécessairement la compréhension des exigences normatives, éthiques et organisationnelles liées à la gestion des données de santé. Cette surestimation des compétences constitue un facteur de vulnérabilité dans les environnements cliniques numériques, en masquant des lacunes en matière de protection des données, de cybersécurité et de gouvernance de l'information (19).

Enfin, les travaux de **Greenhalgh et al.** sur l'implémentation des technologies numériques complexes en santé montrent que l'adoption repose principalement sur l'utilité perçue et la facilité d'usage, souvent au détriment de l'intégration des exigences de gouvernance des données et de conformité réglementaire. Cette analyse fait directement écho à nos résultats, où, malgré une aisance informatique élevée, la formation et la sensibilisation aux enjeux de protection des données demeurent marginales, soulignant la nécessité d'une approche institutionnelle structurée en matière de formation en éthique numérique et en cybersécurité (20).

Tableau 6 : Synthèse des études sur le décalage entre aisance informatique et compétences normatives en santé numérique

Étude	résultat principal	Référence
Norman & Skinner	L'aisance numérique fonctionnelle ne reflète pas une compétence normative en santé numérique.	(17)
McGonigle & Mastrian	L'usage des SIH progresse plus vite que la maîtrise de la sécurité et des obligations réglementaires.	(18)
Tikanmäki et al.	Les professionnels de santé surestiment fréquemment leurs compétences numériques.	(19)
Greenhalgh et al.	L'adoption des technologies privilégie l'utilité perçue au détriment de la gouvernance des données.	(20)
Notre étude	Forte aisance informatique déclarée mais déficit majeur de formation en protection des données et cybersécurité.	–

3. Statut professionnel et perceptions des technologies numériques

Dans notre étude, le statut professionnel constitue un élément important de contextualisation des perceptions et des usages des technologies numériques, dans la mesure où les médecins en formation représentent une part substantielle de l'échantillon. En effet, les internes (16,6 %) et les résidents (23,7 %) constituent ensemble **40,3 %** des répondants, traduisant une forte présence de professionnels récemment formés et exposés précocement aux outils numériques au cours de leur cursus universitaire. Cette proportion élevée de médecins en formation peut contribuer à expliquer l'adhésion globale observée vis-à-vis des SIH et des outils numériques, souvent perçus comme des facilitateurs de la pratique clinique.

À l'inverse, les médecins spécialistes et les professeurs, qui représentent respectivement 31,3 % et 12,6 % de l'échantillon, sont généralement confrontés à des responsabilités cliniques, décisionnelles et organisationnelles accrues. Ces professionnels développent plus fréquemment des perceptions critiques à l'égard des technologies numériques, intégrant davantage les enjeux liés à la sécurité des données, à la fiabilité des

systèmes et à leur impact sur l'organisation des soins (21). Cette hétérogénéité de statuts au sein de notre population étudiée constitue ainsi un facteur explicatif potentiel de la diversité des perceptions observées.

Le statut et les responsabilités des médecins, comme le soulignent **Kwateng et al.**, semblent marquer de façon forte l'acceptabilité et l'usage des systèmes d'information hospitaliers.(22)

Dans ce sens, **Cresswell et al.** ont montré que l'accumulation de l'expérience clinique s'accompagne d'une sensibilité accrue aux défaillances organisationnelles et aux risques systémiques induits par la digitalisation, en particulier lorsque les systèmes d'information sont perçus comme peu ergonomiques ou insuffisamment sécurisés. Ces auteurs soulignent que les professionnels les plus expérimentés sont souvent plus attentifs aux conséquences à long terme des technologies numériques sur la qualité des soins, la sécurité des données et la charge de travail, ce qui peut expliquer des attitudes plus réservées ou critiques vis-à-vis de leur déploiement (23).

4. Rôle de la formation et du contexte organisationnel

Dans notre étude, l'absence de formation structurée en matière de protection des données et de cybersécurité apparaît comme un déterminant central des pratiques observées. En effet, alors que 82,1 % des médecins déclarent une aisance informatique intermédiaire à élevée, seuls 4,7 % rapportent avoir bénéficié d'une formation spécifique en protection des données personnelles et 3,1 % en cybersécurité. Ce décalage met en évidence une insuffisance majeure de formation formelle, susceptible d'exposer les établissements de santé à des usages non conformes et à des vulnérabilités accrues, indépendamment de l'âge, du statut professionnel ou du niveau de compétence technique perçu des utilisateurs.

Ces résultats sont concordants avec plusieurs travaux récents menés dans différents contextes sanitaires. Ainsi, **Giertz et al.**, dans une revue systématique internationale sur la littératie numérique des professionnels de santé, montrent que la formation spécifique en sécurité des données et en gouvernance de l'information demeure largement insuffisante, y

compris dans des contextes où l'exposition aux technologies numériques est élevée. Les auteurs soulignent que l'absence de programmes de formation structurés constitue un facteur majeur limitant la transformation des compétences techniques en pratiques réellement sécurisées(24). De manière similaire, **Boonstra et Broekhuis** rapportent que le déploiement des systèmes d'information en santé, lorsqu'il n'est pas accompagné d'une stratégie de formation adaptée, favorise des usages hétérogènes et parfois non conformes, indépendamment du profil sociodémographique des professionnels.(25)

Par ailleurs, le rôle du contexte organisationnel apparaît déterminant dans l'appropriation sécurisée des technologies numériques. **Roman et al.** mettent en évidence que la clarté des procédures internes, la gouvernance des systèmes d'information et l'existence de dispositifs institutionnels de formation conditionnent fortement l'adoption de bonnes pratiques en matière de sécurité et de confidentialité des données(26). Cette dimension organisationnelle est également soulignée par **Alanazi et al.**, qui insistent sur l'importance de la culture institutionnelle et des mécanismes de gouvernance dans la réduction des risques liés à la digitalisation. Dans notre étude, l'impact de ce contexte se traduit par la coexistence d'une aisance informatique déclarée élevée et d'une faible proportion de médecins formés aux enjeux de protection des données médicales et de cybersécurité, pourtant indispensables à toute stratégie efficace de conformité, de gouvernance et de sécurisation des systèmes d'information de santé.(27)

Au niveau national, dans la même ligne, les rares études marocaines montrent une tendance identique ; l'étude de **Mouaouia** au CHU Ibn Rochd montre que l'acceptabilité des SIH découle, amplement, de leur ergonomie, de leur adéquation avec les pratiques cliniques et du soutien institutionnel apportés en ce sens. Nos résultats complètent ces éléments en montrant un déterminant largement inaperçu : la formation juridique et éthique particulière à la gestion des données de santé numériques.(28)

L'OMS identifie le **facteur humain** comme un déterminant central de la sécurité des systèmes d'information en santé. Dans ses rapports consacrés à la santé numérique et à la

cybersécurité, l'OMS souligne que, en l'absence de compétences adaptées et de cadres institutionnels clairs, les professionnels développent des **stratégies de contournement** visant à préserver la continuité et l'efficacité des soins, mais au prix d'une **exposition accrue aux violations de confidentialité et aux incidents de sécurité** (29). Ces stratégies, bien que compréhensibles dans un contexte de contraintes cliniques, renforcent la vulnérabilité globale des systèmes d'information hospitaliers.

La **formation en santé numérique ne peut être considérée donc comme un complément optionnel**, mais constitue un **levier essentiel de prévention des risques** liés à la digitalisation des données médicales. À défaut, l'augmentation de l'usage des technologies numériques s'accompagne inévitablement d'une multiplication des pratiques à risque, compromettant la sécurité des données et la confiance des patients dans les systèmes de soins.

Dans l'ensemble, les résultats confirment que les perceptions et les pratiques liées à la digitalisation des données médicales résultent d'une interaction complexe entre facteurs individuels (âge, statut, expérience), organisationnels (formation, procédures, gouvernance) et contextuels (infrastructure, charge de travail). Ni l'âge ni le statut professionnel ne suffisent, à eux seuls, à expliquer les attitudes observées. Cette complexité plaide en faveur d'une approche intégrée de la transformation numérique, associant formation, gouvernance institutionnelle et accompagnement organisationnel.

II. Adoption et usage des systèmes d'information hospitaliers

1. Un niveau d'adoption intermédiaire : la persistance de modèles hybrides

Dans notre étude, l'analyse de l'adoption des systèmes d'information hospitaliers (SIH) met en évidence une digitalisation encore incomplète et hétérogène au sein des établissements de santé. En effet, 54,6 % des répondants exercent dans un environnement majoritairement fondé sur le support papier, avec un recours partiel aux outils numériques, tandis que 16,8 % déclarent une utilisation quasi exclusive du dossier papier. À l'inverse, seule une minorité des professionnels interrogés (7,6 %) travaille dans des structures entièrement numérisées, traduisant une adoption encore limitée des SIH pleinement intégrés.

Cette configuration reflète la persistance de modèles dits hybrides, caractérisés par la coexistence de systèmes papier et numériques au sein d'un même établissement ou d'un même parcours de soins. Elle s'inscrit dans les constats formulés par l'OMS qui souligne que, dans de nombreux systèmes de santé, en particulier dans les pays à revenu faible ou intermédiaire, la transition numérique reste progressive, fragmentée et inégalement déployée, en raison de contraintes liées aux infrastructures, à l'interopérabilité des systèmes, à la gouvernance des données et à la formation des professionnels (37).

À l'échelle internationale, cette situation contraste avec celle observée dans certains pays ayant atteint des niveaux d'adoption plus avancés. Ainsi, aux États-Unis, près de 96 % des hôpitaux non fédéraux et environ 78 % des médecins exerçant en cabinet utilisent des dossiers médicaux électroniques certifiés, traduisant une informatisation largement généralisée du système de santé (38). En Europe, environ 87 % des États membres disposent d'un dossier de santé électronique national ou de systèmes interconnectés, bien que le degré d'intégration et d'usage effectif varie selon les pays (39). Ces données illustrent une digitalisation plus aboutie, tout en mettant en évidence des défis persistants liés à l'interopérabilité, à la sécurité et à la gouvernance des données.

Ainsi, les résultats de notre étude situent le contexte marocain dans une phase intermédiaire de transition numérique, caractérisée par une informatisation partielle et la coexistence prolongée de pratiques papier et numériques. Cette situation peut limiter les bénéfices attendus des SIH, notamment en matière de continuité de l'information, de traçabilité et d'efficacité des soins, tout en générant une complexité organisationnelle accrue pour les professionnels de santé.

2. Impact perçu des SIH sur la continuité et la coordination des soins

Malgré une digitalisation encore partielle des systèmes d'information hospitaliers, les perceptions exprimées par les médecins interrogés mettent clairement en évidence les bénéfices cliniques et organisationnels associés à l'usage des SIH, en particulier en matière de continuité et de coordination des soins. Ces résultats rejoignent les données de la

littérature internationale, qui montrent que même des systèmes partiellement déployés peuvent améliorer l'accès à l'information clinique, réduire les ruptures informationnelles et soutenir des décisions médicales plus cohérentes au sein des équipes de soins (40).

Dans notre étude, l'amélioration de la qualité et de la continuité des soins constitue le bénéfice le plus largement reconnu, avec 76,6 % des médecins exprimant une perception favorable. Ce résultat s'inscrit pleinement dans les fourchettes rapportées à l'échelle internationale, généralement comprises entre 70 et 80 %, où la digitalisation est associée à une meilleure disponibilité des données médicales, à une réduction des pertes d'information et à une continuité accrue de la prise en charge, en particulier dans les parcours de soins complexes (41). Cette convergence suggère que, même dans des contextes de digitalisation incomplète, les apports cliniques des SIH sont clairement perceptibles par les professionnels de santé.

De manière similaire, la facilitation de la coordination des soins est fortement reconnue par les médecins interrogés, avec **75,9 %** de perceptions favorables. Ce niveau est comparable à celui rapporté dans la littérature internationale, où les taux varient généralement entre **65 et 75 %** (42). Cette perception reflète le rôle central des outils numériques dans le partage transversal de l'information entre services et professionnels, et rejoint les travaux soulignant que l'accès partagé aux données médicales favorise une coordination plus fluide et une meilleure cohérence des décisions cliniques (43).

L'amélioration de la sécurité clinique est également perçue de manière favorable par **68,7 %** des répondants, un niveau cohérent avec les données internationales, rapportées entre **60 et 70 %** (44). Cette perception suggère que les professionnels associent les dossiers médicaux informatisés à une réduction des erreurs liées à la lisibilité, à la perte d'informations ou à la redondance d'examens, comme décrit dans les travaux de **Menachemi et Collum**. Il convient toutefois de souligner que cette amélioration perçue concerne principalement la sécurité des processus cliniques, et ne préjuge pas nécessairement d'un niveau élevé de sécurité informatique ou de protection des données.(45)

Concernant l'évaluation globale du rapport bénéfices–risques, **64,7 %** des médecins estiment que les bénéfices de la digitalisation l'emportent sur les risques, un résultat proche des valeurs rapportées dans la littérature internationale, généralement comprises entre **55 et 65 %** (46). Cette appréciation traduit une acceptation globalement favorable des SIH, tout en laissant apparaître une conscience des risques associés à leur usage, notamment en matière de confidentialité et de cybersécurité, comme le soulignent les travaux de **Greenhalgh et al.** (20).

En revanche, la traçabilité des accès aux dossiers médicaux constitue un point de divergence notable entre notre étude et les données internationales. Seuls **27,5 %** des médecins interrogés perçoivent la traçabilité comme un bénéfice effectif des SIH, contre des taux compris entre **55 et 65 %** dans la littérature internationale (47). Cet écart suggère une intégration incomplète ou peu visible des fonctionnalités avancées de traçabilité dans le contexte étudié. Il peut refléter l'absence de mécanismes de journalisation accessibles aux utilisateurs, un déficit de formation sur ces fonctionnalités ou encore une gouvernance insuffisamment formalisée des accès aux données médicales.

Le tableau 7 et la figure 17 présentent une comparaison des avantages perçus de la digitalisation des données médicales dans notre étude et dans d'autres contextes.

Tableau 7 : Bénéfices perçus de la digitalisation des données médicales selon les professionnels de santé, comparés aux données de la littérature internationale

Dimensions	Notre étude – professionnels de santé Marrakech (%)	Littérature internationale (%)	Références
Amélioration de la qualité et de la continuité des soins	76,6	70-80	(41)
Facilitation de la coordination des soins	75,9	65-75	(42 ; 43)
Amélioration de la sécurité clinique	68,7	60-70	(44)
Bénéfices perçus supérieurs aux risques	64,7	55-65	(46)
Traçabilité des accès aux dossiers médicaux	27,5	55-65	(47)

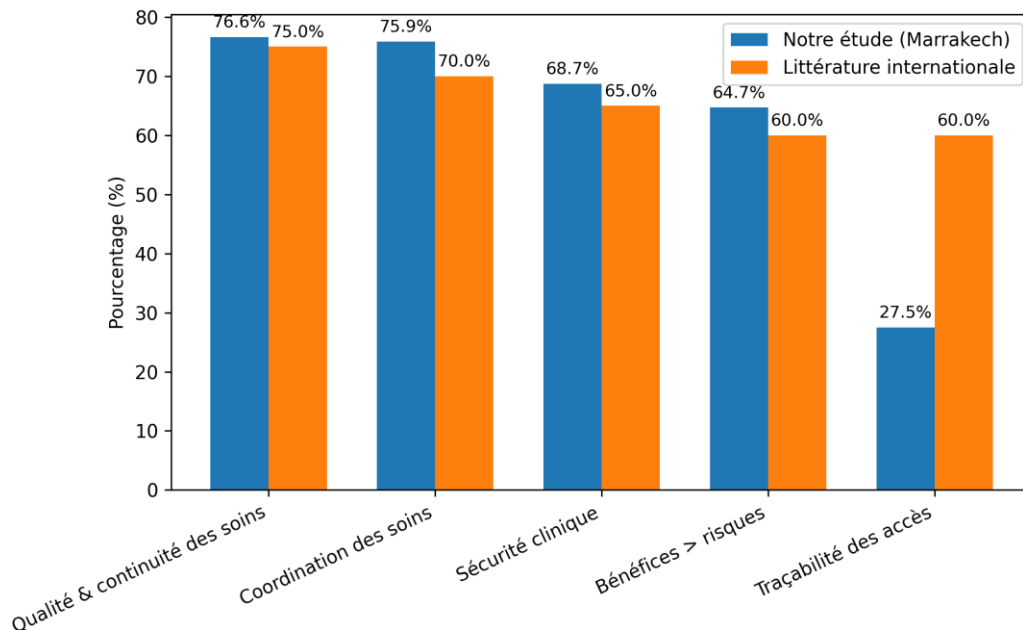


Figure 17 : Analyse comparative des bénéfices perçus de la digitalisation des données médicales selon les professionnels de santé et la littérature internationale

3. Contraintes institutionnelles et disparités public-privé

La forte représentation du secteur public dans notre échantillon, qui regroupe 86,3 % des médecins interrogés, impose de replacer ces résultats dans un contexte institutionnel spécifique, marqué par des contraintes structurelles importantes. Cette prédominance du secteur public constitue un élément explicatif majeur du niveau intermédiaire d'adoption des SIH observé dans notre étude, caractérisé par la persistance de modèles hybrides et une informatisation incomplète des processus cliniques.

Les supports d'accès aux données numériques corroborent cette lecture. Certes, l'ordinateur de l'établissement est bien le principal moyen d'accès ($n = 190$), une partie non infime des professionnels utilise des supports personnels, en particulier, des ordinateurs ($n = 80$) et des smartphones ($n = 60$). Ce phénomène, qui fait recours à des équipements non institutionnels, peut avoir des causes pratiques : l'entretien du poste informatique est insuffisant, il n'y en a pas dans l'un de nos services, on recherche une solution plus rapide ou plus accessible, etc. Cependant, elle pose des enjeux cruciaux sur la sécurité des données et

la gouvernance des accès, surtout lorsque ces supports ne sont pas sous les mêmes standards de sécurité que les outils institutionnels.

Dans sa Stratégie mondiale sur la santé numérique 2020–2025, l'OMS rapporte que, dans de nombreux pays à revenu intermédiaire, les établissements publics de santé sont confrontés à des **contraintes budgétaires persistantes**, à des **processus décisionnels institutionnels complexes** et à une **charge de travail élevée**, limitant leur capacité à déployer des systèmes d'information hospitaliers complets, intégrés et interopérables. L'OMS souligne également que ces contraintes freinent les investissements dans l'infrastructure numérique, la maintenance des systèmes et la formation des professionnels, affectant ainsi l'usage effectif et sécurisé des technologies numériques en santé (37).

À l'inverse, le **secteur privé**, qui ne représente que **13,7 %** des répondants dans notre étude, dispose généralement de **ressources financières et organisationnelles plus importantes**, favorisant l'adoption de solutions numériques plus ergonomiques et modulables. Ce contraste entre secteurs public et privé est également décrit dans les analyses régionales de l'OMS portant sur la région **MENA**, qui mettent en évidence des **disparités d'accès à l'information clinique numérisée** et des niveaux variables de maturité des systèmes d'information selon le type d'établissement. Ces inégalités organisationnelles sont susceptibles d'influencer indirectement la qualité, la continuité et la sécurité des soins, indépendamment des compétences individuelles des professionnels.(48)

4. Fragmentation régionale et limites de l'intégration nationale

Les expériences régionales dans la région MENA mettent en évidence que la fragmentation des SIH constitue un obstacle majeur à la transformation numérique en santé. En Égypte, les travaux de **Alorbany et al.** rapportent que, malgré le déploiement progressif de dossiers médicaux électroniques dans de nombreux établissements hospitaliers, l'absence d'une architecture nationale unifiée limite encore fortement l'interopérabilité entre structures et l'exploitation des données de santé à grande échelle, réduisant ainsi l'impact organisationnel et clinique attendu des systèmes d'information hospitaliers (49).

De manière comparable, les études menées en Tunisie, notamment celles de **Ben Romdhane et al.**, décrivent une digitalisation centrée sur des modules fonctionnels isolés, tels que les systèmes de laboratoire, de facturation ou d'imagerie médicale, sans intégration complète du parcours patient ni vision transversale des données cliniques. Cette approche modulaire limite les bénéfices en matière de continuité et de coordination des soins et freine l'émergence de systèmes d'information hospitaliers pleinement intégrés.(50)

Ces constats contrastent avec les modèles observés dans plusieurs pays européens, où la maturité numérique des systèmes de santé apparaît plus avancée. Dans la région OMS Europe, la diffusion des dossiers de santé électroniques s'appuie sur des cadres réglementaires robustes, des standards nationaux d'interopérabilité et des mécanismes de gouvernance structurés, favorisant l'échange sécurisé et longitudinal des données médicales entre professionnels et établissements (51). Ces expériences soulignent que la réussite des systèmes d'information hospitaliers repose sur une articulation étroite entre technologie, réglementation, gouvernance des données, formation des professionnels et accompagnement du changement.

Dans cette perspective, les recommandations formulées par l' OMS rappellent que la numérisation des systèmes de santé constitue avant tout un projet organisationnel et stratégique de long terme, nécessitant une vision nationale intégrée plutôt qu'une juxtaposition d'initiatives locales ou sectorielles (52). L'analyse conjointe des expériences régionales et européennes met ainsi en évidence que l'enjeu central de la transformation numérique réside moins dans le niveau d'équipement que dans la capacité des systèmes de santé à assurer une intégration cohérente, interopérable et gouvernée des données médicales.

5. Charge administrative et paradoxes de l'adoption des systèmes d'information hospitaliers

L'analyse met en évidence un **paradoxe central de l'adoption des systèmes d'information hospitaliers** : alors que leurs bénéfices cliniques et organisationnels sont largement reconnus par les professionnels, leur usage reste associé à une **perception**

persistante d'augmentation de la charge administrative. Dans notre étude, **35,0 %** des médecins expriment un accord ou un fort accord avec l'affirmation selon laquelle l'informatisation accroît la charge administrative, tandis qu'une proportion non négligeable adopte une position intermédiaire. Ce constat est cohérent avec les observations rapportées par **Cresswell et Sheikh**, qui décrivent une augmentation du temps consacré à la saisie des données, une duplication des tâches et une navigation complexe entre interfaces lorsque les systèmes sont partiellement intégrés ou insuffisamment ergonomiques (53). De manière similaire, les rapports de l'OMS soulignent que la coexistence de supports papier et numériques dans les phases de transition génère une **double charge documentaire**, susceptible d'altérer l'adhésion des professionnels aux SIH (37).

Au-delà de la charge administrative, l'analyse des **contraintes et des risques perçus** associés à la digitalisation des données médicales révèle des préoccupations majeures d'ordre **sécuritaire et organisationnel**, globalement concordantes avec les données internationales. Le **risque de fuite massive de données** constitue la principale inquiétude exprimée par les médecins interrogés, avec **71,8 %** des répondants se déclarant en accord ou en fort accord avec cette affirmation. Ce niveau apparaît légèrement supérieur à celui rapporté dans plusieurs enquêtes internationales, notamment celles analysées par **Kruse et al.** et **Jalali et al.**, qui mettent en évidence une sensibilité croissante des professionnels de santé aux cybermenaces dans un contexte marqué par la multiplication des cyberattaques ciblant les établissements de santé et par une médiatisation accrue des incidents de sécurité (54,55).

Par ailleurs, **64,0 %** des médecins estiment que la digitalisation facilite l'accès non autorisé à des informations médicales sensibles, et **58,5 %** considèrent qu'elle favorise des consultations injustifiées des dossiers médicaux. Ces proportions sont proches de celles rapportées par **Appari et Johnson** et **Rindfleisch et al.**, qui décrivent des vulnérabilités persistantes liées à la gestion des droits d'accès, à l'utilisation d'identifiants partagés et à l'insuffisance des mécanismes de traçabilité dans les systèmes d'information hospitaliers (56,57). Ces résultats traduisent une perception de fragilité des dispositifs de contrôle des accès, particulièrement marquée dans les contextes de digitalisation partielle.

Enfin, la **confiance dans la sécurité informatique des systèmes d'information hospitaliers** apparaît particulièrement faible dans notre étude, avec seulement **22,7 %** des médecins exprimant un accord ou un fort accord avec cette affirmation. Ce niveau est nettement inférieur à ceux rapportés dans les pays disposant de systèmes plus matures, où la confiance des professionnels est renforcée par l'existence de cadres de gouvernance formalisés, de politiques de sécurité visibles et de formations institutionnalisées. Cet écart suggère que, dans le contexte étudié, la digitalisation incomplète des systèmes, associée à un **déficit de formation**, de **sensibilisation** et de **gouvernance de la sécurité**, contribue à une perception accrue de vulnérabilité (58).

Dans l'ensemble, ces résultats mettent en évidence que les **risques perçus de la digitalisation des données médicales** demeurent importants et parfois amplifiés dans notre contexte. Ils soulignent la nécessité d'une approche intégrée de la transformation numérique, reposant sur une **meilleure intégration des systèmes**, une **réduction de la charge administrative induite**, le **renforcement des dispositifs de sécurité** et le développement de **programmes de formation structurés**, condition indispensable à une adoption durable et sécurisée des systèmes d'information hospitaliers.

(Tableau 8 et Figure 18)

Tableau 8 : Contraintes et risques perçus liés à la digitalisation des données médicales

Contraintes / risques	Notre étude (%)	Littérature internationale (%)	Références
Augmentation de la charge administrative	35,0	30-45	(53)
Risque de fuite massive de données	71,8	60-70	(54 ; 55)
Accès non autorisé à des informations sensibles	64,0	55-65	(56)
Consultations injustifiées facilitées par l'accès numérique	58,5	50-60	(57)
Faible confiance dans la sécurité des SIH	22,7	40-55	(58)

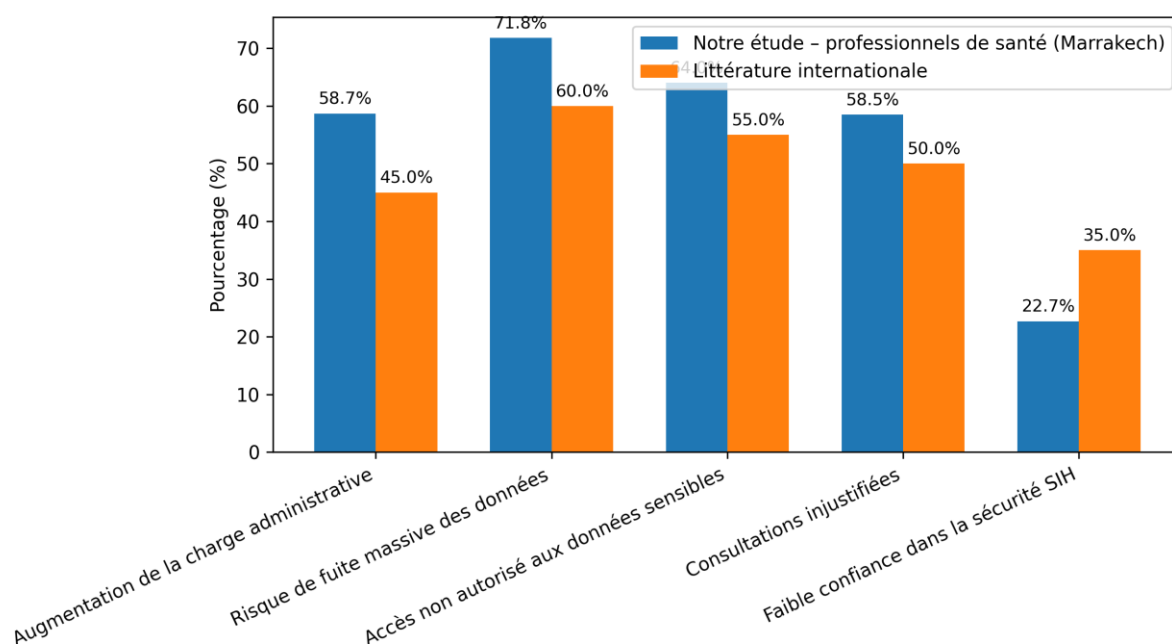


Figure 18 : Contraintes et risques perçus liés à la digitalisation des données médicales, comparaison entre notre étude et la littérature internationale

Au Total, l'adoption des systèmes d'information hospitaliers au Maroc se situe à un stade intermédiaire de la transition numérique. Les bénéfices cliniques et organisationnels sont clairement identifiés par les professionnels, mais la numérisation demeure hétérogène, fragmentée et génératrice de charges administratives persistantes. La confrontation de ces résultats aux expériences régionales et européennes souligne que l'évolution vers des SIH intégrés et interopérables dépend autant de stratégies nationales cohérentes, de gouvernance des données, de ressources humaines formées et d'infrastructures adaptées que de solutions technologiques en tant que telles.

III. Cybersécurité en santé au Maroc : responsabilité individuelle et gouvernance institutionnelle :

Dans notre étude, l'insuffisance de formation structurée et l'absence de cadres opérationnels clairement formalisés contribuent à un **transfert implicite de la responsabilité de la sécurité numérique vers le professionnel individuel**. Dans un contexte clinique contraint par la charge de travail et l'urgence décisionnelle, la protection des données médicales repose alors sur des **arbitrages personnels**, réalisés sans soutien institutionnel structuré, exposant les professionnels à des dilemmes récurrents entre exigences de sécurité et impératifs de continuité des soins.

Cette problématique est analysée de manière approfondie par L'OMS qui considère la cybersécurité en santé comme un **enjeu systémique et organisationnel**, et non comme une responsabilité individuelle isolée. L'OMS souligne que l'absence de politiques institutionnelles claires, de procédures standardisées et de mécanismes de gouvernance favorise une **individualisation inappropriée de la responsabilité**, conduisant à des compromis défavorables entre conformité sécuritaire et efficacité clinique (58).

Cette analyse est renforcée par les travaux de **Greenhalgh et al.**, dans le cadre du modèle NASSS, qui montrent que l'échec ou la fragilité des technologies numériques complexes en santé est fréquemment lié à une **insuffisante prise en compte des dimensions organisationnelles et de gouvernance**, plutôt qu'à des limitations techniques. Selon ces auteurs, lorsque les responsabilités ne sont pas clairement distribuées au niveau institutionnel, les professionnels développent des stratégies adaptatives individuelles, augmentant l'hétérogénéité des pratiques et les risques de non-conformité (20).

De manière complémentaire, **Cresswell et Sheikh** mettent en évidence que l'absence de gouvernance explicite des systèmes d'information hospitaliers conduit à une **fragmentation des responsabilités**, où la sécurité des données devient implicitement intégrée aux pratiques cliniques quotidiennes, sans cadre normatif partagé. Cette situation favorise une tension

structurelle entre performance clinique et sécurité numérique, au détriment d'une gestion collective et anticipée des risques (53).

Enfin, les recommandations conjointes de l'OMS et de l'**Organisation de Coopération et de Développement Économiques** insistent sur le fait que la cybersécurité en santé doit être envisagée comme une **responsabilité institutionnelle intégrée**, reposant sur des politiques claires, des procédures opérationnelles, des mécanismes de contrôle et une culture organisationnelle partagée, plutôt que sur la seule vigilance individuelle des professionnels.(59)

Ainsi, les résultats de notre étude s'inscrivent dans une convergence internationale montrant que la **sécurisation des données médicales ne peut être durablement assurée sans une gouvernance institutionnelle forte**, capable d'encadrer, de soutenir et d'harmoniser les pratiques individuelles. Le renforcement de cette gouvernance apparaît comme un levier central pour réduire les pratiques à risque, sécuriser l'usage des technologies numériques et préserver la confiance des professionnels et des patients dans les systèmes d'information de santé.

Au Maroc, la CNDP joue un rôle actif dans la sensibilisation et la promotion de la protection des données, y compris dans le secteur de la santé. Toutefois, ces actions demeurent insuffisamment intégrées aux curricula initiaux et continus des professionnels de santé, limitant leur impact opérationnel (60).

Cette situation crée une tension structurelle entre, d'une part, un cadre réglementaire et institutionnel existant et, d'autre part, une faible institutionnalisation des compétences en cybersécurité et en gouvernance des données comme prérequis de la pratique clinique numérique. L'OMS recommande à ce titre des politiques nationales concertées combinant normes réglementaires, standards de formation, mécanismes de certification et dispositifs d'évaluation continue des compétences (37).

En résumé, l'analyse des compétences numériques des professionnels de santé met en évidence une **fracture pédagogique et organisationnelle** au cœur de la transformation digitale en santé. L'aisance informatique déclarée ne se traduit pas automatiquement en compétence

opérationnelle pour gérer les enjeux spécifiques de la protection des données médicales et de la cybersécurité.

Cette dissociation favorise l'émergence de pratiques à risque, exposant les établissements et les patients à des violations potentielles de la confidentialité et de la sécurité des données. Les orientations convergentes de l'OMS et les initiatives de la CNDP soulignent une exigence stratégique claire : **institutionnaliser la formation continue en santé numérique**, en l'ancrant dans les parcours professionnels, la gouvernance des données et les stratégies nationales de digitalisation (52,60).

IV. Perceptions éthiques et respect du secret médical

1. Continuité des soins versus confidentialité : une tension éthique structurelle

L'analyse des perceptions éthiques des professionnels de santé met en évidence, dans notre étude, une tension structurelle entre les impératifs de continuité et d'efficacité des soins dans un environnement numérique et les exigences fondamentales de respect du secret médical et de protection des données personnelles. Cette tension ne relève pas d'un débat théorique abstrait, mais s'inscrit dans des situations concrètes de pratique clinique, comme en témoigne le fait que **52,9 %** des médecins interrogés déclarent ressentir un conflit entre la nécessité de partager l'information pour assurer la continuité des soins et le respect strict de la confidentialité du patient.

Dans des contextes cliniques caractérisés par une charge de travail élevée, une pression temporelle importante et une organisation souvent fragmentée des soins, les outils numériques sont largement perçus comme des facilitateurs indispensables de la communication interprofessionnelle. Cette perception est cohérente avec les résultats de notre étude, dans laquelle **75,9 %** des médecins estiment que la digitalisation facilite la coordination des soins, et **76,6 %** qu'elle améliore la qualité et la continuité de la prise en charge. Ces bénéfices cliniques renforcent l'acceptabilité des technologies numériques, mais contribuent également à banaliser des pratiques de partage de l'information dont le cadre éthique et sécuritaire n'est pas toujours clairement défini.

L'OMS souligne que la rapidité de circulation de l'information médicale constitue un déterminant majeur de la qualité et de la sécurité des soins, en particulier dans les situations d'urgence, de prise en charge multidisciplinaire ou de transitions entre services (52,37). Toutefois, l'OMS insiste également sur le fait que cette circulation de l'information doit s'inscrire dans des dispositifs sécurisés et gouvernés, afin d'éviter que l'amélioration de l'efficacité clinique ne se fasse au détriment des principes éthiques fondamentaux.

Dans notre étude, cette ambivalence se traduit par des perceptions et des pratiques parfois contradictoires : si le secret médical est considéré comme prioritaire par 81,4 % des médecins, y compris face aux demandes administratives, une proportion non négligeable reconnaît néanmoins des pratiques susceptibles de l'entamer, notamment dans des situations perçues comme urgentes ou organisationnellement contraignantes. Cette coexistence d'une forte adhésion aux principes éthiques et de pratiques de contournement reflète une tension éthique structurelle, exacerbée par la digitalisation des données de santé en l'absence de cadres institutionnels clairs et de formations adaptées.

Ainsi, les résultats de notre étude confirment que la digitalisation des systèmes d'information hospitaliers, tout en améliorant la continuité et la coordination des soins, reconfigure profondément les modalités d'application du secret médical. Cette évolution impose une réflexion éthique renouvelée, intégrant à la fois les exigences de performance clinique et les impératifs de confidentialité, et souligne la nécessité d'une gouvernance explicite des usages numériques afin de soutenir les professionnels dans leurs arbitrages quotidiens.

2. Pratiques numériques à risque et fragilisation du secret médical

Les résultats de notre enquête mettent en évidence une perception élevée des risques éthiques associés à certaines pratiques numériques courantes, en particulier l'usage de messageries grand public et le partage d'identifiants d'accès aux systèmes d'information hospitaliers. En effet, 34,0 % des médecins interrogés estiment acceptable, dans certaines situations urgentes, l'envoi d'informations médicales identifiantes via des messageries non

sécurisées, tandis que 45,8 % déclarent avoir déjà communiqué leurs identifiants à un collègue. Ces pratiques traduisent une fragilisation des principes de confidentialité et de responsabilité individuelle, malgré une adhésion théorique forte au respect du secret médical.

Ces comportements s'inscrivent dans ce que Cresswell et al. et Greenhalgh et al. décrivent comme des contournements organisationnels (workarounds), définis comme des adaptations informelles mises en œuvre par les professionnels afin de faire face aux contraintes organisationnelles, techniques ou temporelles. Selon ces auteurs, ces pratiques ne relèvent pas d'une volonté délibérée de transgression, mais répondent à des impératifs d'efficacité immédiate et de continuité des soins, en particulier lorsque les outils institutionnels sont perçus comme insuffisamment accessibles, ergonomiques ou adaptés aux réalités du terrain (61).

Sur le plan éthique et sécuritaire, ces usages ont toutefois des conséquences majeures sur la gouvernance des données médicales. Ils compromettent la confidentialité des informations de santé, rendent la traçabilité des accès difficile, voire impossible, et diluent la responsabilité individuelle en cas d'incident. Dans notre étude, cette fragilité est cohérente avec la faible proportion de médecins percevant la traçabilité des accès comme effective (27,5 %), suggérant une insuffisante visibilité ou appropriation des mécanismes de contrôle existants.

Des études menées en Europe et en Amérique du Nord rapportent des constats similaires, identifiant le recours à des outils non institutionnels pour le partage d'informations cliniques comme l'un des facteurs les plus fréquemment associés aux violations de données en milieu hospitalier (1). Ces travaux soulignent que la persistance de telles pratiques reflète moins un déficit éthique individuel qu'un désalignement entre les exigences de la pratique clinique et les cadres techniques et organisationnels disponibles.

Ainsi, les résultats de notre étude confirment que la prévention des pratiques numériques à risque ne peut reposer uniquement sur des rappels normatifs ou des injonctions individuelles. Elle nécessite une approche systémique, intégrant l'amélioration des outils institutionnels, la clarification des procédures, la formation des professionnels et une

gouvernance éthique explicite, afin de réduire le recours aux contournements organisationnels tout en préservant la continuité et la qualité des soins.

3. Cadre juridique marocain et exigences de conformité éthique

Au Maroc, la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue le socle juridique de la protection des données médicales. Elle impose des principes stricts de licéité, de finalité, de proportionnalité, de transparence et de sécurité, avec un régime renforcé pour les données sensibles, dont les données de santé (7).

La loi prévoit notamment des obligations de déclaration ou d'autorisation préalable auprès de la CNDP ainsi que la mise en place de mesures techniques et organisationnelles adaptées. Ces exigences trouvent un prolongement direct dans le Code de déontologie médicale marocain, qui érige le secret professionnel en obligation éthique absolue, indépendante du support ou du mode de transmission de l'information médicale.

La convergence entre les cadres juridique et déontologique est claire : la continuité des soins ne saurait justifier une suspension implicite des garanties de confidentialité. Comme le soulignent plusieurs analyses doctrinales, le numérique ne modifie pas la nature du secret médical, mais en complexifie profondément les modalités d'application (62,63).

4. Consentement éclairé et autonomie du patient à l'ère numérique

Un autre enjeu éthique majeur mis en évidence par notre étude concerne la mise en œuvre effective du consentement éclairé dans le contexte des pratiques numériques. Bien que le cadre juridique national, notamment la loi marocaine n°09-08, pose le consentement de la personne concernée comme fondement du traitement des données médicales, ce principe apparaît, dans la pratique, insuffisamment formalisé et inégalement appliqué. Ainsi, seuls 23,0 % des médecins interrogés estiment que les patients sont informés du fait que leurs données sont conservées dans des systèmes numériques, tandis que 46,7 % expriment un désaccord ou un fort désaccord avec cette affirmation.

Cette insuffisance de l'information préalable du patient se retrouve également dans le cadre de l'utilisation secondaire des données. En effet, 52,2 % des répondants considèrent que l'utilisation des données de santé à des fins de recherche ou de registres épidémiologiques est expliquée aux patients et que leur consentement est recherché lorsque cela est requis, traduisant une hétérogénéité marquée des pratiques et une application partielle des exigences réglementaires.

Dans les environnements numériques de santé, la facilité de circulation, de duplication et de réutilisation des données accroît la responsabilité des professionnels et des institutions en matière d'information et de consentement. Shabani et al. soulignent que l'absence d'information claire et traçable du patient concernant les usages de ses données crée un double écart : juridique, au regard des obligations de protection des données personnelles, et éthique, en fragilisant la relation de confiance entre le patient et le système de soins (62).

Dans notre étude, cette tension se traduit par une reconnaissance croissante de la nécessité d'un contrôle renforcé par les patients eux-mêmes, puisque 68,8 % des médecins estiment que les patients devraient pouvoir limiter l'accès à certaines informations sensibles contenues dans leur dossier médical. Cette position témoigne d'une évolution des représentations professionnelles, intégrant progressivement le patient comme acteur de la gouvernance de ses données de santé.

Ainsi, nos résultats suggèrent que la digitalisation des données médicales, lorsqu'elle n'est pas accompagnée de dispositifs explicites d'information et de recueil du consentement, fragilise un principe éthique central de la pratique médicale. Le renforcement de procédures formalisées de consentement, adaptées aux usages numériques et intégrées aux systèmes d'information hospitaliers, apparaît dès lors indispensable pour concilier innovation technologique, respect des droits du patient et conformité aux exigences éthiques et juridiques.

5. Droits du patient, contrôle des données et confiance numérique

La loi marocaine n°09-08 reconnaît aux patients des droits fondamentaux sur leurs données personnelles, incluant notamment le droit d'accès, de rectification et d'opposition au traitement. Ces droits constituent un pilier central de la confiance numérique, laquelle conditionne l'acceptabilité sociale et éthique des systèmes d'information en santé, en particulier dans un contexte de digitalisation croissante des données médicales.

Or, les résultats de notre étude mettent en évidence un écart significatif entre ce cadre juridique et sa mise en œuvre effective dans la pratique clinique. En effet, seuls 23,0 % des médecins estiment que les patients sont informés du fait que leurs données sont conservées dans des systèmes numériques, tandis que 68,7 % considèrent au contraire que les patients sont insuffisamment informés sur l'utilisation de leurs données de santé. Cette insuffisance d'information contribue à limiter la capacité des patients à exercer pleinement leurs droits, pourtant garantis par la loi.

Par ailleurs, la question du contrôle effectif des données par le patient apparaît comme un enjeu éthique majeur. Dans notre étude, 68,8 % des médecins expriment leur accord avec l'idée que les patients devraient pouvoir limiter l'accès à certaines informations sensibles contenues dans leur dossier médical. Cette position traduit une reconnaissance croissante, au sein du corps médical, de la nécessité d'une gouvernance plus participative des données de santé, intégrant le patient comme acteur à part entière et non comme simple bénéficiaire passif des soins.

Ces résultats s'inscrivent dans la continuité des analyses de Shabani et al., qui montrent que la digitalisation des données médicales tend à accentuer l'asymétrie d'information entre institutions de santé et patients lorsque les dispositifs d'information, de transparence et de participation ne sont pas explicitement intégrés aux parcours de soins. Selon ces auteurs, l'absence de visibilité sur les usages des données fragilise la confiance des patients et peut compromettre l'acceptabilité des systèmes numériques, malgré leurs bénéfices cliniques potentiels (62,63).

Ainsi, nos résultats suggèrent que la consolidation de la confiance numérique ne repose pas uniquement sur la sécurité technique des systèmes d'information, mais également sur la capacité des institutions de santé à rendre effectifs les droits des patients en matière d'information, de contrôle et de participation aux décisions relatives à l'utilisation de leurs données. Le renforcement de dispositifs d'information clairs, accessibles et traçables apparaît dès lors comme une condition essentielle pour aligner la pratique clinique quotidienne avec les exigences juridiques et éthiques de la protection des données personnelles (69,70).

6. Pratiques numériques à risque : analyse comparative avec la littérature

L'analyse comparative entre les résultats de notre enquête menée auprès des professionnels de santé de Marrakech et les données issues de la littérature internationale met en évidence des convergences marquées tant dans la nature que dans la fréquence des pratiques numériques à risque associées à la gestion des données médicales (tableau 6).

En premier lieu, l'usage de messageries non sécurisées pour l'échange d'informations cliniques apparaît comme une pratique largement répandue. Dans notre étude, 34,0 % des médecins interrogés déclarent juger acceptable, dans certaines situations urgentes, l'envoi d'informations médicales identifiantes via des messageries grand public. Ce résultat est comparable à celui rapporté par Tikanmäki, qui estime qu'environ 40 % des professionnels de santé ont recours à des applications de messagerie non institutionnelles pour des échanges cliniques (19). Cette convergence suggère que le recours à ces outils constitue un phénomène transversal, étroitement lié aux impératifs de rapidité, de disponibilité et de coordination interprofessionnelle, indépendamment du contexte géographique ou institutionnel.

De même, le partage d'identifiants professionnels ou l'utilisation des accès d'un collègue représente une vulnérabilité significative dans notre population étudiée. Dans notre enquête, 45,8 % des médecins déclarent avoir déjà communiqué leurs identifiants à un collègue. Ces proportions sont supérieures, mais comparables, à celles rapportées par Bryant, qui estime que 30 à 35 % des professionnels de santé partagent leurs identifiants dans les établissements hospitaliers (65). Cette pratique, souvent motivée par des contraintes

organisationnelles ou des limitations ergonomiques des systèmes d'information hospitaliers, compromet directement la traçabilité des accès et la responsabilité individuelle, pourtant centrales dans la gouvernance des données médicales.

Le stockage local non sécurisé de données patients constitue également un point de convergence notable. Dans notre étude, 27,6 % des répondants reconnaissent stocker des documents patients sur des supports non sécurisés, tandis que 32,1 % déclarent transférer des données médicales vers des supports personnels. Ces résultats sont proches de ceux rapportés par Netschert et al, qui montrent qu'environ 45 % des professionnels de santé conservent des informations sensibles sur des supports locaux ou personnels insuffisamment protégés (66), et rejoignent également les constats formulés par l'OMS concernant la persistance de pratiques de stockage à risque dans les systèmes de santé en cours de digitalisation (67). Cette similitude met en évidence une vulnérabilité structurelle commune, résultant à la fois de pratiques individuelles inadaptées et d'insuffisances des infrastructures institutionnelles de stockage sécurisé.

Par ailleurs, la question du consentement éclairé dans les usages numériques révèle une tendance préoccupante. Dans notre étude, seuls 23,0 % des médecins estiment que les patients sont informés que leurs données sont conservées dans des systèmes numériques, tandis que 52,2 % considèrent que l'utilisation des données à des fins de recherche est expliquée aux patients lorsque cela est nécessaire. Ces résultats sont cohérents avec ceux rapportés par CaseGuard, selon lesquels près de 50 % des usages numériques des données médicales reposent sur un consentement implicite ou insuffisamment documenté, un constat également mis en évidence dans les analyses de l'OMS (68). Cette situation souligne un écart persistant entre les exigences juridiques et éthiques et la réalité des pratiques cliniques quotidiennes, notamment dans des contextes d'urgence ou de communication informelle.

Enfin, l'absence ou l'insuffisance de signalement des incidents de cybersécurité constitue l'un des écarts les plus marqués, tant au niveau local qu'international. Dans notre étude, seuls 19,9 % des médecins déclarent savoir à qui signaler un incident de cybersécurité, tandis que 47,8 % expriment un désaccord ou un fort désaccord avec cette

affirmation. Ces résultats rejoignent les estimations issues des rapports conjoints de l'ENISA et de l'ECSO, selon lesquels plus de 60 % des incidents de cybersécurité en milieu de santé ne font pas l'objet d'un signalement formel (69,70). Cette convergence traduit l'existence d'une culture de la sécurité encore largement réactive, plutôt que proactive, au sein des établissements de santé, et met en évidence la nécessité de renforcer les dispositifs de sensibilisation, de formation et de gouvernance des incidents (Tableau 6).

Tableau 9 : Comparaison des pratiques numériques à risque observées dans notre étude et dans la littérature internationale

Pratique à risque	Résultats de notre étude (FMPM)	Résultats d'autres études	Références
Usage de messageries non sécurisées pour le partage d'informations cliniques	≈ 62 % des professionnels déclarent utiliser des messageries grand public (ex. WhatsApp) pour des échanges cliniques	45-55 % des professionnels de santé utilisent des applications non sécurisées pour la communication clinique	(19)
Partage d'identifiants d'accès aux SIH	≈ 62 % utilisent des identifiants partagés ou ceux d'un collègue	30-41 % rapportent le partage d'identifiants dans les hôpitaux	(65)
Stockage local non sécurisé de données médicales	≈ 48 % déclarent stocker des données patients sur des supports personnels	28-38 % des professionnels conservent des données cliniques sur des dispositifs locaux non chiffrés	(66)
Consentement implicite ou insuffisamment documenté pour les usages numériques	≈ 57 % estiment que le consentement numérique est rarement formalisé	40-50 % des usages numériques reposent sur un consentement implicite ou incomplet	(68)
Absence de signalement formel des incidents de sécurité	≈ 64 % déclarent ne pas connaître ou ne pas utiliser de procédure de signalement	50-65 % des incidents ne sont pas officiellement signalés en milieu hospitalier	(69,70)

Au total, la confrontation des perceptions des soignants, des cadres juridiques marocains et des exigences éthiques met en lumière une zone de friction persistante entre la

promesse des outils numériques et la réalité des pratiques cliniques. Les usages à risque identifiés apparaissent moins comme des transgressions volontaires que comme des réponses adaptatives à des contraintes organisationnelles fortes.

Toutefois, ces adaptations produisent des effets juridiquement et éthiquement problématiques lorsqu'elles se substituent à des dispositifs de gouvernance formalisés. La protection du secret médical à l'ère numérique ne peut reposer uniquement sur la vigilance individuelle des soignants ; elle exige une articulation cohérente entre normes juridiques, dispositifs organisationnels et accompagnement éthique, condition indispensable à une digitalisation respectueuse des droits fondamentaux des patients.

V. Dimension cybersécurité et risques organisationnels

1. Perception du risque cyber chez les professionnels de santé

L'analyse de la dimension cybersécurité des systèmes d'information hospitaliers (SIH) met en évidence, dans notre étude, une perception élevée du risque cyber chez les professionnels de santé, sans que cette conscience du danger ne s'accompagne systématiquement de dispositifs opérationnels clairement identifiés ou pleinement fonctionnels de prévention et de gestion des incidents. En effet, 52,9 % des médecins interrogés estiment qu'une violation de données aurait un impact grave sur la confiance des patients, traduisant une sensibilité marquée aux conséquences éthiques et relationnelles des cyberincidents.

Toutefois, cette perception du risque contraste avec un faible niveau de confiance dans la sécurité des systèmes existants, puisque seuls 22,7 % des répondants déclarent avoir confiance dans la sécurité informatique de leur établissement, tandis que 46,0 % expriment un désaccord ou un fort désaccord. Cette dissociation entre conscience du risque et capacité perçue à le maîtriser constitue un constat récurrent dans la littérature internationale consacrée à la cybersécurité en santé.

À l'échelle mondiale, les établissements de santé figurent parmi les secteurs les plus exposés aux cybermenaces, notamment aux attaques par rançongiciel, au phishing ciblé et à

la compromission des systèmes d'information critiques (71). Cette vulnérabilité est largement expliquée par la valeur stratégique des données médicales, la dépendance des soins à la disponibilité des systèmes numériques et l'interconnexion croissante des infrastructures hospitalières. Les professionnels évoluent ainsi dans des environnements où le risque cyber est clairement identifié, mais où les outils, responsabilités et procédures de cybersécurité demeurent insuffisamment visibles ou structurés, comme le soulignent également les autorités sanitaires européennes (71).

2. Vulnérabilités techniques et pratiques numériques à risque

Les résultats de notre étude mettent en évidence plusieurs vulnérabilités techniques et pratiques numériques à risque, parmi lesquelles figure en premier lieu le stockage local non sécurisé de données médicales. En effet, 27,6 % des médecins déclarent stocker des documents patients sur des supports non sécurisés, tandis que 32,1 % reconnaissent transférer des données médicales vers des supports personnels. Ces pratiques exposent directement les données sensibles à des risques d'accès non autorisé, de perte ou d'exfiltration.

Ces résultats sont cohérents avec la littérature internationale, HE. Et al identifient le stockage local et l'usage de supports personnels comme l'un des vecteurs d'attaque les plus fréquents dans les organisations de santé (72). Lorsque les données sont conservées en dehors d'environnements centralisés et sécurisés, elles deviennent particulièrement vulnérables aux intrusions externes, aux accès internes non contrôlés et aux incidents accidentels. Les cybercriminels exploitent régulièrement ces failles, notamment en tirant parti de systèmes obsolètes, de configurations non mises à jour ou de dispositifs insuffisamment protégés, afin d'élever leurs privilèges et d'exfiltrer des informations sensibles (71).

Par ailleurs, ces vulnérabilités techniques s'inscrivent dans un contexte de pratiques numériques hybrides, marqué par la coexistence du papier et du numérique. Cette hybridation favorise des contournements pragmatiques des règles de sécurité, souvent motivés par des impératifs de continuité et de rapidité des soins, mais au détriment de la traçabilité des accès

et de la responsabilité individuelle, comme en témoigne la faible proportion de médecins percevant la traçabilité des accès comme effective (27,5 %).

3. Failles organisationnelles et déficit de gouvernance

Au-delà des aspects techniques, notre analyse met en évidence que les failles organisationnelles constituent un déterminant central de la vulnérabilité cyber des établissements de santé. L'absence ou la faible visibilité de procédures formalisées apparaît comme une faiblesse structurelle majeure. Ainsi, seuls 25,0 % des médecins interrogés déclarent connaître l'existence de règlements ou de procédures écrites encadrant l'utilisation des données médicales numériques, tandis que 54,0 % indiquent ne pas en avoir connaissance.

Ce déficit de gouvernance se traduit également par une faible culture du signalement des incidents. Dans notre étude, seuls 19,9 % des répondants déclarent savoir à qui signaler un incident de cybersécurité, alors que 47,8 % expriment un désaccord ou un fort désaccord avec cette affirmation. Cette absence de circuits de signalement clairement identifiés limite l'apprentissage organisationnel et empêche l'amélioration continue de la posture de sécurité.

Ces constats rejoignent les résultats de He et al. (2021), qui montrent que les incidents graves en milieu hospitalier résultent plus fréquemment de défaillances organisationnelles et humaines, absence de gouvernance structurée, responsabilités mal définies, procédures non documentées, que de vulnérabilités techniques isolées (72). À l'échelle internationale, les dispositifs de remontée des incidents et les équipes de réponse dédiées (CERT, CSIRT) sont pourtant identifiés comme des piliers essentiels de la résilience cyber des systèmes de santé (73).

Dans l'ensemble, les résultats de notre étude confirment que la cybersécurité hospitalière ne peut être appréhendée uniquement sous l'angle technique. Elle repose sur une articulation étroite entre perception du risque, pratiques professionnelles, organisation institutionnelle et gouvernance, soulignant la nécessité de renforcer simultanément la

formation, les procédures, les mécanismes de signalement et la responsabilité collective pour améliorer durablement la sécurité des systèmes d'information en santé.

4. Illustrations internationales des impacts cliniques et organisationnels

Les cyberattaques survenues ces dernières années dans des établissements de santé à l'échelle internationale illustrent de manière concrète le caractère multifactoriel et systémique du risque cyber. Des attaques par rançongiciel ont entraîné, dans plusieurs hôpitaux nord-américains et européens, des interruptions prolongées des systèmes d'information, le détournement d'ambulances, la suspension de services critiques et un retour contraint aux procédures papier, avec des retards de prise en charge et une dégradation de la qualité des soins (74-71).

- Ransomware paralysant plusieurs hôpitaux en Californie (2024)

Un groupe de cybercriminels a revendiqué le vol de 17 millions de dossiers patients dans une attaque par rançongiciel touchant trois hôpitaux du réseau PIH Health (Downey, Good Samaritan, Whittier) ainsi que des cliniques et services associés. Les interruptions IT ont perturbé les soins et forcé une réaction réglementaire. (75)

- Cyberattaque contre deux hôpitaux au Massachusetts (2025)

Deux hôpitaux communautaires (Heywood Hospital et Athol Hospital) ont subi une cyberattaque récente entraînant la mise hors ligne de leurs systèmes IT, le détournement des ambulances, et la suspension de services critiques comme la radiologie et les laboratoires. (76)

- Attaque ransomware contre un hôpital français (Corbeil-Essonnes, 2023)

Un rançongiciel a gravement perturbé le Centre hospitalier de Corbeil-Essonnes, forçant le personnel à revenir à des pratiques papier et retarder des interventions, avec une rançon demandée de 10 M\$ selon la presse. (77)

Ces exemples, bien que génériques et non liés à des institutions locales, démontrent la gravité potentielle des attaques cyber dans le secteur de la santé, où une violation de la confidentialité se conjugue souvent à une perturbation directe de la prise en charge des

patients et à des coûts organisationnels importants, tant financiers qu'opérationnels ou réputationnels.

5. Vers une gouvernance intégrée du risque cyber en santé

Les vulnérabilités mises en évidence dans notre étude soulignent que le renforcement de la cybersécurité hospitalière ne peut se limiter à l'implémentation de solutions technologiques isolées. Il nécessite une approche systémique intégrant infrastructures techniques, gouvernance organisationnelle et facteurs humains.

Sur le plan technique, les recommandations internationales préconisent la mise en œuvre de contrôles robustes, tels que le chiffrement des données au repos et en transit, l'authentification multi-facteurs, la segmentation des réseaux et la sécurisation des dispositifs médicaux connectés, afin de réduire la surface d'attaque (78).

Toutefois, ces mesures doivent être soutenues par une gouvernance institutionnelle forte, reposant sur des politiques claires de sécurité de l'information, une définition explicite des rôles et responsabilités (référents cybersécurité, comités de pilotage) et des procédures formalisées de gestion des incidents et de revue des accès. La littérature converge pour considérer que la gouvernance constitue le socle de la résilience cyber : sans leadership et sans cadre organisationnel structuré, les dispositifs techniques demeurent largement inefficaces.

Enfin, la formation continue et la gestion des accès représentent un levier central. L'application du principe du moindre privilège, associée à des mécanismes de traçabilité et d'audit, doit s'accompagner de programmes de formation ciblés sur l'hygiène numérique, la reconnaissance des menaces et le signalement obligatoire des incidents. De nombreuses études montrent que le facteur humain constitue à la fois la principale vulnérabilité et la première ligne de défense des SIH.

Au total, l'analyse de la cybersécurité dans les systèmes d'information hospitaliers met en lumière un paradoxe structurant : une perception élevée du risque cyber coexiste avec des vulnérabilités organisationnelles, techniques et culturelles persistantes. Le stockage local non

sécurisé, l'absence de procédures visibles et le déficit de signalement des incidents traduisent une maturité cyber encore insuffisante, dans laquelle la responsabilité de la sécurité repose excessivement sur les individus plutôt que sur des dispositifs institutionnels structurés.

Ce constat renforce la nécessité d'inscrire la cybersécurité hospitalière dans une stratégie nationale cohérente, articulant gouvernance, infrastructures résilientes, formation continue et politiques d'accès claires. Une telle approche apparaît indispensable pour garantir simultanément la sécurité des données médicales, la protection des patients et la continuité des soins dans un environnement numérique de plus en plus exposé (37).

VI. Mise en perspective avec la stratégie nationale de e-Santé

1. Ambition stratégique nationale et enjeux de maturité opérationnelle

La mise en perspective de nos résultats empiriques avec la stratégie nationale de e-Santé met en évidence un décalage structurel entre l'ambition politique affichée et le niveau de maturité opérationnelle observé au sein des établissements de santé. Cette situation n'est pas spécifique au contexte marocain. L'Organisation mondiale de la Santé souligne en effet que de nombreux pays engagés dans des programmes de santé numérique traversent une phase intermédiaire caractérisée par une adoption technologique rapide, mais une gouvernance encore incomplète des usages et des données (37).

Au Maroc, la feuille de route nationale de digitalisation du secteur de la santé vise à améliorer la continuité des soins, la coordination interprofessionnelle et le pilotage du système par les données (79). Toutefois, les résultats de notre étude suggèrent que la transformation numérique progresse davantage par superposition d'outils numériques que par une reconfiguration globale et cohérente des processus cliniques et organisationnels. Ce phénomène correspond à ce que Greenhalgh et al. décrivent comme une digitalisation fragmentée ou patchwork digitalization, dans laquelle les technologies sont déployées sans intégration systémique suffisante (20).

2. Le Dossier Patient Partagé: pilier stratégique et conditions de faisabilité

Le DPP constitue l'un des axes structurants de la stratégie nationale de e-Santé. Conçu comme un outil longitudinal, interopérable et sécurisé, il vise à centraliser l'information médicale du patient tout au long de son parcours de soins. Cette orientation est cohérente avec les recommandations internationales, l'OMS considérant le dossier médical électronique longitudinal comme un levier majeur d'amélioration de la qualité, de la sécurité et de la continuité des soins, à condition qu'il repose sur des standards robustes d'interopérabilité, de gouvernance et de protection des données (37).

Cependant, nos résultats mettent en évidence des conditions locales de mise en œuvre encore fragiles. La coexistence persistante du papier et du numérique, la traçabilité jugée insuffisante des accès et la diffusion limitée des identifiants personnels constituent autant d'obstacles à l'opérationnalisation d'un DPP pleinement fonctionnel. Comme le montrent plusieurs études européennes, un dossier partagé centralisé ne peut produire ses effets qu'à la condition que les systèmes d'information locaux soient eux-mêmes homogènes, sécurisés et correctement intégrés (80).

Ainsi, le DPP apparaît moins comme un simple projet technologique que comme un révélateur du niveau global de maturité numérique du système de santé. En l'absence d'une consolidation préalable des SIH locaux, des procédures et des compétences humaines, le risque est celui d'un outil central ambitieux mais difficilement appropriable sur le terrain.

3. Temporalité de la transformation numérique et charge organisationnelle

La stratégie nationale de e-Santé s'inscrit dans une dynamique volontariste de modernisation, mais nos données invitent à interroger la temporalité réelle de cette transformation. La persistance de pratiques hybrides papier/numérique et la perception d'une charge administrative accrue par une proportion significative de professionnels illustrent un phénomène largement documenté dans la littérature internationale : à court terme, l'introduction des systèmes numériques peut augmenter la complexité du travail clinique lorsqu'elle n'est pas accompagnée d'une refonte des processus (81).

Ce décalage entre objectifs stratégiques et réalités organisationnelles a également été observé dans plusieurs pays de la région MENA, où les initiatives de e-Santé se heurtent à des contraintes de ressources, de formation et de gouvernance, limitant l'impact réel des investissements technologiques (82). Dans ce contexte, la réussite de la feuille de route nationale dépend moins de la multiplication des outils que de leur intégration fonctionnelle et de leur alignement avec les pratiques cliniques quotidiennes.

4. Confiance numérique du patient : condition clé de réussite de la stratégie e-Santé

L'un des apports majeurs de notre étude réside dans la mise en évidence du rôle central de la confiance numérique du patient, encore fragile dans le contexte actuel. Les perceptions des professionnels indiquent que les patients sont jugés insuffisamment informés sur la conservation numérique de leurs données médicales ainsi que sur leurs droits d'accès, de limitation et de contrôle.

Ces constats s'inscrivent directement dans le cadre de la loi marocaine n°09-08, qui reconnaît aux personnes concernées des droits fondamentaux d'information, d'accès et de maîtrise de leurs données personnelles, ainsi que dans les recommandations de la CNDP, qui insiste sur la transparence et la responsabilisation des responsables de traitement (60).

La littérature internationale converge sur ce point : la réussite des programmes de santé numérique repose sur la confiance des citoyens, laquelle est conditionnée par la perception de la sécurité, de la confidentialité et de l'utilité des systèmes (37,83). La confiance limitée exprimée dans la sécurité informatique des établissements constitue ainsi un signal d'alerte majeur pour toute stratégie fondée sur la centralisation et le partage élargi des données, comme le DPP.

5. Une tension structurante entre ambition stratégique et réalité de terrain

La confrontation de nos résultats avec la stratégie nationale de e-Santé met en évidence une tension structurante. D'un côté, une ambition légitime de modernisation, d'interopérabilité et de pilotage du système de santé par la donnée ; de l'autre, une réalité de

terrain marquée par des pratiques hétérogènes, des compétences inégalement distribuées et une gouvernance encore incomplète.

Cette tension ne doit pas être interprétée comme un échec, mais comme une phase critique de transition, caractéristique des transformations numériques complexes. L'OMS souligne que les stratégies de e-Santé les plus efficaces sont celles qui investissent simultanément dans les infrastructures, les compétences humaines, les cadres juridiques et la relation de confiance avec les usagers (37).

6. Implications pour la stratégie nationale

En définitive, notre étude suggère que la stratégie nationale de e-Santé gagnerait à intégrer explicitement la confiance numérique du patient comme un indicateur de performance à part entière, au même titre que l'interopérabilité ou la couverture fonctionnelle des SIH. Sans cette confiance, construite par la transparence, la sécurité effective et le respect des droits des patients, le DPP risque de demeurer un projet techniquement ambitieux mais socialement fragile, exposé à des résistances implicites tant du côté des professionnels que des usagers.

VII. Forces, limites et perspectives de l'étude

1. Forces de l'étude

Cette étude présente plusieurs contributions significatives sur les plans scientifique et méthodologique. Elle figure parmi les premiers travaux menés au Maroc abordant de manière intégrée la digitalisation des données médicales en tenant compte simultanément des dimensions organisationnelles, cliniques, éthiques, juridiques et de cybersécurité, à partir des perceptions et des pratiques des médecins. Cette approche globale permet d'appréhender une problématique complexe, encore insuffisamment explorée dans le contexte national, et de dépasser une lecture strictement technico-organisationnelle de la digitalisation.

L'un des atouts majeurs de ce travail réside dans la diversité des profils professionnels inclus. La participation d'internes, de résidents, de médecins généralistes, de spécialistes ainsi que de professeurs de médecine et de chirurgie offre une vision transversale des usages

numériques à différents niveaux du système de santé. Cette pluralité permet d'identifier des perceptions différenciées selon l'expérience professionnelle, le niveau de responsabilité et le degré d'exposition aux systèmes d'information hospitaliers, renforçant ainsi la richesse descriptive et interprétative de l'analyse.

La taille de l'échantillon (380 répondants) constitue également un élément de robustesse pour une étude descriptive de ce type. Elle autorise l'identification de tendances claires et cohérentes concernant les usages, les pratiques et les représentations liées à la gestion numérique des données de santé. Par ailleurs, le recours à un questionnaire structuré et multidimensionnel a permis d'explorer de manière approfondie des dimensions souvent étudiées séparément dans la littérature, telles que les pratiques individuelles de cybersécurité, la connaissance du cadre réglementaire, la gouvernance des accès et les dilemmes éthiques rencontrés dans la pratique quotidienne.

Enfin, l'interprétation des résultats à la lumière de la littérature internationale et des cadres normatifs en vigueur, notamment la loi 09-08 et les recommandations institutionnelles, confère une solidité supplémentaire à l'analyse, en mettant en évidence à la fois des convergences avec les données internationales et des spécificités propres au contexte marocain.

2. Limites de l'étude

Certaines limites doivent néanmoins être prises en considération lors de l'interprétation des résultats. En premier lieu, le recours à un questionnaire auto-administré expose l'étude à des biais déclaratifs. Les données recueillies reposent sur les perceptions et les pratiques rapportées par les médecins eux-mêmes, sans observation directe ni audit objectif des systèmes d'information ou des comportements effectifs. Un biais de désirabilité sociale est donc possible, en particulier pour des thématiques sensibles telles que le respect du secret médical, l'éthique ou la cybersécurité, certains participants pouvant être enclins à sur-déclarer des pratiques conformes ou à minimiser des comportements à risque.

Par ailleurs, un biais de perception ne peut être exclu, dans la mesure où des notions telles que la « cybersécurité », la « traçabilité » ou l'existence de « procédures écrites » peuvent être interprétées différemment selon le niveau de formation, l'expérience professionnelle ou l'exposition antérieure à ces concepts. Toutefois, la cohérence interne des résultats, notamment la convergence entre perception élevée des risques, faible connaissance des procédures, pratiques à risque rapportées et confiance limitée dans la sécurité des systèmes, suggère que ces biais n'invalident pas la portée analytique des données, mais contribuent au contraire à refléter la réalité vécue par les professionnels.

Une autre limite concerne la représentativité géographique de l'échantillon, majoritairement centré sur Marrakech et ses régions avoisinantes. Cette concentration peut restreindre l'extrapolation des résultats à l'ensemble du territoire national, où les niveaux d'équipement numérique, les infrastructures et les pratiques organisationnelles peuvent être hétérogènes. Néanmoins, les grandes villes universitaires et hospitalières constituent des pôles stratégiques de la transformation numérique du système de santé, ce qui permet de capter des dynamiques précoces, tout en exposant à une possible surestimation du niveau de maturité numérique par rapport à des régions plus périphériques.

Le caractère transversal de l'étude constitue également une limite importante. Il ne permet ni d'analyser l'évolution des pratiques dans le temps, ni d'établir des relations causales entre la digitalisation, les comportements observés et leurs conséquences cliniques ou organisationnelles. De plus, l'absence de méthodes qualitatives complémentaires limite la compréhension approfondie de certains enjeux complexes, notamment les arbitrages éthiques, les logiques institutionnelles ou les résistances au changement.

Enfin, l'étude se concentre volontairement sur le point de vue des médecins utilisateurs finaux, sans intégrer les perspectives des administrateurs des systèmes d'information, des responsables informatiques, des RSSI ou des délégués à la protection des données. Cette absence empêche une évaluation objective du niveau réel de sécurité des infrastructures et de la conformité réglementaire, mais met en lumière une déconnexion persistante entre les

sphères clinique et informatique, contribuant aux incompréhensions et aux pratiques de contournement observées.

3. Implications et Perspectives :

Les résultats de ce travail soulignent la nécessité de développer une stratégie cohérente et progressive d'accompagnement de la digitalisation des données médicales. Ils mettent en évidence un besoin important de renforcement des compétences des médecins en matière de protection des données, d'éthique numérique et de cybersécurité, afin de favoriser des pratiques conformes aux exigences réglementaires et déontologiques.

Sur le plan institutionnel, ces constats plaident pour l'élaboration et la diffusion de procédures internes formalisées, de chartes d'utilisation des systèmes d'information et de dispositifs clairs de gestion des incidents, en lien avec les obligations prévues par la loi 09-08 et sous le contrôle de la CNDP. Le rôle des directions hospitalières apparaît central pour structurer cette gouvernance, assurer la formation continue et soutenir les professionnels dans un environnement numérique en constante évolution.

D'un point de vue scientifique, cette étude ouvre des perspectives de recherche prometteuses. Des travaux longitudinaux permettraient d'évaluer l'impact réel de la digitalisation sur la sécurité des soins, la charge de travail et la relation médecin-patient. De même, des approches qualitatives et des études mixtes intégrant les acteurs techniques et institutionnels offriraient un éclairage plus fin sur les freins, les leviers et les conditions d'une transformation numérique sécurisée et éthiquement responsable.

Enfin, à l'heure de l'essor de technologies émergentes telles que l'intelligence artificielle, l'Internet des objets médicaux et les dossiers médicaux partagés, ces résultats soulignent la nécessité d'une gouvernance nationale renforcée, capable de concilier innovation technologique, respect des principes éthiques et protection effective des données de santé.

C. Recommandations :

À la lumière des résultats de cette étude, des cadres juridiques et déontologiques marocains, ainsi que des orientations internationales en matière de e-santé, les recommandations suivantes s'inscrivent dans une logique intégrée et pragmatique. Elles visent à réduire le décalage observé entre les exigences légales et éthiques, d'une part, et les pratiques effectives des professionnels de santé, d'autre part, tout en préservant la continuité, la qualité et la sécurité des soins.

L'objectif central est de rendre la conformité juridique et éthique opérationnelle, compréhensible et soutenable dans la pratique clinique quotidienne.

1. Recommandations au niveau des établissements de santé

La transformation numérique des structures de soins nécessite en priorité un renforcement de la gouvernance des systèmes d'information hospitaliers (SIH). Il est recommandé d'améliorer la fiabilité des infrastructures numériques par des actions régulières de maintenance, de mise à jour, de sauvegarde et par la mise en place de plans de continuité d'activité. L'interopérabilité des systèmes doit être encouragée afin de limiter les ruptures d'information et les vulnérabilités techniques.

La formalisation et la diffusion de procédures internes claires relatives à l'accès, à l'utilisation et au partage des données médicales numériques constituent une priorité. Ces procédures doivent s'appuyer sur le principe du « besoin d'en connaître », définir précisément les droits d'accès selon les fonctions, limiter le recours aux identifiants partagés et prévoir des révisions périodiques des habilitations, notamment lors des changements de service ou de poste.

La traçabilité des accès et des actions sur les dossiers médicaux (consultation, modification, exportation) doit devenir une exigence opérationnelle, soutenue par des audits internes réguliers. Par ailleurs, l'implication des encadrants cliniques et des chefs de service dans la gouvernance numérique apparaît essentielle pour encadrer les usages, accompagner

les nouveaux professionnels et promouvoir des pratiques conformes, contribuant ainsi à une responsabilisation collective.

2. Recommandations pédagogiques et de formation

Les résultats de l'étude mettent en évidence un déficit important de formation des professionnels de santé en matière de protection des données et de cybersécurité. Il est recommandé d'instaurer une formation obligatoire, continue et adaptée aux réalités hospitalières, portant sur la gestion sécurisée des accès, les bonnes pratiques numériques, l'identification des tentatives de phishing, le stockage sécurisé des données et la conduite à tenir en cas d'incident.

Une sensibilisation structurée à la loi marocaine 09-08 doit être intégrée à la formation initiale et continue, afin de renforcer la compréhension des notions fondamentales (données sensibles, consentement, finalité, sécurité, responsabilité). De plus, l'intégration d'un module d'éthique du numérique en santé, en lien avec la déontologie médicale, permettrait d'aborder les dilemmes liés au secret médical en environnement informatisé, au partage de l'information et à l'usage secondaire des données.

Au-delà des enseignements formels, le développement d'une véritable culture institutionnelle de sécurité numérique constitue un enjeu majeur. Celle-ci repose sur la sensibilisation continue, les retours d'expérience après incidents et la valorisation des comportements responsables.

3. Recommandations réglementaires et institutionnelles

Au niveau national, un renforcement du rôle d'accompagnement, de sensibilisation et de contrôle de CNDP apparaît nécessaire afin d'aider les établissements de santé à traduire les exigences légales en pratiques opérationnelles.

Il est recommandé d'encourager l'instauration d'obligations de conformité explicites pour les établissements de santé, incluant l'existence de procédures écrites, la désignation de référents, la formation du personnel, la sécurisation des supports numériques et la documentation des traitements de données. La mise en place d'audits réguliers et de

dispositifs de suivi continu (revue des droits d'accès, contrôle des identifiants partagés, analyse des journaux de connexion) permettrait d'objectiver le niveau de maturité des SIH et d'anticiper les vulnérabilités.

Enfin, une adaptation progressive du cadre juridique national aux risques numériques émergents, notamment ceux liés à l'intelligence artificielle, à l'Internet des objets médicaux et à l'interconnexion croissante des systèmes, contribuerait à maintenir un équilibre entre innovation technologique et protection des droits fondamentaux.

4. Recommandations relatives aux pratiques cliniques

Les pratiques quotidiennes de partage d'informations médicales doivent être encadrées de manière explicite. Il est recommandé de privilégier les canaux institutionnels sécurisés et de limiter la circulation de données identifiantes au strict nécessaire, conformément au principe de minimisation.

L'usage de messageries non sécurisées doit faire l'objet de règles claires. En l'absence de solutions institutionnelles adaptées, ces outils ne devraient pas être utilisés pour transmettre des informations directement identifiantes, sauf situations exceptionnelles dûment justifiées, avec anonymisation maximale. À moyen terme, le déploiement de messageries professionnelles sécurisées, intégrées ou interopérables avec les SIH, apparaît indispensable afin de concilier efficacité clinique et respect des exigences de confidentialité.

5. Recommandations relatives à l'information et à l'implication du patient

La sensibilisation des patients à leurs droits en matière de données de santé constitue un levier essentiel pour une digitalisation éthique et durable du système de soins. Il est recommandé de développer des dispositifs d'information clairs, accessibles et adaptés aux différents niveaux de littératie, expliquant les modalités de collecte, de stockage, d'utilisation et de protection des données, ainsi que les droits reconnus par la loi marocaine 09-08.

Cette information peut s'appuyer sur des supports variés (documents d'information, affichage institutionnel, plateformes numériques, information orale au cours de la prise en charge), intégrés de manière pragmatique au parcours de soins. Elle ne doit pas être perçue

comme une contrainte administrative supplémentaire, mais comme un investissement dans la relation médecin-patient, favorisant la transparence, l'adhésion aux dispositifs numériques et la confiance.

En redonnant au patient une place active dans la gouvernance de ses données personnelles, le système de santé renforce sa crédibilité éthique et sociale, tout en contribuant à prévenir les situations de méfiance ou de rupture de la relation de soins dans un contexte de digitalisation croissante.

Au total, l'ensemble de ces recommandations converge vers une même exigence : faire de la protection des données personnelles et de la cybersécurité des composantes intrinsèques de la qualité et de la sécurité des soins. En articulant gouvernance institutionnelle, formation, pratiques cliniques sécurisées, implication du patient et audits réguliers, elles dessinent une trajectoire réaliste vers une e-santé marocaine éthiquement robuste, juridiquement conforme et organisationnellement soutenable.

Les principales recommandations issues de ce travail sont synthétisées dans le Tableau 7, puis intégrées dans un modèle conceptuel global présenté à la Figure 20, illustrant leur articulation au sein d'une gouvernance éthique et sécurisée des données de santé.

Tableau 10 : Recommandations opérationnelles pour une e-santé conforme et sécurisée

Axe	Recommandations clés	Finalité
Formation	Formation obligatoire et continue, en lien avec la CNDP, en protection des données, cybersécurité et éthique du numérique	Renforcer la culture éthique et réduire les pratiques à risque
Gouvernance des accès	Procédures internes normalisées définissant les droits d'accès, la traçabilité et les responsabilités selon le principe du moindre privilège	Assurer traçabilité, responsabilité et conformité légale
Outils numériques	Déploiement de messageries professionnelles sécurisées et encadrement de l'usage des supports personnels	Garantir confidentialité et continuité des soins
Information du patient	Dispositifs d'information clairs et accessibles sur les droits des patients et la gouvernance des données de santé	Renforcer la confiance et la transparence
Cybersécurité	Audits périodiques de cybersécurité et procédures formalisées de prévention et de gestion des incidents	Améliorer la résilience et la sécurité des établissements



Figure 19 :Modèle intégré de gouvernance éthique et sécurisée des données de santé



La digitalisation des données médicales s'impose aujourd'hui comme un levier essentiel de modernisation du système de santé, en améliorant la qualité, la continuité et la coordination des soins. À travers les systèmes d'information hospitaliers, les dossiers patients informatisés et les outils numériques de santé, elle offre des opportunités significatives d'optimisation des pratiques cliniques et organisationnelles. Toutefois, cette transformation concerne un domaine particulièrement sensible, où la protection des données conditionne le respect du secret médical, la confiance des patients et la légitimité des dispositifs numériques.

Cette thèse a permis d'analyser, dans le contexte marocain, les perceptions, les pratiques et les connaissances des médecins face à la digitalisation des données médicales, en mettant en lumière les enjeux éthiques et sécuritaires qui l'accompagnent. Les résultats révèlent une transition numérique encore inachevée, caractérisée par une coexistence de pratiques papier et numériques, ainsi qu'une hétérogénéité dans l'appropriation des outils et des règles de gouvernance des données.

Si les bénéfices attendus de la digitalisation sont largement reconnus par les professionnels de santé, notamment en matière de qualité et de continuité des soins, ils sont contrebalancés par des préoccupations importantes liées à la confidentialité, à la sécurité des systèmes et à la traçabilité des accès. Les pratiques observées traduisent moins une opposition au numérique qu'une adaptation pragmatique à des contraintes organisationnelles, dans un environnement où les procédures formalisées, la formation spécifique et la culture de sécurité restent insuffisamment développées.

Sur le plan éthique, le secret médical demeure un principe central, mais son application est rendue plus complexe par la multiplication des acteurs, des supports et des usages de l'information médicale. Le cadre juridique et déontologique existant offre une protection théorique solide, mais sa traduction opérationnelle demeure inégale, soulignant un décalage persistant entre les normes et les pratiques effectives.

En définitive, cette étude met en évidence que la réussite de la transformation numérique en santé ne dépend pas uniquement des technologies déployées, mais repose avant tout sur la gouvernance des données, la formation des professionnels et l'intégration des principes

éthiques et sécuritaires dans les pratiques quotidiennes. La digitalisation des données médicales ne pourra être durable et efficiente que si elle est pensée comme un projet global, conciliant innovation technologique, protection des droits fondamentaux et qualité des soins au bénéfice des patients et du système de santé marocain.



RESUME

Introduction :

La digitalisation des données médicales constitue aujourd'hui un axe majeur de modernisation des systèmes de santé, visant à améliorer la continuité, la qualité et la coordination des soins. Toutefois, cette transformation s'inscrit dans un champ particulièrement sensible, celui des données de santé, dont la protection soulève des enjeux éthiques, juridiques et sécuritaires majeurs. Dans le contexte marocain, la transition numérique progresse de manière hétérogène et interroge les pratiques réelles des professionnels de santé face aux exigences de confidentialité, de secret médical et de cybersécurité.

Objectif :

Évaluer les connaissances, perceptions et pratiques des professionnels de santé de Marrakech et de sa région vis-à-vis de la digitalisation des données médicales, en analysant ses implications éthiques et sécuritaires, afin d'identifier les bénéfices perçus, les limites observées et les leviers d'amélioration.

Méthodes :

Une étude quantitative transversale descriptive et analytique a été menée auprès de 380 médecins exerçant à Marrakech et dans sa région, à l'aide d'un questionnaire structuré auto-administré. Les variables étudiées portaient sur les caractéristiques sociodémographiques, le niveau de digitalisation des établissements, l'usage des systèmes d'information hospitaliers, la formation en protection des données et en cybersécurité, ainsi que les perceptions éthiques et sécuritaires liées à la digitalisation des données médicales.

Résultats :

L'échantillon était majoritairement jeune, avec 69,9 % des médecins âgés de moins de 40 ans, et exerçait principalement dans le secteur public (86,3 %). Une aisance informatique intermédiaire à élevée était déclarée par 82,1 % des répondants. Toutefois, la formation spécifique restait très limitée, avec seulement 4,7 % des médecins ayant bénéficié d'une formation en protection des données personnelles et 3,1 % en cybersécurité. L'adoption des systèmes d'information hospitaliers demeurait intermédiaire, marquée par des pratiques hybrides papier/numérique chez 54,6 % des répondants. La majorité des médecins reconnaissait l'impact positif de la digitalisation sur la continuité et la coordination des soins, tandis que 71,8 % estimaient qu'elle augmentait le risque de fuites massives de données. La confiance dans la sécurité informatique des établissements restait faible, exprimée par seulement 22,7 % des médecins.

Conclusion :

La digitalisation des données médicales est perçue par les professionnels de santé comme un levier pertinent d'amélioration de la qualité et de la continuité des soins. Toutefois, son déploiement demeure entravé par des insuffisances en matière de formation, de gouvernance des données et de cybersécurité. Les résultats soulignent la nécessité d'une approche globale intégrant le renforcement des compétences, la clarification des procédures et la consolidation des dispositifs de sécurité, afin d'assurer une digitalisation éthique, sécurisée et respectueuse des droits des patients.

ABSTRACT

Introduction:

The digitalization of medical data has become a major driver of healthcare system modernization, aiming to improve the continuity, quality, and coordination of care. However, this transformation takes place in a particularly sensitive domain—health data—whose protection raises significant ethical, legal, and cybersecurity challenges. In the Moroccan context, digital transition remains heterogeneous and raises questions about the real practices of healthcare professionals in relation to confidentiality, medical secrecy, and cybersecurity requirements.

Objective:

To assess the knowledge, perceptions, and practices of healthcare professionals in Marrakech and its surrounding region regarding the digitalization of medical data, by analyzing its ethical and security implications, in order to identify perceived benefits, observed limitations, and potential areas for improvement.

Methods:

A quantitative cross-sectional descriptive and analytical study was conducted among 380 physicians practicing in Marrakech and its region, using a structured self-administered questionnaire. The variables studied included sociodemographic characteristics, the level of digitalization of healthcare institutions, the use of hospital information systems, training in data protection and cybersecurity, as well as ethical and security-related perceptions associated with the digitalization of medical data.

Results:

The study population was predominantly young, with 69.9% of physicians under the age of 40, and mainly working in the public sector (86.3%). An intermediate to high level of computer proficiency was reported by 82.1% of respondents. However, specific training remained very limited, with only 4.7% having received training in personal data protection and 3.1% in cybersecurity.

The adoption of hospital information systems remained moderate, characterized by hybrid paper-digital practices in 54.6% of cases. Most physicians acknowledged the positive impact of digitalization on care continuity and coordination, while 71.8% believed that digitalization increases the risk of large-scale data breaches. Confidence in the security of institutional information systems remained low, expressed by only 22.7% of respondents.

Conclusion:

The digitalization of medical data is perceived by healthcare professionals as a relevant lever for improving the quality and continuity of care. However, its implementation remains hindered by shortcomings in training, data governance, and cybersecurity. These findings

highlight the need for a comprehensive approach combining capacity building, clarification of procedures, and strengthening of security mechanisms to ensure an ethical, secure digital transition that respects patients' rights.

الملخص

المقدمة:

أصبحت رقمنة المعطيات الطبية محورًا أساسيًا في تحديث الأنظمة الصحية، لما لها من دور في تحسين استمرارية الرعاية وجودتها وتنسيقها. غير أن هذه التحولات تدرج ضمن مجال بالغ الحساسية يتعلق بالمعطيات الصحية، التي تثير حمايتها تحديات أخلاقية وقانونية وأمنية مهمة. وفي السياق المغربي، لا تزال عملية التحول الرقمي غير متجانسة، وتطرح تساؤلات حول الممارسات الفعلية للمهنيين الصحيين في ما يتعلق بسرية المعطيات الطبية، والأمن السيبراني.

الهدف:

تقييم معارف وتصورات وممارسات المهنيين الصحيين بمدينة مراكش ونواحيها تجاه رقمنة المعطيات الطبية، من خلال تحليل انعكاساتها الأخلاقية والأمنية، وذلك بهدف تحديد الفوائد المدركة، والاختلالات المسجلة، وأفاق التحسين الممكنة.

المنهجية:

أنجزت دراسة كمية مقطعية وصفية وتحليلية شملت 380 طبيبًا يزاولون عملهم بمدينة مراكش ونواحيها، وذلك باستخدام استبيان ذاتي منظم. شملت المتغيرات المدروسة الخصائص السوسيو-ديموغرافية، ومستوى رقمنة المؤسسات الصحية، واستعمال نظم المعلومات الاستشفائية، والتكوين في مجال حماية المعطيات والأمن السيبراني، إضافة إلى التصورات الأخلاقية والأمنية المرتبطة برقمنة المعطيات الطبية.

النتائج:

من الأطباء أقل من 40 سنة، ويزاول معظمهم عملهم في القطاع العام 69.9% اتسمت العينة بكونها فتيّة، حيث كان من المشاركين بمستوى متوسط إلى مرتفع من الألفة مع الأدوات المعلوماتية، غير أن 82.1% صرّح. (86.3%) في 3.1% من تكوين في حماية المعطيات الشخصية و 4.7% التكوين المتخصص ظل محدودًا، إذ لم يستفد سوى الأمن السيبراني.

ظل اعتماد نظم المعلومات الاستشفائية في مستوى متوسط، مع هيمنة الممارسات المختلطة بين الورقي والرقمي من الأطباء. وأقرّ أغلب المشاركين بالآثار الإيجابية للرقمنة على استمرارية وتنسيق الرعاية، في حين 54.6% لدى فقط عن ثقتهم في 22.7% أن الرقمنة تزيد من خطر تسرب المعطيات على نطاق واسع، بينما عبّر 71.8% اعتبر أمن الأنظمة المعلوماتية بمؤسساتهم.

الخلاصة:

يُنظر إلى رقمنة المعطيات الطبية من طرف المهنيين الصحيين كرافعة مهمة لتحسين جودة واستمرارية الرعاية الصحية، غير أن تنزيلها العملي ما يزال يواجه تحديات مرتبطة بضعف التكوين، وقصور حوكمة المعطيات، ونقص آليات الأمن السيبراني. وتبرز هذه النتائج الحاجة إلى مقاربة شمولية تجمع بين تعزيز الكفاءات، وتوضيح المساطر، وتقوية أنظمة الحماية، بما يضمن رقمنة أخلاقية وأمنة تحترم حقوق المرضى.



ANNEXES



A – Informations sociodémographiques et professionnelles

A1. Sexe :

- ☐ Féminin
- ☐ Masculin

A2. Tranche d'âge :

- ☐ < 25 ans
- ☐ 25–34 ans
- ☐ 35–44 ans
- ☐ 45–54 ans
- ☐ ≥ 55 ans

A3. Profession principale :

- ☐ Médecin généraliste
- ☐ Médecin spécialiste
- ☐ Interne
- ☐ Résident
- ☐ Infirmier(ère) polyvalent(e)
- ☐ Infirmier(ère) spécialisé(e)
- ☐ Sage-femme
- ☐ Technicien(ne) de santé (lab, imagerie, etc.)
- ☐ Autre (préciser) :

A4. Type d'établissement où vous exercez principalement :

- ☐ CHU
- ☐ Hôpital provincial / régional
- ☐ Centre de santé urbain
- ☐ Centre de santé rural / dispensaire
- ☐ Clinique privée
- ☐ Cabinet médical libéral

• ☐ Autre :A5. Secteur d'exercice :

• ☐ Public

• ☐ Privé

A6. Service / unité principale :

• ☐ Médecine interne

• ☐ Chirurgie

• ☐ Urgences / SAMU

• ☐ Réanimation / soins intensifs

• ☐ Gynéco-obstétrique

• ☐ Pédiatrie

• ☐ Psychiatrie / addictologie

• ☐ Consultation externe / médecine de famille

• ☐ Imagerie médicale

• ☐ Laboratoire / biologie

• ☐ Autre :

A7. Ancienneté professionnelle :

• ☐ < 2 ans

• ☐ 2-5 ans

• ☐ 6-10 ans

• ☐ 11-20 ans

• ☐ > 20 ans

A8. Niveau d'aisance générale avec l'outil informatique (ordinateur, smartphone, applications) :

• ☐ 1 Très faible

• ☐ 2

• ☐ 3 Moyen

• ☐ 4

• ☐ 5 Très élevé

A9. Avez-vous déjà reçu une formation formelle en :

a) Éthique médicale / déontologie :

- ☐ Oui, durant le cursus universitaire
- ☐ Oui, en formation continue
- ☐ Non / ne se souvient pas

b) Protection des données personnelles (loi 09-08, CNDP, etc.) • ☐ Oui

- ☐ Non / ne se souvient pas

c) Cybersécurité appliquée aux établissements de santé :

- ☐ Oui, formation structurée (cours, atelier, e-learning)
- ☐ Oui, formation ponctuelle / sensibilisation
- ☐ Non

B – Organisation des systèmes d'information et outils numériques

B1. Dans votre établissement, les dossiers des patients sont :

- ☐ Exclusivement sur support papier
- ☐ Majoritairement sur papier avec quelques outils informatiques
- ☐ Majoritairement informatisés (système d'information hospitalier / logiciel métier)
- ☐ Entièrement informatisés

****B2. Utilisez-vous un dossier patient informatisé ou un système d'information hospitalier (SIH) pour vos patients ?**

- ☐ Oui, pour la majorité des patients
- ☐ Oui, mais seulement dans certains services
- ☐ Non
- ☐ Je ne sais pas

B3. À quelle fréquence consultez-vous un dossier médical informatisé (SIH, Dossier Patient Partagé, logiciel de clinique, etc.) ?

- ☐ Jamais
- ☐ Rarement (moins d'une fois par semaine)

- ☐ 1–3 fois par semaine
- ☐ Presque tous les jours de travail
- ☐ Pour quasiment tous les patients

B4. Outils numériques utilisés dans votre pratique (plusieurs réponses possibles) :

- ☐ Dossier papier classique
- ☐ Système d'information hospitalier (SIH) public
- ☐ Logiciel de clinique / cabinet privé
- ☐ PACS / système d'archivage d'images
- ☐ Plateforme de téléconsultation ou télémédecine
- ☐ Messagerie professionnelle de l'établissement • ☐ Messagerie personnelle (Gmail, Yahoo, etc.)
- ☐ Applications de messagerie instantanée (WhatsApp, Telegram, etc.) pour transmettre des informations médicales
- ☐ Autre :

B5. Supports utilisés pour accéder aux données médicales numériques (plusieurs réponses possibles) :

- ☐ Ordinateur de l'établissement
- ☐ Ordinateur portable personnel
- ☐ Smartphone personnel
- ☐ Autre :

B6. Disposez-vous d'un identifiant et d'un mot de passe personnels pour accéder au système d'information / dossier médical informatisé ?

- ☐ Oui
- ☐ Non, identifiants partagés au sein de l'équipe
- ☐ Non, j'utilise ceux d'un(e) collègue / secrétaire
- ☐ Non applicable (pas de système informatisé)

B7. Dans votre établissement, existe-t-il un règlement ou une procédure écrite concernant l'utilisation des données médicales numériques (confidentialité, accès,

sanctions) ?

- ☐ Oui, je la/le connais
- ☐ Oui, mais je ne l'ai pas lu(e)
- ☐ Non
- ☐ Je ne sais pas

B8. Selon vous, l'informatisation du dossier patient a amélioré la qualité et la continuité des soins dans votre contexte (service / région) ?

- ☐ 1 Tout à fait en désaccord
- ☐ 2
- ☐ 3 Ni d'accord ni en désaccord
- ☐ 4
- ☐ 5 Tout à fait d'accord

B9. Selon vous, l'informatisation a augmenté la charge administrative pour les soignants ?

(même échelle 1-5)

C – Perceptions globales de la digitalisation (échelle 1-5) 1 = Tout à fait en désaccord ... 5 = Tout à fait d'accord.

- C1. Les dossiers médicaux électroniques utilisés au Maroc améliorent la sécurité clinique (traçabilité, réduction des erreurs).
- C2. Ils facilitent la coordination des soins entre les différents niveaux du système de santé (centre de santé, hôpital provincial, CHU, secteur privé).
- C3. La numérisation rend plus facile l'accès à des informations sensibles par des personnes qui ne devraient pas les consulter.
- C4. Dans le contexte marocain, les bénéfices de la digitalisation pour les patients sont globalement supérieurs aux risques pour la confidentialité.
- C5. Les systèmes actuels permettent de tracer qui a consulté quel dossier et à quel moment.

- C6. La digitalisation augmente le risque de fuite massive de données en cas de cyberattaque (ransomware, piratage, etc.).
- C7. L'accès informatisé peut favoriser la consultation de dossiers sans justification clinique (curiosité, patients connus, personnalités...).
- C8. Les patients au Maroc sont insuffisamment informés sur la manière dont leurs données de santé sont stockées et protégées.
- C9. Les patients devraient avoir la possibilité de limiter l'accès à certaines informations sensibles (psychiatrie, VIH, IVG, etc.).
- C10. Je fais globalement confiance au niveau de sécurité informatique de mon établissement.

D – Axe éthique : confidentialité, secret médical,

consentement (1-5)

- D1. Le respect du secret médical reste prioritaire, même face aux demandes administratives (assureurs, CNSS, autorités, etc.).
- D2. Je ressens parfois un conflit entre la nécessité de partager l'information pour la continuité des soins et le respect strict de la confidentialité du patient.
- D3. Dans mon établissement, il est clairement défini qui a le droit d'accéder à quelles parties du dossier médical.
- D4. Il m'arrive de discuter de cas cliniques (diagnostic, détails) dans des lieux ou devant des personnes non autorisées (couloirs, salle d'attente, ascenseur, café de l'hôpital...).
- D5. Il est acceptable, dans certaines situations urgentes, d'envoyer des informations médicales identifiantes via WhatsApp ou autre messagerie non sécurisée.
- D6. Les patients sont informés que leurs données sont conservées dans des systèmes numériques
- D7. L'utilisation des données des patients pour la recherche ou les registres

- épidémiologiques est clairement expliquée aux patients et leur consentement est
- recherché lorsqu'il est nécessaire.
- D8. Les données utilisées pour la recherche devraient être au minimum pseudonymisées
- et idéalement anonymisées lorsqu'elles sont transmises à des tiers (universités, laboratoires, etc.).
- D9. L'utilisation de données de santé à des fins commerciales (industries, assurances, plateformes privées) est problématique, même si les données sont pseudonymisées.
- D10. Je me sens suffisamment formé(e) sur le plan éthique pour prendre des décisions
- concernant l'utilisation des données de mes patients (soins, recherche, registres, enseignement).

E – Axe cybersécurité : pratiques individuelles (1 = jamais,

5 = toujours)

- E1. Je verrouille ma session ou mon poste de travail dès que je m'absente, même brièvement.
- E2. Je modifie régulièrement mes mots de passe (au moins tous les 3-6 mois).
- E3. J'utilise des mots de passe forts et différents selon les systèmes
- E4. Il m'est arrivé de communiquer mon mot de passe ou mes identifiants à un(e) collègue pour des raisons pratiques.
- E5. J'utilise parfois le même mot de passe pour mon travail, ma messagerie personnelle
- et d'autres comptes (réseaux sociaux, etc.).
- E6. Il m'arrive de transférer des comptes rendus, résultats ou images médicales vers ma
- messagerie personnelle ou vers mon téléphone pour les imprimer ou les consulter plus
- facilement.

- E7. Je suis attentif(ve) aux emails suspects (phishing), liens ou pièces jointes douteuses et
- je les signale le cas échéant.
- E8. Je stocke parfois des documents contenant des données de patients sur des supports
- non sécurisés (clé USB personnelle, ordinateur à domicile)
- E9. En cas d'incident (perte d'un support, mail envoyé au mauvais destinataire, suspicion de piratage...), je sais à qui le signaler dans mon établissement.
- E10. Pour moi, la cybersécurité est avant tout de la responsabilité des services informatiques, plus que celle des professionnels de santé.

F – Perception des risques et culture de sécurité (1–5)

- F1. Je pense que les hôpitaux et cliniques marocains sont des cibles potentielles pour des
- attaques informatiques ou du vol de données.
- F2. Une violation de données médicales pourrait avoir un impact grave sur la confiance
- des citoyens dans le système de santé marocain.
- F3. Une cyberattaque paralysant le système d'information pourrait compromettre la
- continuité des soins.
- F4. La direction de mon établissement prend au sérieux la cybersécurité et la protection
- des données de santé.

G – Connaissances du cadre légal et institutionnel au

Maroc

- G1. Avant ce questionnaire, connaissiez-vous l'existence de la loi marocaine n° 09–08
- relative à la protection des personnes physiques à l'égard du traitement des données à

- caractère personnel ?
- ☐ Oui, je la connais bien
- ☐ Oui, j'en ai entendu parler sans détails
- ☐ Non

G2. La loi 09-08 s'applique selon vous :

- Uniquement aux données administratives (nom, adresse, etc.)
- ☐ Uniquement aux données de santé
- ☐ À tout traitement de données à caractère personnel, y compris les données de santé
- ☐ Je ne sais pas

G3. Savez-vous ce qu'est la CNDP (Commission Nationale de contrôle de la protection des Données à caractère Personnel) ?

- Oui, je connais son rôle
 - Oui, de nom seulement
 - Non
- G4. Dans votre pratique (cabinet, clinique, laboratoire, pharmacie, etc.), savez-vous s'il

y a eu une démarche de conformité à la loi 09-08 (déclarations, autorisations, guide de conformité...) ?

- ☐ ☐ Oui
- ☐ ☐ Non
- ☐ ☐ Je ne sais pas
- ☐ ☐ Non applicable

G5. Je connais les procédures à suivre en cas de fuite de données, perte de dossiers, ou accès non autorisé (à qui déclarer, quels formulaires, etc.).

- ☐ ☐ 1 Tout à fait en désaccord
- ☐ ☐ 2
- ☐ ☐ 3
- ☐ ☐ 4

- ☐ 5 Tout à fait d'accord

Section H – Situations pratiques (cocher la réponse qui correspond le plus à votre pratique réelle)

H1. Transmission d'images via WhatsApp

Aux urgences, vous souhaitez demander l'avis d'un spécialiste non présent sur place et pensez

à lui envoyer une photo d'une lésion. Que faites-vous le plus probablement ?

- J'envoie la photo avec le visage ou des éléments identifiants du patient.
- J'envoie la photo après avoir supprimé tout élément identifiant (visage, nom, numéro...).
- J'utilise uniquement une messagerie ou une solution sécurisée fournie par l'établissement.
- Je préfère téléphoner sans envoyer d'image.

H2. Accès au dossier d'un proche hospitalisé dans mon établissement

- Je consulte son dossier pour me rassurer ou informer la famille, sans autorisation particulière.
- Je consulte le dossier seulement si le patient me donne clairement son accord.
- Je ne consulte pas son dossier, même si j'y ai accès, pour respecter le secret médical.
- Autre :

H3. Demande d'un responsable administratif

Un responsable vous demande une liste de patients avec leurs diagnostics pour un rapport urgent, en vous proposant d'utiliser votre adresse email personnelle si la messagerie institutionnelle ne fonctionne pas. • ☐ J'envoie les données complètes via ma messagerie personnelle.

- J'envoie uniquement des données anonymisées.
- Je refuse et propose une solution plus sécurisée (clé chiffrée, messagerie professionnelle...).

- Je demande un écrit (ordre de mission, courrier officiel) avant tout envoi.

H4. Utilisation secondaire des données pour la recherche

Vous participez à une étude rétrospective sur des dossiers de patients suivis dans votre service.

- L'autorisation du comité d'éthique suffit, il n'est pas nécessaire d'informer les patients.
- Quand c'est possible, il est souhaitable d'informer les patients et d'obtenir leur accord.
- Les données doivent être systématiquement anonymisées avant analyse ou transmission.
- Je ne vois pas d'enjeu particulier, puisque la recherche vise l'intérêt des patients.



1. **Rothstein MA.**
Ethical issues in big data health research: Currents in contemporary bioethics. *J Law Med Ethics*. 2015;43(2):425–429.
2. **Häyrinen K, Saranto K, Nykänen P.**
Definition, structure, content, use and impacts of electronic health records: a review of the research literature. *Int J Med Inform*. 2008;77(5):291–304.
3. **Islam SMR, et al.**
The Internet of Things for Health Care: a comprehensive survey. *IEEE Access*. 2015;3:678–708.
4. **Kruse CS, et al.**
Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1–10.
5. Royaume du Maroc. Loi n°09–08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. *Bulletin Officiel* n°5714; 2009.
6. **El Ouazzani A, et al.**
Knowledge and attitudes of health professionals regarding personal data protection in Morocco. *Pan Afr Med J*. 2019
7. **Beauchamp TL, Childress JF.**
Principles of biomedical ethics. 7th ed. Oxford: Oxford University Press; 2013.
8. **Vayena E, Blasimme A, Cohen IG.**
Machine learning in medicine: addressing ethical challenges. *PLoS Med*. 2018;15(11):e1002689.
9. Ministère de la Santé et de la Protection Sociale (Maroc). Stratégie de transformation digitale du système de santé. Rabat.2020–2025
10. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD). *Journal officiel de l'Union européenne*; 2016.
11. Health Insurance Portability and Accountability Act (HIPAA) of 1996. U.S. Department of Health and Human Services; 1996.
12. European Union Agency for Cybersecurity (ENISA). Data protection and cybersecurity in healthcare.
13. **Gagnon MP, Desmartis M, Labrecque M, et al.**
Factors influencing ICT adoption. *J Med Syst*. 2012;36(1):241–277.
14. **Venkatesh V, Morris MG, Davis GB, Davis FD.**
User acceptance of information technology: toward a unified view. *MIS Q*. 2003;27(3):425–478.
15. **Yusof MM, Kuljis J, Papazafeiropoulou A, Stergioulas LK.**
An evaluation framework for health information systems: human, organization and technology–fit factors (HOT–fit). *Int J Med Inform*. 2008;77(6):386–398.

16. **Holden RJ, Karsh BT.**
The Technology Acceptance Model: its past and its future in health care. *J Biomed Inform.* 2010;43(1):159–172.
17. **Norman CD, Skinner HA.**
eHealth literacy: essential skills for consumer health in a networked world. *J Med Internet Res.* 2006;8(2):e9.
18. **McGonigle D, Mastrian KG.**
Nursing informatics and the foundation of knowledge. 4th ed. Burlington (MA): Jones & Bartlett Learning; 2018.
19. **Tikanmäki M, et al.**
Health professionals' digital competence and perceived skills. *Stud Health Technol Inform.*
20. **Greenhalgh T, et al.**
Beyond adoption: a new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up of health and care technologies. *J Med Internet Res.*
21. **Kwateng KO, et al.**
Health professionals' acceptance of hospital information systems.
22. **Cresswell KM, et al.**
Understanding the effects of digitalisation on clinical work.
23. **Giertz H, et al.**
Digital health literacy of healthcare professionals: a systematic review.
24. **Boonstra A, Broekhuis M.**
Barriers to the acceptance of electronic medical records.
25. **Roman LC, et al.**
Organizational determinants of health information security.
26. **Alanazi HO, et al.**
Information security governance in healthcare organizations.
27. **Mouaouia A.**
Acceptabilité des systèmes d'information hospitaliers au CHU Ibn Rochd.
28. **Organisation mondiale de la Santé (OMS).** Global strategy on digital health / Cybersecurity in health.
29. **Office of the National Coordinator for Health IT (ONC).** Adoption of electronic health records in the United States. U.S. Department of Health and Human Services
30. **European Commission.** eHealth and electronic health records in Europe. [lieu]: European Commission
31. **Black AD, et al.**
The impact of eHealth on the quality and safety of healthcare.
32. **Jones SS, et al.**
Health information technology and care coordination.

33. **Kruse CS, et al.**
Health information technology and care coordination: a systematic review.
34. **Menachemi N, Collum TH.**
Benefits and drawbacks of electronic health records.
35. **Buntin MB, et al.**
Health information technology: laying the infrastructure.
36. **Adler–Milstein J, et al.**
The impact of health IT on information sharing and traceability. [référence à compléter].
[année à compléter];[volume(n°)]:[pages].
37. World Health Organization. Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021.
38. Office of the National Coordinator for Health Information Technology. Office–based physician electronic health record adoption. U.S. Department of Health and Human Services
39. European Commission. eHealth Digital Service Infrastructure (eHDSI) and electronic health records in Europe. European Commission
40. **Black AD, Car J, Pagliari C, et al.**
The impact of eHealth on the quality and safety of healthcare: a systematic overview. PLoS Med. 2011;8(1):e1000387.
41. **Buntin MB, Burke MF, Hoaglin MC, Blumenthal D.**
The benefits of health information technology: a review of the recent literature. Health Aff (Millwood). 2011;30(3):464–471.
42. **Kruse CS, Stein A, Thomas H, Kaur H.**
The use of electronic health records to support population health: a systematic review. J Med Syst. 2018;42:214.
43. **Jones SS, Rudin RS, Perry T, Shekelle PG.**
Health information technology: an updated systematic review with a focus on meaningful use. Ann Intern Med. 2014;160(1):48–54.
44. **Shekelle PG, Morton SC, Keeler EB.**
Costs and benefits of health information technology. Evidence Report/Technology Assessment No. 132. Rockville (MD): Agency for Healthcare Research and Quality (AHRQ); 2006.
45. **Menachemi N, Collum TH.**
Benefits and drawbacks of electronic health record systems. Risk Manag Healthc Policy. 2011;4:47–55.
46. **Boonstra A, Broekhuis M.**
Barriers to the acceptance of electronic medical records by physicians. BMC Health Serv Res. 2010;10:231.
47. **Adler–Milstein J, Pfeifer E.**
Information blocking: is it occurring and what policy strategies can address it? Milbank Q. 2017;95(1):117–135.

48. World Health Organization, Regional Office for the Eastern Mediterranean. Digital health in the Eastern Mediterranean Region: situation analysis and way forward. Cairo: WHO EMRO; 2022.
49. **Alorbany M, Hassanain M, Al-Saggaf UM, et al.**
Challenges and barriers to the implementation of electronic health records in developing countries: the case of Egypt. *Int J Med Inform.* 2017;103:1–10.
50. **Ben Romdhane H, Ben Ayed H, Ben Henda N, et al.**
Hospital information systems in Tunisia: limits of modular digitalization and perspectives for integration. *Int J Med Inform.* 2014;83(12):877–885.
51. World Health Organization, Regional Office for Europe. From innovation to implementation: eHealth in the WHO European Region. Copenhagen: WHO Regional Office for Europe; 2016.
52. World Health Organization. Recommendations on digital interventions for health system strengthening. Geneva: World Health Organization; 2019.
53. **Cresswell KM, Sheikh A.**
Organizational issues in the implementation and adoption of health information technology innovations: an interpretative review. *Int J Med Inform.* 2013;82(5):e73–e86.
54. **Kruse CS, Frederick B, Jacobson T, Monticone DK.**
Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care.* 2017;25(1):1–10.
55. **Jalali MS, Kaiser JP, Maheshwari S.**
Cybersecurity in hospitals: a systematic review of attacks and vulnerabilities. *J Med Internet Res.* 2019;21(7):e14410.
56. **Appari A, Johnson ME.**
Information security and privacy in healthcare: current state of research. *Int J Internet Enterp Manag.* 2010;6(4):279–314.
57. **Rindfleisch TC.**
Privacy, information technology, and health care. *Commun ACM.* 1997;40(8):92–100.
58. World Health Organization. Cybersecurity in the health sector: guidelines for healthcare institutions. Geneva: World Health Organization; 2022.
59. World Health Organization; Organisation for Economic Co-operation and Development (OECD). Building trust in health systems: governance and cybersecurity of health data. Paris/Geneva: OECD-WHO; 2020.
60. Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). Guide de conformité à la loi n°09-08 et bonnes pratiques en matière de protection des données personnelles. Rabat: CNDP; [année à compléter].
61. **Cresswell KM, Bates DW, Sheikh A.**
Ten key considerations for the successful implementation and adoption of large-scale health information technology. *J Am Med Inform Assoc.* 2013;20(e1):e9–e13.
62. **Shabani M, Bezuidenhout L, Borry P.**
Attitudes of research participants and the general public towards genomic data sharing. *PLoS One.* 2014;9(10):e110908.

63. European Commission. Ethics guidelines for trustworthy artificial intelligence. Brussels: European Commission; 2019.
64. **Vayena E, Blasimme A.**
Health research with big data: time for systemic oversight. J Law Med Ethics. 2018;46(1):119–129.
65. **Bryant T.**
Password sharing in healthcare organizations. J AHIMA. 2016;87(5):34–39.
66. **Netschert J, Behrendt S, Schütte J.**
Information security awareness in healthcare. Int J Med Inform. 2017;103:1–10.
67. World Health Organization. Cybersecurity in the health sector: guidelines for healthcare institutions. Geneva: World Health Organization; 2022.
68. World Health Organization. Ethics and governance of artificial intelligence for health. Geneva: World Health Organization; 2021.
69. European Union Agency for Cybersecurity (ENISA). Cybersecurity challenges in the healthcare sector. Heraklion: ENISA; 2021.
70. ENISA; European Cyber Security Organisation (ECSO). Cybersecurity in healthcare: sectoral analysis. Brussels: ENISA/ECSO; 2020.
71. ENISA. Health Threat Landscape / analyses cyber santé (ransomware, phishing, etc.). [à compléter : titre exact, année, lieu, éditeur].
72. **He Y, et al.**
Healthcare cybersecurity challenges and solutions: a systematic review. [à compléter : revue exacte, année, volume, pages/e-location]. (*Tu as noté "JMIR/2021" → à préciser*).
73. **ENISA.**
Ressources/capacités CSIRT (cadres et recommandations). [à compléter : titre exact, année, lieu, éditeur].
74. **Neprash HT, et al.**
Impacts des cyberattaques sur les hôpitaux.
75. PIH Health Californie 2024
76. Heywood & Athol Hospital (Massachusetts) 2025
77. Corbeil-Essonnes
78. National Institute of Standards and Technology. Security and privacy controls for information systems and organizations (NIST SP 800–53 Rev. 5). Gaithersburg (MD): NIST
79. Ministère de la Santé et de la Protection Sociale (Maroc). Actualité / annonce autour DMP/FSE. Rabat: Ministère
80. European Commission. Digital Decade eHealth indicator study (accès EHR, eID, maturité). Brussels: European Commission
81. **Fennelly O, et al.**
Cresswell KM, et al
82. Région MENA : contraintes ressources/formation/gouvernance. [à compléter : rapport OMS/EMRO ou étude, titre/année].

83. World Health Organization; Organisation for Economic Co-operation and Development (OECD). Building trust in health systems: governance and cybersecurity of health data. Paris/Geneva: OECD-WHO; 2023.

قسم الطبيب

أقسم بالله العظيم

أن أراقب الله في مهنتي

وأن أصون حياة الانسان في كافة أطوارها في كل الظروف والأحوال

باذلة وسعي في إنقاذها من الهلاك والمرض والألم والقلق

وأن أحفظ للناس كرامتهم واستر عورتهم وأكتم سرهم

وأن أكون على الدوام من وسائل رحمة الله

باذلة رعايتي الطبية للقريب والبعيد والصالح والطالح والصديق والعدو

وأن أثابر على طلب العلم وأسخره لنفع الانسان لا لأذاه

وأن أوقر من علمني وأعلم من يصغرنى

وأكون أختا لكل زميل في المهنة الطبية متعاونين على البر والتقوى

وأن تكون حياتي مصداق إيماني في سري وعلاانيتي

نقية مما يشينها تجاه الله ورسوله والمؤمنين

والله على ما أقول شهيد

أطروحة رقم 87

سنة 2026

رقمنة المعطيات الطبية: بين الأخلاقيات والأمن

الأطروحة

قدمت ونوقشت علانية يوم 2026/02/06
من طرف

السيدة لمياء بوصيري

المزودة في 2000/02/16 ببني ملال
لنيل شهادة الدكتوراه في الطب

الكلمات الأساسية:

الرقمنة – المعطيات الطبية – الأخلاقيات – الأمن السيبراني – القانون 08-09

اللجنة

الرئيس

المشرف

الحكام



م. الزياتي

أستاذ في الطب الباطني

ع. الرايسي

أستاذ في أمراض الدم السريرية

ي. قاموس

أستاذ في التخدير و الإنعاش

إ. السعدي

أستاذ في علم الأورام الطبية

السيد

السيد

السيد

السيد

