

MDTPlatform

Instructions for Use

English

Version 4

Draft · 26 September 2026



Nordic AI Medical ApS
Slotsmarken 12, 1. th., 2970 Hørsholm, Denmark
support@nordicaimedical.com



MDT Oplæg
Oplæg

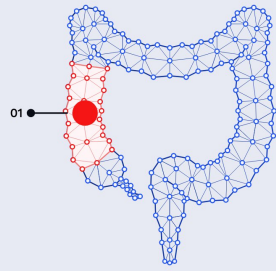
Kortsigtet risiko
Høj 72

Patientdetaljer

ASA 3	Performance 0	BMI 20 kg/m ²
Hb 8 mmol/L	CEA 12 µg/L	eGFR 90 mL/min/1.73m ²
cTNM cT2N1M0		
Karcinotype AC	MMR-status pMMR	

Komorbiditeter

- Diabetes
- Tidligere tromboemboli



Topografisk snapshot

- 01 Primær cancer
Colon ascendens

Billeder
Der er ingen billeder at vise.

< Forrige patient

Næste patient >

Instructions for use for MDTPlatform

Contents

1	Introduction	4
2	Product Description	5
2.1	Intended Purpose	5
2.2	Intended Patient Population	5
2.3	Medical Indications	5
2.4	Contraindications	6
2.5	Intended User	6
2.6	Intended Use	6
2.7	Precautions/Warnings	8
2.8	Clinical claims	9
2.8.1	Non-clinical Claims	9
3	Safety Instructions	10
3.1	General safety remarks	10
3.2	Operation of the Device	10
3.3	Side Effects and Contraindications	10
4	Installation and Uninstallation	11
5	Operation	11
5.1	Logging in and out	11
5.1.1	Logging in	11
5.1.2	Logging in with an organisation account	12
5.1.3	Logging in with a local account	12
5.1.4	Access awaiting approval	13
5.1.5	Logging out	13
5.2	Creating new series of meetings	14
5.3	Editing series of meetings	15
5.4	Deleting series of meetings	16
5.5	Adding patients to a meeting	16
5.6	Editing information about patients	18
5.7	Removing patients from a meeting	19
5.8	Sorting patients in a meeting	20
5.9	Approving meetings	20
5.10	Editing meeting information for a specific meeting	21
5.11	Toggling dark and light mode	21
5.12	Toggling presentation mode	22
5.13	Contacting support	22
5.13.1	Support contact in the page footer	22
5.13.2	Help on the product information page	23

5.14	Reporting errors, bugs or areas of improvement	23
5.15	Administering users and access	23
5.15.1	Administration overview	23
5.15.2	Approving access requests	24
5.15.3	Creating local users	24
5.15.4	Managing users	25
5.15.5	Configuring the identity provider	25
5.15.6	Reviewing the access log	26
6	Troubleshooting	27
7	Technical Data	29
7.1	Software classification	29
7.2	Requirements for hosting	29
7.3	System minimum requirements	29
7.4	Supported web browsers	29
8	Legal notices	29
9	Symbols and definitions in MDTPlatform	30
10	Declaration of Conformity	30

1 Introduction

We prepared these instructions with great care. If you find details here that do not match how the system works, please tell us so that we can correct them as quickly as possible.

Report any serious incident that has occurred in relation to the device to Nordic AI Medical ApS and to the competent authority of the Member State in which you or the patient are established. Undesirable side effects not described in these instructions for use should also be reported to Nordic AI Medical ApS. Please use the contact details below for this purpose.

The specifications and figures in this user manual are subject to change due to visual or technical improvements.

All trademarks named and shown are trademarks of the respective proprietor and are recognized as being protected.

Reprinting, translation and duplication, even of excerpts, require the written permission of the manufacturer.

Information about the product and the manufacturer

Name: MDTPlatform

Version: v1.0.0

UDI-DI: 05745001289003

Release date: 10 September 2026

A product of

Name: Nordic AI Medical ApS

Address: Slotsmarken 12, 1. th.

2970 Hørsholm, Denmark

Email: support@nordicaimedical.com

Website: www.nordicaimedical.com

Version of these instructions for use

Version 4

Date: 26 September 2026 (draft)

2 Product Description

2.1 Intended Purpose

MDTPlatform is a software application consisting of a user interface (MDTPlus) for presenting patient information and an embedded model (STR-CRC) for prediction of a patient's short-term risk after elective resection for colorectal cancer with curative intent in adult patients. Short-term risk is defined as a composite outcome of 1-year postoperative mortality, any Clavien-Dindo 4a or 4b complication within 30 days postoperatively, or any readmission of length 4 to 30 days starting within the first 14 days after discharge. The device is used at multidisciplinary team meetings and in adjacent clinical situations (preoperative planning and postoperative follow-up), once curatively intended surgery has been decided upon; it supports and does not replace clinical decision-making.

In the user interface the output of the embedded model, referred to as STR-CRC in this document, is presented under the heading "Kortsigtet risiko" on the patient page and in the column "Risiko" of the patient list.

The model outputs a risk rank from 0 to 100. Risk strata and their labels are configured by the deploying site per meeting series and are a presentation of the rank, not a model output. In the user interface the rank is presented as this stratification, for example A, B, C and D in increasing order of risk.

MDTPlatform is not intended to be used to decide if surgery should be performed, nor does it directly specify perioperative treatments.

2.2 Intended Patient Population

MDTPlatform is intended to be used in newly referred adult patients (≥ 18 years) with a coded diagnosis of primary CRC for whom curatively intended surgery has been decided upon (see 2.3 for indications).

2.3 Medical Indications

Use of MDTPlatform is indicated in situations where all of the below conditions apply:

- Patient aged 18 or above
- Patient newly referred for a diagnosis of primary CRC based on one of the below given diagnosis code systems (* denotes diagnosis codes with any character or number afterwards).
 - ICD-10: diagnosis codes C18* (Malignant neoplasm of colon), C19* (Malignant neoplasm of rectosigmoid junction), C20* (Malignant neoplasm of rectum) or C21* (Malignant neoplasm of anus and anal canal)
 - ICD-11: diagnosis codes 2B9* (malignant neoplasm of large intestine (specifically; colon, rectosigmoid junction, rectum, unspecified site, or other specified site) or, 2C00.* (malignant neoplasm of anus or anal canal).
 - SKS (Danish system): DC18* (Malignant neoplasm of the large intestine [translated from "Kræft i tyktarmen" (Danish)]), DC19* (Malignant neoplasm of the rectosigmoid junction [translated from "Kræft i overgangen mellem tyktarm og endetarm" (Danish)]), DC20* (Malignant neoplasm of the rectum [translated from "Kræft i

endetarmen" (Danish)) or DC21* (Malignant neoplasm of the anus or anal canal [translated from "Kræft i endetarmssåbningen eller analkanalen" (Danish)]).

- In cases where elective surgery for one of the above given diagnoses with curative intent has been decided upon.

2.4 Contraindications

There are no contraindications.

2.5 Intended User

MDTPlatform is intended only to be used by certified healthcare personnel involved in the perioperative care of patients with CRC.

2.6 Intended Use

Intended place of operation

MDTPlatform is intended to be used at hospital departments involved in perioperative care of the intended patient population (see 2.2 and 2.3).

Intended use environment

MDTPlatform is intended to be used on a computer, tablet or other digital device that can access the applications.

Minimum requirements

To operate MDTPlatform as intended, the deployment must meet the following minimum requirements for hardware, IT-network characteristics and IT-security measures, including protection against unauthorised access:

- Hardware and browser: a computer or tablet able to run Microsoft Edge version 137 or newer, or Google Chrome version 137 or newer, with a display and a keyboard or touch input. MDTPlatform runs in the browser: no software is installed on the device you use it from, and no patient data is stored on that device.
- IT-network characteristics: MDTPlatform protects the connection between the device you use it from and the hospital's MDTPlatform deployment. The deployment answers only over an encrypted connection (HTTPS), using a certificate the hospital issues for it. An unencrypted request is redirected to the encrypted address. Without its certificate the deployment does not start. The application obtains the risk score from the STR-CRC inference unit in the same hospital-controlled deployment. Internal service connections are isolated by network policy. The application sends operational health and lifecycle information outwards to Nordic AI Medical over authenticated HTTPS. Nordic AI Medical opens no connection into the hospital network.
- IT-security measures, including protection against unauthorised access:
 - **User registration.** A hospital administrator registers every person in MDTPlatform before that person can sign in. The administrator assigns each person's roles in MDTPlatform. The administrator either creates a local account with a username and password or approves the access request of a verified identity from the hospital identity provider. Each of the two creates a new account with that sign-in identity. MDTPlatform provides no operation to add a sign-in identity to an existing account. One account may hold several such identities.
 - **Account lifecycle.** Administrators can disable and re-enable accounts. MDTPlatform provides no account-deletion operation. A role change takes effect on the person's

next request. Removing a sign-in identity from an account ends that person's existing sessions; the account keeps its other identities.

- **Local credentials.** Installation, local-account registration and password reset each generate a five-word temporary password ("Midlertidig adgangskode" in the user interface) that is displayed once. The hospital must give it only to the named person through an approved confidential channel. The person must choose a new password before MDTPlatform creates a normal session. Five consecutive failed attempts lock the account for 15 minutes. The lock then clears automatically, or an administrator can clear it sooner.
- **Identity-provider accounts.** MDTPlatform supports one hospital identity provider per installation. The hospital administrator must configure the issuer, client identifier, confidential client secret and any private-PKI root CA certificate. The certificate contains public key material; the administrator must not upload a CA private key. The administration screen displays the exact callback address as a read-only value derived from the installed public address. The administrator must register that displayed address unchanged at the identity provider, test the connection and register each identity-provider user in MDTPlatform before use.
- **Identity binding.** Each account carries one or more identity bindings, each a unique pairing of an identity provider and the subject that provider asserts. An account carries no email address or other contact data. A pending access request holds the claims the identity provider asserted, an email address among them where the provider asserts one, until the request is approved or rejected, or expires after 30 days. When a person signs in through the identity provider with an identity the device does not yet recognise, MDTPlatform holds the request as a pending access request for an administrator to approve. Approval creates a new account and adds the binding. An administrator can remove one binding at a time and confirms each removal in a dialog that states its consequence. MDTPlatform provides no operation to clear all of an account's bindings at once, and it refuses to remove the last binding of the last enabled administrator. Each removal ends the affected sessions and is recorded in the audit log.
- **Credential custody.** The hospital must protect the confidentiality of generated temporary passwords, user-chosen passwords and the identity-provider client secret. It must protect the integrity of any uploaded root CA certificate. The hospital must report suspected disclosure through its security procedure and use the documented reset or recommissioning procedure.
- **Storage encryption.** MDTPlatform encrypts its clinical store at rest, and the snapshots it writes are encrypted as well. Nordic AI Medical holds no copy of the key that decrypts them.
- **Backup volume.** The hospital provides a durable backup volume separate from the clinical store and protects it through its ordinary backup service. The reference profile supports a 20 GiB encrypted store, an 80 GiB store volume, 25 GiB disk-backed scratch, 30 GiB application ephemeral-storage capacity and a 400 GiB backup volume. The hospital confirms at least 25 MiB/s on the slowest backup or recovery storage path. A site with a different storage path must qualify its selected resources using the operator runbook.
- **Backup schedule and alerts.** MDTPlatform publishes a verified encrypted copy of the whole store each day, starting at 03:00 UTC, with bounded retries after failure. It retains each payload for at least fourteen days and keeps at least seven complete payloads. The hospital checks the backup health. A successful scheduled publication older than 36 hours is reported as stale and requires the hospital operator's attention.

- **Recovery and key rotation.** The hospital operator stops clinical service by selecting maintenance mode and follows the written runbook. Recovery validates a selected encrypted backup and materializes the store on a blank target volume. Key rotation also uses a blank target with a newly generated key. The source volume remains unchanged. Before clinical use resumes, the hospital operator must check the recovered data under the hospital's incident procedure. Identify and reapply erasures, access changes and other relevant operations performed since the restore point, and re-enter later records from the clinical record. There is no automatic return to an earlier store.
- **Commissioning order.** The hospital operator runs the documented installation procedure to initialize the encrypted store and first administrator, supply the device key and backup volume, and check installation. The initial authenticated surveillance exchange completes activation. Once activation is complete, a surveillance outage does not prevent local clinical scoring.
- **Non-serving states.** The clinical service remains unavailable until commissioning and installation checks succeed. Planned maintenance displays the maintenance page. A startup, store or key failure displays the support state. The operator investigates the condition through the runbook before restoring service.
- **Browser certificate.** The hospital issues the certificate the deployment presents to the browser, supplies it at installation, and renews it before it expires.
- **Surveillance credential.** Nordic AI Medical supplies the hospital deployment's surveillance credential. The hospital stores it in the designated secret and protects it from disclosure. Suspected compromise requires replacement through the agreed support procedure. The application verifies the receiver's signed reply before recording acknowledged state.
- **Key custody.** The hospital protects the browser certificate and its private key and reports suspected compromise through its security procedure. It also holds the device key for the encrypted clinical store, mounts it read-only and restricts administrative access. A lost key leaves its encrypted store and backups unrecoverable. The hospital retains each historical key while an artefact needing it is retained and for thirty days afterwards. Nordic AI Medical holds no copy of these device keys.
- **Malware protection.** The hospital provides malware protection for the host environment; MDTPlatform ships no anti-malware component.

Intended duration and intended frequency of use

MDTPlatform is intended to be used transiently during clinical decision-making scenarios, which typically lasts between 1 and 30 minutes depending on the complexity of the patient case.

An example could include:

- Initial diagnosis: Used once during the initial multidisciplinary team (MDT) meeting to assess preoperative risk.
- Pre-surgical planning: Used as needed in the days or weeks leading up to surgery, depending on changes in patient condition or updated data.
- Post-surgical follow-up planning: Used transiently during postoperative MDT discussions to evaluate ongoing risks and guide further management.

The device is expected to be used 1-4 times per patient across the perioperative period, but this may vary based on individual patient needs.

2.7 Precautions/Warnings

Users must observe the following precautions when using MDTPlatform

- MDTPlatform may only be used by authorized healthcare personnel
- Do not use MDTPlatform to decide whether surgery is indicated or not
- Use risk score for decision support only. Always use clinical judgement.
- Read and understand these instructions for use before using MDTPlatform.

2.8 Clinical claims

Performance claims

- MDTPlatform is a software application consisting of a user interface (MDTPlus) for presenting patient information and an embedded model (STR-CRC) for prediction of a patient's short-term risk after elective resection for colorectal cancer with curative intent in adult patients.
- STR-CRC discriminates the composite short-term risk outcome with an area under the ROC curve at or above 0.70, the predefined goal stated in the Investigator's Brochure v3.0, when tested out of sample (data not used for training) in a cohort compliant with the intended medical context (see section 2.3).
- STR-CRC, when used for stratification, will separate risk stratification groups based on the observed rate of the composite short-term risk outcome.

Benefit claims

- When patient data is presented by MDTPlatform, variability in clinical decision making between clinicians is reduced.
 - As measured by reduced entropy in suggested treatment when exposing the same patient cases to several clinicians using the MDTPlatform, compared to standard practice.
- 15% or more of surveyed clinicians using MDTPlatform report that the information provided by the model (that is, the short-term risk) supports them in making a clinical decision on perioperative treatment for the patient.
 - According to a 7-point Likert scale where 5, 6 or 7 are considered relevant to clinical decision making.
- 50% or more of surveyed clinicians using MDTPlatform report that the displayed information is relevant to clinical decision making.
 - According to a 7-point Likert scale where 5, 6 or 7 are considered relevant to clinical decision making.
- 25% or more of surveyed clinicians using MDTPlatform report that it provides a better overview of the current patient's treatment course, in the context of multidisciplinary decision making compared to usual practice.
 - According to a 7-point Likert scale where 5, 6 or 7 is considered better than usual practice.

2.8.1 Non-clinical Claims

- MDTPlus can store and display patient-specific data.
 - According to verification and validation report.

Disclaimers

- MDTPlatform does not provide decision support for deciding if a patient should receive surgery.
- MDTPlatform does not provide guidance on specific perioperative treatment pathways.
- MDTPlatform does not claim to reduce the risk of death or complications.
- Any treatments that clinicians decide on based on output from MDTPlatform should be either standard of care, evidence based, or based in research.

3 Safety Instructions

Read these instructions for use carefully. They are part of the device and have to be available at all times. Only use the device for the intended purpose described in this document (see chapter 2.1).

For your own safety as well as for the safety of your patients and according to the requirements of the Medical Device Regulation, please observe the following:

WARNING: Important safety or performance information or immediate response from operator required.

CAUTION: Other important information with or without the need of operator response.

3.1 General safety remarks

	CAUTION: Only use MDTPlatform in the intended patient population
	CAUTION: Only authorized healthcare personnel may use MDTPlatform.
	CAUTION: Do not use MDTPlatform to decide whether surgery is indicated or not.

Table 3.1: General remarks

3.2 Operation of the Device

	Use risk score for decision support only. Always use clinical judgement.
	CAUTION: Use MDTPlatform in Microsoft Edge version 137 or newer, or Google Chrome version 137 or newer. Compatibility with other browsers cannot be guaranteed.
	CAUTION: Users should read and understand the instructions for use before use.

Table 3.2: Operation of the Device

The warnings and cautions above accompany the device risk controls. The risk assessment in 08_00_002 records the residual risks and their acceptance.

3.3 Side Effects and Contraindications

Possible side effects, adverse effects, and risks:

Misinterpretation of a prediction could contribute to inappropriate allocation of perioperative resources and affect patient outcomes. The available evidence does not establish how often this occurs. In the historical usability evaluation all five participants detected a deliberately incorrect stratification; this small evaluation does not estimate adverse-event frequency.

MDTPlatform makes no claim to reduce death or complications. Always assess its output with the patient's clinical information and professional judgment.

There are no contraindications for using MDTPlatform.

4 Installation and Uninstallation

The customer and Nordic AI Medical ApS establish the deployment, data protection and account administration arrangements. The hospital-controlled deployment may be installed on site or in infrastructure controlled by the customer in a cloud environment.

On-site Solution

1. The hospital operator installs MDTPPlatform in hospital-controlled infrastructure using the release-matched installation runbook and acceptance protocol.
2. User handling is done by the healthcare facility's IT department or an administrator at the department buying the MDTPPlatform solution.
3. A local instance of the MDTPPlatform website is then accessible via the departments/healthcare institutions local intranet.
4. Uninstallation is performed by the IT department, supported by Nordic AI Medical ApS.

Cloud Solution

1. The customer selects and controls the cloud hosting environment and assesses its data protection and operational arrangements. The same hospital-controlled deployment and installation acceptance requirements apply.
2. The hospital administrator creates or approves local or hospital-identity-provider accounts and grants meeting-series membership to authorised users.
3. The hospital administrator manages user access. Meeting-series membership controls access to the associated patient records.
4. The end-user accesses MDTPPlatform via a website on the internet.
5. The hospital operator removes access and uninstalls the deployment under the agreed termination procedure. The hospital retains or erases clinical data, backups and keys according to its applicable record-retention obligations.

5 Operation

The user interface is in Danish and names the product "MDT+". The labels in quotation marks below are the labels the user interface shows. The illustrations show MDTPPlatform v1.0.0 with example data. A marker in an illustration, for example 5.8.2, points to the control that step 2 of section 5.8 uses.

5.1 Logging in and out

5.1.1 Logging in

The "Log ind" page shows the login methods the hospital has set up: an organisation account through the hospital identity provider, a local account with a username and password, or both. When both methods are set up, the page asks "Hvordan vil du logge ind?". When one method is set up, the page shows that method directly.

1. Open the MDTPPlatform address provided by the hospital in Microsoft Edge or Google Chrome, version 137 or newer.
2. Select "Log ind" on the start page "Velkommen til MDT+".
3. Select the login method on the "Log ind" page (section 5.1.2 or 5.1.3).

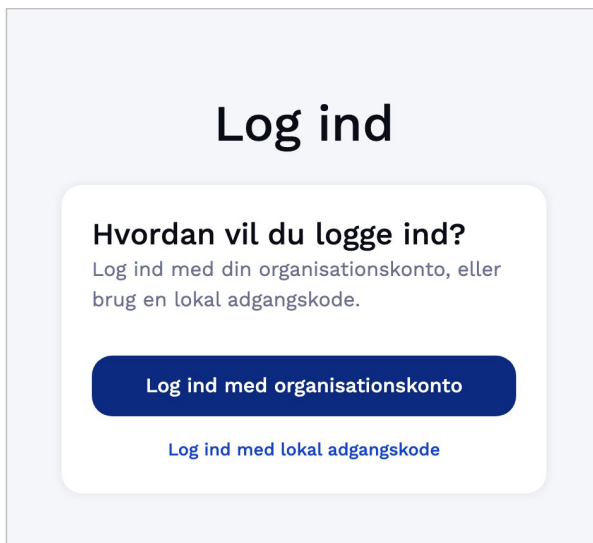


Figure 1. The “Log ind” page with the two login methods

5.1.2 Logging in with an organisation account

1. Select “Log ind med organisationskonto”. At some sites the button carries the name of the hospital or region instead.
2. Log in at the hospital identity provider.
3. Check that the page “Bekræft, hvem du er” shows your name.



Figure 2. The page “Bekræft, hvem du er”

4. Select “Fortsæt” to open your meetings.

If the page shows another person’s name, select “Log ind som en anden bruger” and log in again at the hospital identity provider.

5.1.3 Logging in with a local account

1. Select “Log ind med lokal adgangskode”. When the hospital has set up local accounts only, the username and password fields are shown directly.

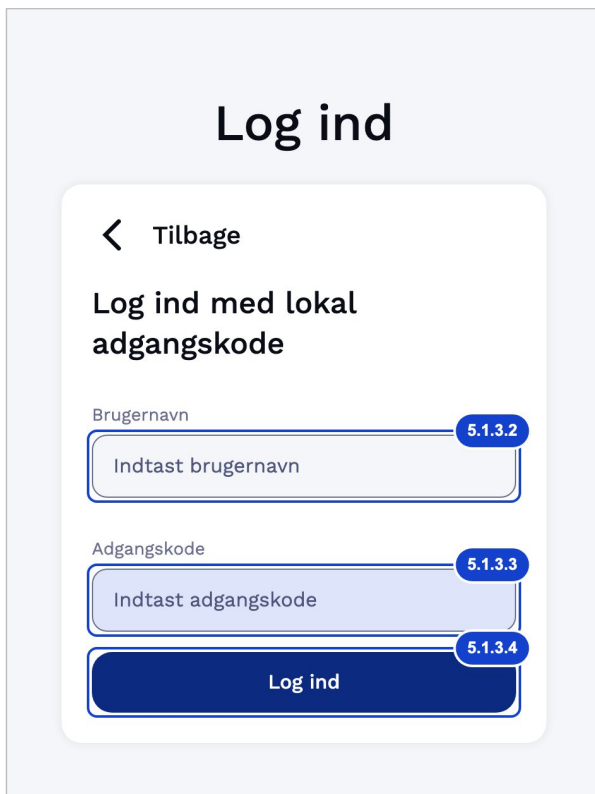


Figure 3. Login with a local account

2. Enter your username in “Brugernavn”.
3. Enter your password in “Adgangskode”.
4. Select “Log ind”.

MDTPatform opens the page “Vælg en ny adgangskode” when you log in with a temporary password from the hospital administrator:

1. Enter a new password in “Ny adgangskode”. The page lists the requirements under “Krav til adgangskoden”. The password must have at least 15 characters.
2. Enter the same password in “Bekræft ny adgangskode”.
3. Select “Gem adgangskode”.

Five consecutive failed login attempts lock a local account for 15 minutes. The lock then clears automatically, or the hospital administrator can clear it sooner (section 5.15.4).

5.1.4 Access awaiting approval

The first time you log in with an organisation account that has no MDTPatform user, the page “Adgang afventer godkendelse” opens. Your organisation has confirmed who you are, and the login is recorded as an access request for the hospital administrator (section 5.15.2).

1. Ask the hospital administrator to approve your access request.
2. Wait until you are told that your access is approved.
3. Select “Log ind igen” and log in with your organisation account.

5.1.5 Logging out

While you are logged in, the “Log ud” button is in the top right corner of the page header. On a narrow screen, select the round menu button at the top right to find it.

1. Select “Log ud” to log out of the device.



Figure 4. The “Log ud” control in the page header

After logging out, MDTPlatform shows the start page.

5.2 Creating new series of meetings

Creating a series of meetings requires administrative rights. An administrator sees the link “Admin” on the “Mine møder” page.

1. Select “Admin” on the “Mine møder” page. The “Administration” page opens on its overview (section 5.15.1).
2. Select “Møderække” to open the list of series of meetings.

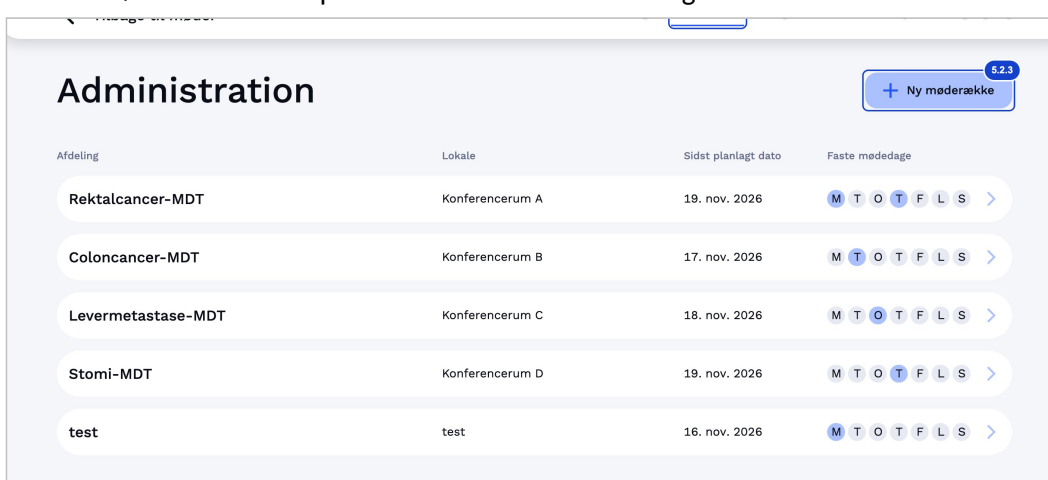


Figure 5. The list of series of meetings

3. Select “Ny møderække”.
4. Enter the department in “Afdeling”.
5. Enter the room where the meetings are held in “Lokale”.
6. Select the weekdays on which the meetings recur under “Faste mødedage”.
7. Select “Opret møderække” to create the series of meetings.

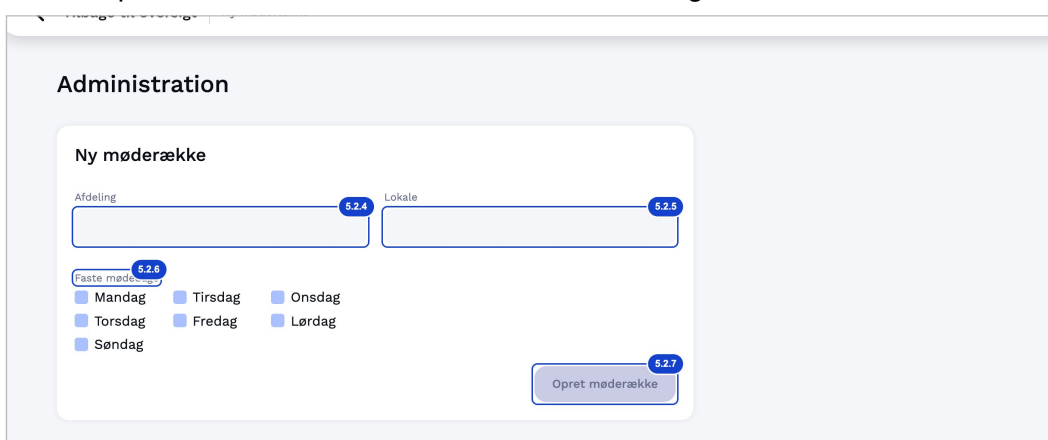


Figure 6. The page “Ny møderække”

MDTPlatform then opens the page of the new series of meetings. Add users, the risk strata and contact groups there as described in section 5.3.

5.3 Editing series of meetings

Editing a series of meetings requires administrative rights.

1. Select “Admin” on the “Mine møder” page.
2. Select “Møderækker”.
3. Select the series of meetings you want to edit in the list.

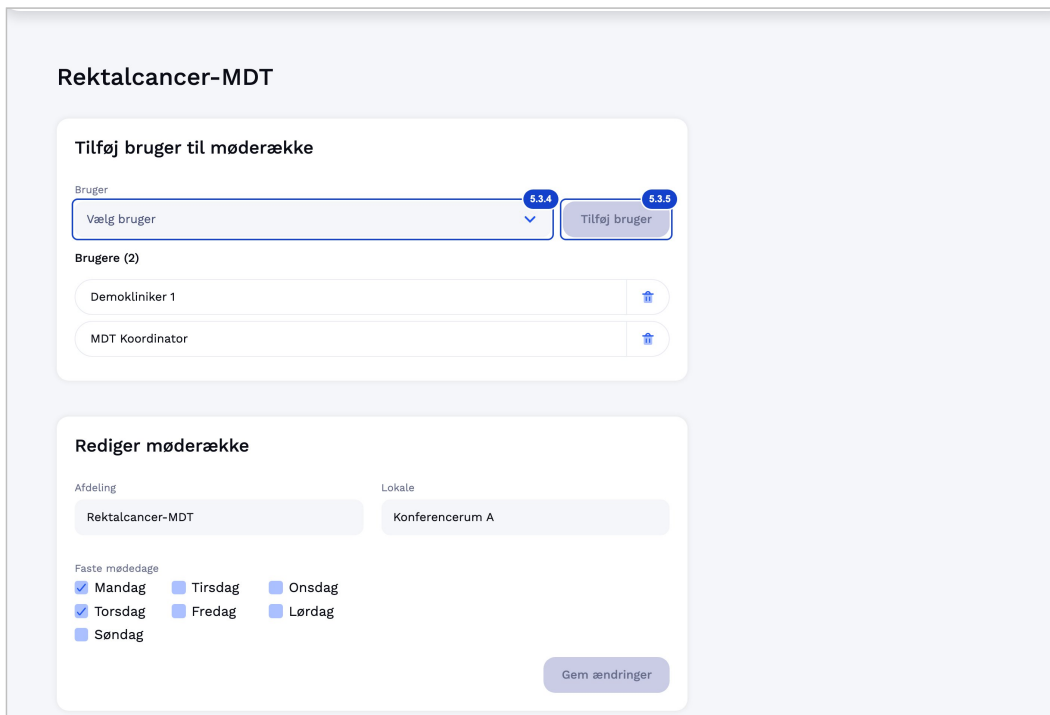


Figure 7. The page of a series of meetings

Users of the series. Only users added to a series of meetings can see its meetings and patients. A user must exist on the “Brugere” page before it can be added (section 5.15).

4. To add a user, select the user in the field “Bruger” under “Tilføj bruger til møderække”.
5. Select “Tilføj bruger”.
6. To remove a user, select the recycle-bin icon next to the user’s name in the “Brugere” list. The removal takes effect at once.

Place and weekdays.

7. To change the department, room or weekdays, adjust the fields under “Rediger møderække”.
8. Select “Gem ændringer” to save the changes.

Risk strata. The risk strata under “Model konfiguration” translate the risk rank from 0 to 100 into the labels shown for each patient in this series of meetings. Each stratum has a label in “Navn” and an upper limit in “Grænseværdi”, and the highest stratum always ends at 100. A series of meetings holds at most four strata.

9. To add a stratum, select “Tilføj konfiguration”. The control is shown while the series holds fewer than four strata.
10. Enter the label in “Navn” and the upper limit in “Grænseværdi” for each stratum.
11. To remove a stratum, select the recycle-bin icon (“Slet konfiguration”) on its row.
12. Select “Gem konfiguration”.
13. Select “Fortsæt” in the dialog “Er du sikker?”. The new strata apply at once for all users of the series of meetings.

Contact groups. Contact groups are shown at the bottom of each meeting with status “Klar” in the series of meetings.

14. To add a group, enter the group name in “Gruppenavn” under “Ny gruppe”.
15. Enter the first contact person’s name in “Navn” and contact information in “Kontakt info”.
16. Select “Opret gruppe”.
17. To add a contact to a group, enter the name in “Navn” and the contact information in “Kontakt info” under “Tilføj kontakt” in that group.
18. Select “Tilføj”.
19. To delete a contact, select the recycle-bin icon next to the contact’s name and confirm with “Slet”.
20. To delete a group together with its contacts, select the recycle-bin icon next to the group name and confirm with “Slet”.

5.4 Deleting series of meetings

Deleting a series of meetings requires administrative rights.

1. Select “Admin” on the “Mine møder” page.
2. Select “Møderække”.
3. Select the series of meetings you want to delete in the list.
4. Select “Slet møderække” at the bottom of the page. On a narrow screen, select the recycle-bin icon in the bar at the top of the page instead.
5. Select “Slet møderække” in the dialog “Slet møderække” to delete the series of meetings.



Figure 8. The dialog “Slet møderække”

The deletion cannot be undone. MDTPlatform then shows the list of series of meetings.

5.5 Adding patients to a meeting

1. On the “Mine møder” page, select the meeting where you want to add a patient.

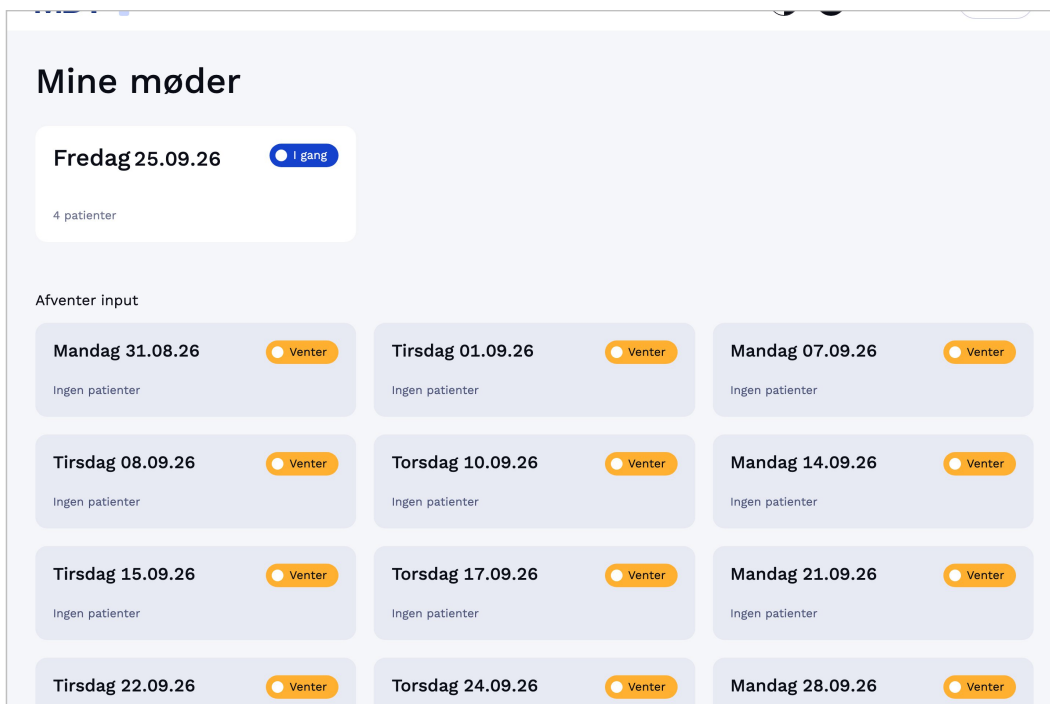


Figure 9. The page “Mine møder”

2. Select “Tilføj patient” above the patient list, or the “Tilføj patient” field below it.

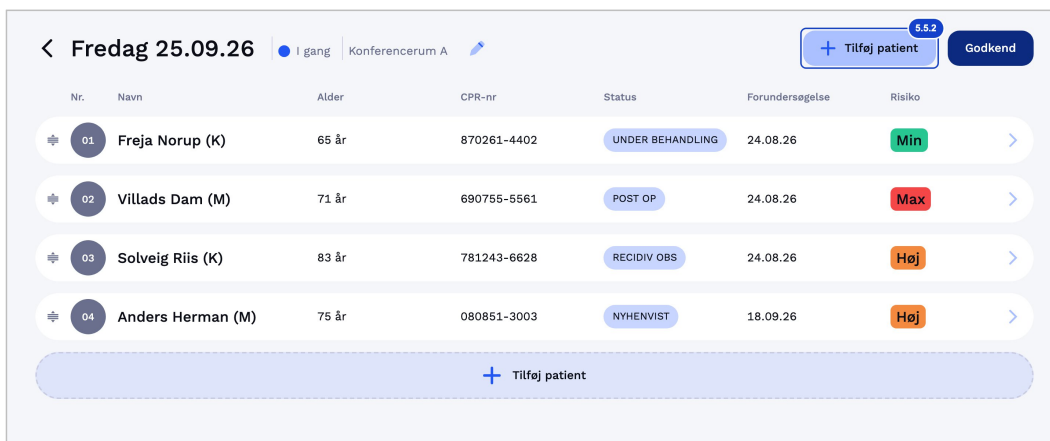


Figure 10. A meeting with its patient list

Patients can only be added to meetings with status “Venter” and “I gang”. Adding the first patient to a meeting with status “Venter” changes the status to “I gang”. To add a patient to a meeting with status “Klar”, first select “Rediger patientliste”. The status changes to “I gang” and “Tilføj patient” becomes available.

3. Enter the patient’s CPR number in “CPR-nummer” on the page “Opret patient”.
4. Select “Gem CPR-nummer”.

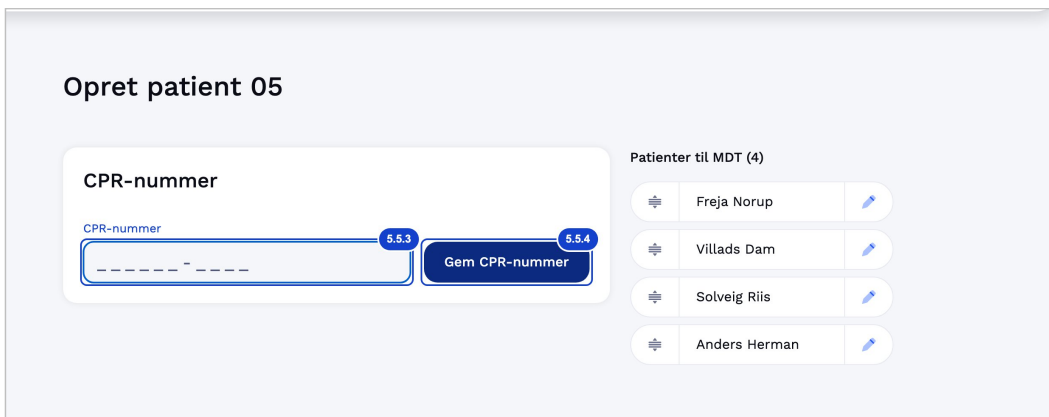


Figure 11. The page “Opret patient”

5. Enter the patient information on the page that opens.
6. Select “Gem patient” to save, or “Gem og luk” to save and open the patient page. After “Gem patient” the page stays open in a browser window at least 768 pixels wide and returns to the patient list in a narrower window.

5.6 Editing information about patients

1. On the “Mine møder” page, select the meeting where you want to edit information about a patient.
2. Select the patient in the patient list. The patient page opens and shows the risk under “Kortsigtet risiko”.

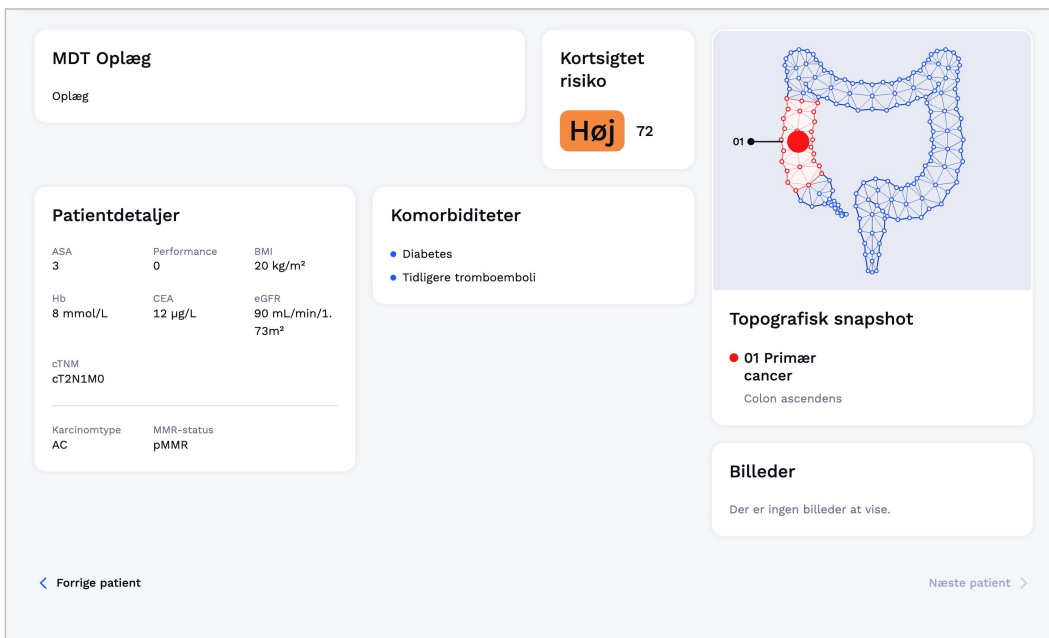


Figure 12. The patient page with the short-term risk

3. Select “Rediger information”.
4. Edit the previously saved information.

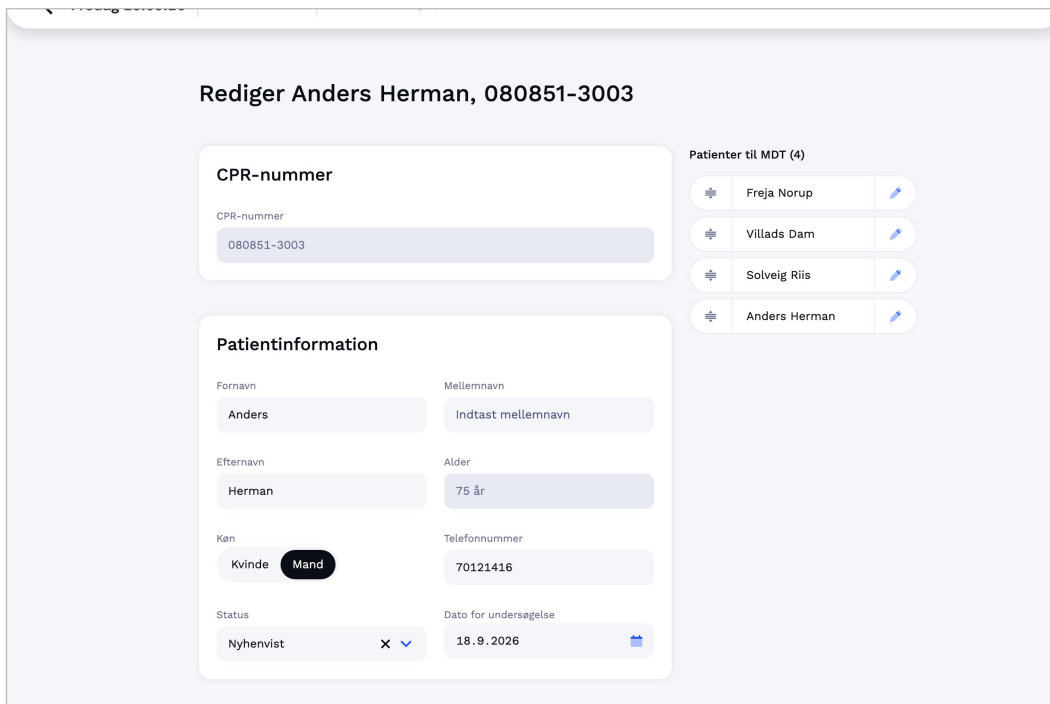


Figure 13. The edit patient form

5. Select “Gem patient” to save, or “Gem og luk” to save and open the patient page. After “Gem patient” the page stays open in a browser window at least 768 pixels wide and returns to the patient list in a narrower window.

Reading the risk. “Kortsigtet risiko” shows the risk stratum label configured for the series of meetings (section 5.3) and the risk rank from 0 to 100. While the risk is being calculated, the card shows three moving dots. When no risk can be shown, the card shows the reason, for example “Prædiktion utilgængelig: risikotallet kunne ikke hentes” or “Modellen kan ikke svare” (chapter 6). Use the risk for decision support only (section 3.2).

5.7 Removing patients from a meeting

1. On the “Mine møder” page, select the meeting where you want to remove a patient.
2. Select the patient you want to remove from the patient list.
3. Select “Rediger information”.
4. Select “Slet fra MDT” at the bottom of the page.
5. Select “Slet patientdata” in the dialog “Du er ved at slette patientdata” to delete the patient from the patient list.



Figure 14. The dialog "Du er ved at slette patientdata"

The deletion cannot be undone. To move the patient to another meeting instead, select "Flyt patient" at the bottom of the page. Select the new meeting in "Dato" in the dialog "Flyt patient" and select "Godkend".

5.8 Sorting patients in a meeting

1. Open the meeting on the "Mine møder" page.
2. Drag the patient by the handle at the left of its row to the new position in the patient list.

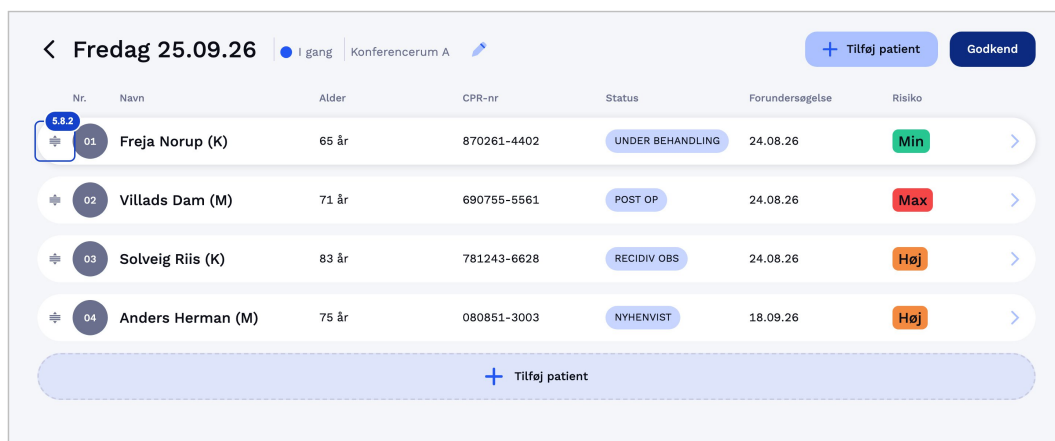
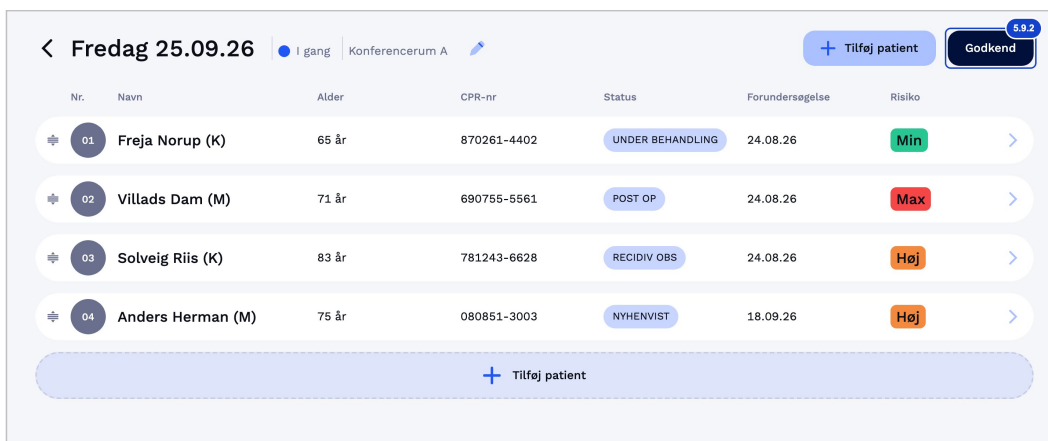


Figure 15. Sorting patients with the drag handle

Patients can only be sorted in meetings with status "Venter" and "I gang". To sort the patients of a meeting with status "Klar", first select "Rediger patientliste". The status changes to "I gang" and the patients can be dragged.

5.9 Approving meetings

1. Open a meeting with status "I gang" on the "Mine møder" page.
2. Select "Godkend" to approve the meeting.



Nr.	Navn	Alder	CPR-nr	Status	Forundersøgelse	Risiko
01	Freja Norup (K)	65 år	870261-4402	UNDER BEHANDLING	24.08.26	Min
02	Villads Dam (M)	71 år	690755-5561	POST OP	24.08.26	Max
03	Solveig Riis (K)	83 år	781243-6628	RECIDIV OBS	24.08.26	Høj
04	Anders Herman (M)	75 år	080851-3003	NYHENVIST	18.09.26	Høj

Figure 16. The “Godkend” control

The status changes to “Klar” and MDTPlatform returns to the “Mine møder” page. “Godkend” is shown only when the meeting holds at least one patient.

5.10 Editing meeting information for a specific meeting

The control for editing the date and room depends on the meeting status.

1. Open the meeting on the “Mine møder” page.
2. Select “Rediger møde”: for a meeting with status “Klar” it is the button at the top right, and for a meeting with status “Venter” or “I gang” it is the pencil icon next to the room.
3. Enter the date in “Dato” and the room in “Lokale” in the dialog “Rediger mødeinformation”.
4. Select “Gem mødeinformation” to save the meeting information.



Rediger mødeinformation

Ændringer er kun reflekteret i MDT+. Hvis du vil sikre at mødeindkaldelser bliver opdateret, skal du foretage ændringer i jeres kalendersystem.

Dato

25.9.2026

Lokale

Konferencerum A

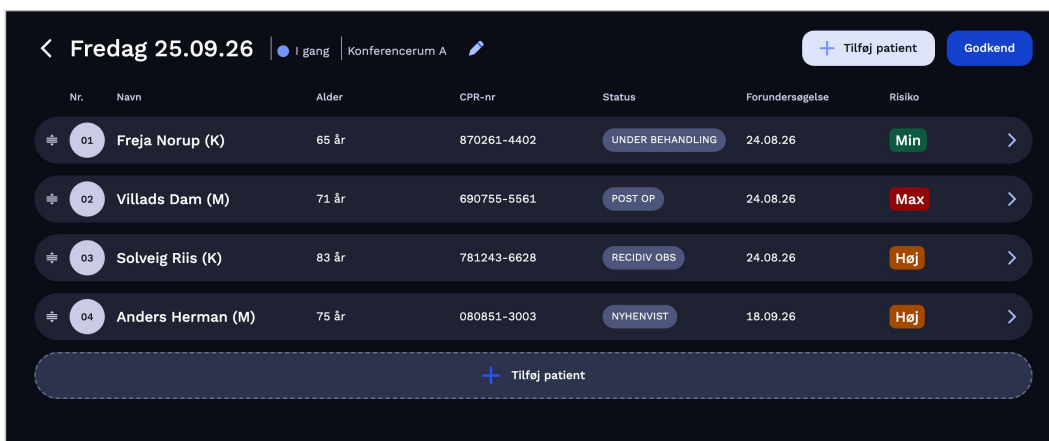
Annuler Gem mødeinformation

Figure 17. The dialog “Rediger mødeinformation”

The date cannot be earlier than the current date in UTC, and a series of meetings holds one meeting per date. The change is made in MDTPlatform only. Update meeting invitations in the hospital calendar system.

5.11 Toggling dark and light mode

1. Select the theme icon (“Skift tema”) at the top right to switch between dark and light mode.



Nr.	Navn	Alder	CPR-nr	Status	Forundersøgelse	Risiko
01	Freja Norup (K)	65 år	870261-4402	UNDER BEHANDLING	24.08.26	Min
02	Villads Dam (M)	71 år	690755-5561	POST OP	24.08.26	Max
03	Solveig Riis (K)	83 år	781243-6628	RECIDIV OBS	24.08.26	Høj
04	Anders Herman (M)	75 år	080851-3003	NYHENVIST	18.09.26	Høj

Figure 18. Dark mode

5.12 Toggling presentation mode

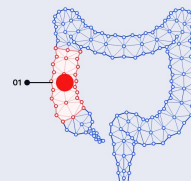
Presentation mode enlarges the content for large screens. The control is shown on the patient page, the “Opret patient” page and the administration pages of a series of meetings when the browser window is at least 1280 pixels wide.

1. Select “Præsenter indhold” at the top of the page.



MDT Oplæg
Oplæg

Kortsigtet risiko
Høj
72



Patientdetaljer
ASA 3 Performance 0
BMI 20 kg/m² Hb 8 mmol/L
CEA 12 µg/L eGFR 90 mL/min/1.73m²
cTNM cT2N1M0
Karcinomtype AC MMR-status pMMR

Komorbiditeter

- Diabetes
- Tidligere tromboemboli

Topografisk snapshot
● 01 Primær cancer
Colon ascendens

Billeder
Der er ingen billeder at vise.

Figure 19. Presentation mode

2. To return to regular mode, select “Stop præsentation”.

5.13 Contacting support

5.13.1 Support contact in the page footer

At the bottom of every MDTPlatform page, the footer shows the contact information for Nordic AI Medical support under “Kontakt”: the opening hours (Monday to Thursday 08.00 to 16.00, Friday 08.00 to 15.00) and the telephone number +45 60 13 41 18.



Figure 20. The page footer with the support contact

Alternatively, contact support@nordicaimedical.com.

5.13.2 Help on the product information page

1. Select "Om MDT+" under "Andet" in the page footer.
2. Find the support e-mail address under "Hjælp".

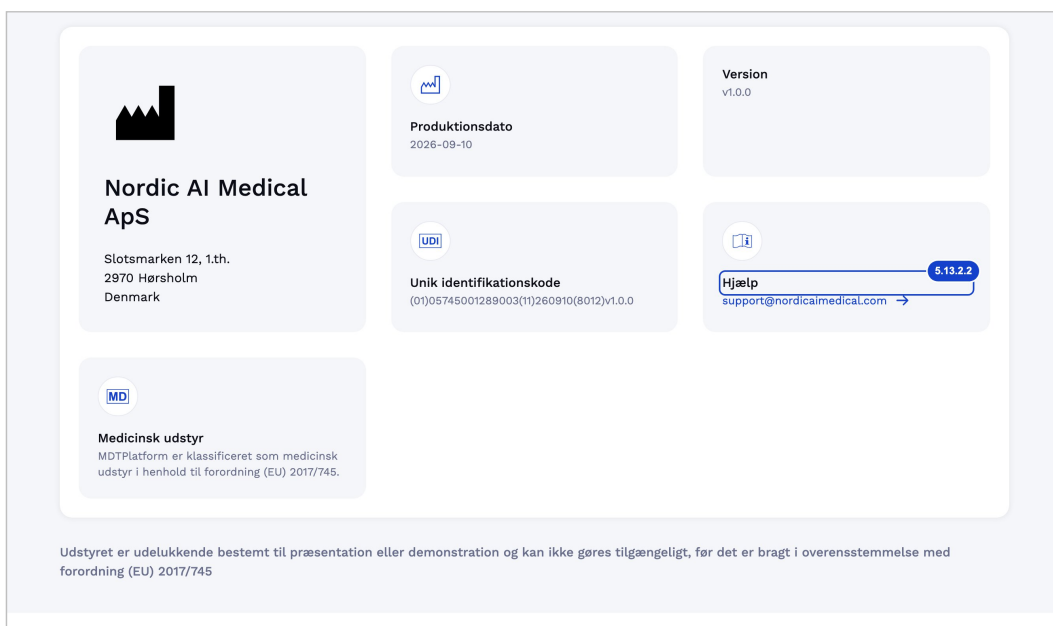


Figure 21. The page "Om MDT+"

The page "Om MDT+" also shows the production date ("Produktionsdato"), the version ("Version") and the unique device identifier ("Unik identifikationskode") of the installed MDTPatform.

5.14 Reporting errors, bugs or areas of improvement

Report errors, bugs and suggestions for improvement to support@nordicaimedical.com.

5.15 Administering users and access

The functions in this section require a user with administrative rights.

5.15.1 Administration overview

1. Select "Admin" on the "Mine møder" page.

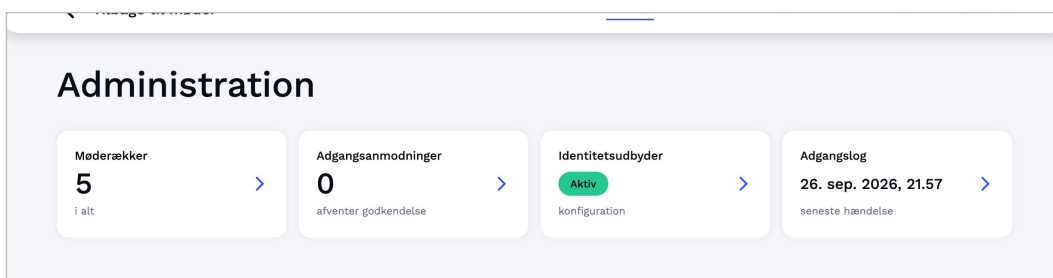


Figure 22. The administration overview

The “Administration” page opens on “Oversigt”. The menu at the top leads to “Oversigt”, “Møderækker”, “Brugere”, “Identitetsudbyder” and “Adgangsløg”. The overview shows four cards:

- “Møderækker”: the number of series of meetings.
- “Adgangsmodninger”: the number of access requests awaiting approval.
- “Identitetsudbyder”: the state of the identity-provider configuration.
- “Adgangsløg”: the time of the latest access event.

When the backup needs attention, the overview shows a notice above the cards. Forward the notice to the hospital operator.

5.15.2 Approving access requests

1. Select “Brugere” in the administration menu.

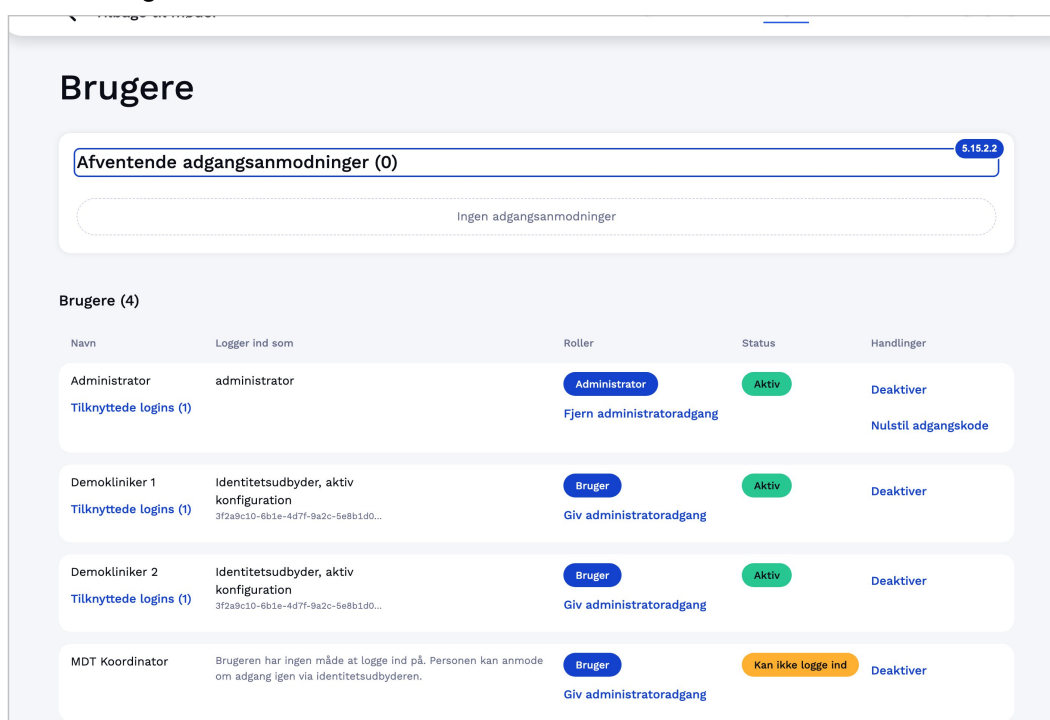


Figure 23. The page “Brugere”

2. Find the request under “Afventende adgangsanmodninger”.
3. Check the name in “Visningsnavn” and correct it if needed. The identity provider supplies the name, and MDTPlatform does not verify it.
4. Select “Administratoradgang” only for a person who needs administrative rights.
5. Select the series of meetings the person needs under “Medlemskab af møderækker”.
6. Select “Godkend”.

To refuse a request, select “Afvis” and confirm with “Afvis”. The person can request access again by logging in.

5.15.3 Creating local users

A local user logs in with a username and password. Create a local user for a person who cannot log in through the hospital identity provider.

1. Enter the username in “Brugernavn” under “Ny lokal bruger”.
2. Enter the person’s name in “Visningsnavn”.

3. Select "Administratoradgang" only for a person who needs administrative rights.
4. Select "Opret bruger".
5. Give the temporary password shown under "Midlertidig adgangskode til" to the named person only, through a confidential channel approved by the hospital.
6. Add the user to the series of meetings the person needs (section 5.3).

The temporary password is shown once. The person chooses a new password at the first login (section 5.1.3).

5.15.4 Managing users

The list "Brugere" shows each user's name, how the user logs in, the roles, the status and the available actions.

- To give or remove administrative rights, select "Giv administratoradgang" or "Fjern administratoradgang".
- To stop a user from logging in, select "Deaktiver" and confirm with "Deaktiver". The user is logged out at once.
- To let a deactivated user log in again, select "Genaktiver".
- To clear the lock of a locked local user, select "Lås op".
- To give a local user a new temporary password, select "Nulstil adgangskode" and confirm with "Nulstil adgangskode". Give the new temporary password to the person as described in section 5.15.3.
- To remove one of a user's logins, select "Tilknyttede logins", then "Fjern login", and confirm with "Fjern". The user is kept.

MDTPlatform refuses to deactivate the last administrator who logs in with a local password and refuses to remove that user's administrative rights. It also refuses to remove the last login of the last administrator. The installation therefore always keeps one administrator.

5.15.5 Configuring the identity provider

A hospital administrator configures the hospital identity provider. A configuration is saved as a draft, tested and then activated.

1. Select "Identitetsudbyder" in the administration menu.

Identitetsudbyder

Aktiv konfiguration

Udsteder-URL
https://login.eksempel.dk/realms/hospital

Klient-id
mdtplatform

Udbydertype
Generisk OpenID Connect

Rodcertifikat
Intet (systemets certifikatlayer bruges)

Visningsnavn på login-knappen
Ikke angivet (standardteksten bruges) [Rediger visningsnavn](#)

Skift klienthemmelighed

Konfigurationskladde

Konfigurationen gemmes som en kladde, indtil du aktiverer den. Felterne er forudfyldt med den aktive konfiguration.

Udsteder-URL
https://login.eksempel.dk/realms/hospital 5.15.5.2

Udbyderens HTTPS-udstederadresse fra dens OpenID Connect-metadata. Eksempel på vært og sti: login.eksempel.dk/realms/hospital.

Klient-id
mdtplatform 5.15.5.3

Klienthemmelighed

Den klient, der er registreret for denne installation hos udbyderen.

Udstedes af udbyderen sammen med klient-id'et. Den gemmes, men vises aldrig igen.

Figure 24. The page "Identitetsudbyder"

2. Enter the issuer address in "Udsteder-URL" under "Konfigurationskladde".
3. Enter the client identifier in "Klient-id".
4. Enter the client secret in "Klienthemmelighed".
5. Check that "Udbydertype" reads "Generisk OpenID Connect".
6. Enter the text for the login button in "Visningsnavn på login-knappen", if wanted.
7. Register the address shown in "Redirect-URI" unchanged at the identity provider.
8. Select "Gem kladde".
9. Select "Test forbindelsen" under "Test af kladden".
10. Select "Test login i browseren" and confirm with "Start test".
11. Log in at the identity provider. MDTPlatform returns to the page "Identitetsudbyder" afterwards.
12. Select "Aktiver konfigurationen" and confirm with "Aktiver". The control is shown once the draft is saved and can be selected after a successful test login.

When the identity provider uses a certificate from the hospital's own certificate authority, add that authority's root certificate after step 8:

1. Paste the root certificate into "Certifikat (PEM-tekst)" under "Tilføj rodcertifikat".
2. Select "Tilføj certifikat".
3. Select "Brug til kladden" next to the certificate under "Betroede rodcertifikater".

Paste the certificate only. MDTPlatform refuses text that holds a private key.

MDTPlatform blocks replacement of the active identity-provider configuration while any user account remains linked to it. This restriction applies even when all users are logged out. If replacement is blocked, MDTPlatform shows "Handlingen kunne ikke gennemføres. Prøv igen." Contact support to plan replacement of an identity provider that has linked accounts. To replace only the client secret of the active configuration, select "Skift klienthemmelighed". To change only the text of the login button, select "Rediger visningsnavn".

5.15.6 Reviewing the access log

The access log records who accessed which data and when.

1. Select "Adgangslog" in the administration menu.

Adgangslog

Eksporter som CSV

Fra

dd/mm/yyyy, --,--

5.15.6.2

Til

dd/mm/yyyy, --,--

5.15.6.3

Bruger-id

Anvend filter

Indtast id'et præcis som det står i kolonnen Bruger-id.
Loggen viser bruger-id'er. Navnene står i CSV-eksporten.

Tidspunkt	Bruger-id	Handling	Berørt data	Datakategori	Detaljer
2026-09-26T19:57:30.506Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Adgangslog set accessLogList	Adgangslog	Sikkerhed security	-
2026-09-26T19:57:29.014Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Testlogin afsluttet authOldcTestResult	Identitetsudbyder	Sikkerhed security	-
2026-09-26T19:57:28.982Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Rodcertifikater set authOldcTrustAnchorsList	Identitetsudbyder	Sikkerhed security	-
2026-09-26T19:57:28.980Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Identitetsudbyder set authOldcConfigRead	Identitetsudbyder	Sikkerhed security	-
2026-09-26T19:57:27.501Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Identitetsudbyder set authOldcConfigRead	Identitetsudbyder	Sikkerhed security	-
2026-09-26T19:57:27.499Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Adgangsmodninger set authPendingList	Bruger	Sikkerhed security	-
2026-09-26T19:57:27.498Z	3f2a9c10-6b1e-4d7f-9a2c-5e8b1d0c4a77	Møderækker set seriesList	Møderækker	Administrative oplysninger administrative	-

Figure 25. The page “Adgangslog”

- Enter the start and end of the period in “Fra” and “Til”, and a user id in “Bruger-id” if needed.
- Select “Anvend filter”.
- Select “Indlæs flere” to show older events.
- Select “Eksporter som CSV” to save the filtered log as a file.

“Fra” and “Til” are read on the computer’s clock, and the column “Tidspunkt” shows times in UTC. The log shows user ids. The CSV export also holds the names.

6 Troubleshooting

Problem	Possible solution
I cannot create a series of meetings	Only a user with administrative rights can create a series of meetings (section 5.2). Contact the hospital administrator.
I cannot find my meetings	Only users added to a series of meetings see its meetings (section 5.3). Ask the hospital administrator to add you to the series of meetings.
I forgot my password	For a local account, ask the hospital administrator to reset the password (section 5.15.4). For an organisation account, follow the password recovery procedure of the hospital identity provider.
The page shows “Adgang afventer godkendelse”	Your organisation account has no MDTPatform user yet. Ask the hospital administrator to approve your access request, then select “Log ind igen” (section 5.1.4).
My local account is locked	Five consecutive failed login attempts lock the account for 15 minutes. Wait 15 minutes, or ask the hospital administrator to select “Lås op” (section 5.15.4).
The page shows “Systemet er	The deployment is being set up, maintained or restored. The

Problem	Possible solution
ikke klar"	page checks again by itself. If the interruption continues, contact the hospital operator or support.
"Kortsigtet risiko" shows three moving dots	The risk is being calculated. Wait for the result. When the card shows "Dette tager længere end normalt; kontakt support hvis det fortsætter", contact support.
"Kortsigtet risiko" shows "Prædiktion utilgængelig: risikotallet kunne ikke hentes"	The risk could not be retrieved. Open the patient page again. If the message remains, contact the hospital operator or support.
"Kortsigtet risiko" shows "Modellen kan ikke svare"	The model gave no risk for the saved patient information: it rejected the information, or its answer could not be used. Check the patient information (section 5.6) and save it again. If the message remains, contact support.

7 Technical Data

7.1 Software classification

Feature	Value
Medical device class according to Regulation EU 2017/745 (MDR)	Product is of Class IIa
Software risk classification according to EN 62304:2006+A1:2015	Product is Class A

7.2 Requirements for hosting

The following requirements must be met by any hosting provider.

- Network segmentation
- Firewall
- Encrypted HTTPS for browser access and outbound receiver communication; isolated internal service connections
- Hospital identity provider authentication, including multi-factor authentication where required by hospital policy
- Complex password policy
- Role based access control
- Audit log
- Environment control for server facility
 - Access control
 - Surveillance
 - Fire suppression
 - Power redundancy
 - Climate control
- Server backup plan

7.3 System minimum requirements

MDTPlatform runs the gateway, clinical application and STR-CRC inference unit on hospital-controlled Kubernetes infrastructure. The surveillance receiver and receiver database run separately in NAIM-controlled infrastructure. The reference hospital qualification profile is 8 vCPUs and 16 GB RAM, with the storage, browser, network and security requirements stated in section 2.6. The hospital operator follows the release-matched installation and acceptance runbook.

7.4 Supported web browsers

Web application	Microsoft Edge version 137 or newer, or Google Chrome version 137 or newer.
-----------------	---

8 Legal notices

In the case of the user or customer experiencing or being made aware of any serious incident, or of any adverse event which could have led to a serious incident, this must be reported without delay to Nordic AI Medical ApS and to the competent authority of the Member State in which the user or the patient is established. Please see contact information in Chapter 1.

9 Symbols and definitions in MDTPlatform

Symbol	Meaning
	Manufacturer name and address Supplementary see EN ISO 15223-1
	Unique Device Identifier (UDI) Supplementary see EN ISO 15223-1
	Date of manufacture Supplementary see EN ISO 15223-1
	CE label (for Class II/III products, the four-digit identification number of the Notified Body involved must be indicated) CE mark may NOT be placed on a device prior to declaration of conformity is obtained.
	Indicates that the device is a medical device Supplementary see EN ISO 15223-1
	Indicates that the user should reference the instructions for use Supplementary see EN ISO 15223-1
	Warning (Warnings have their origin in risk assessment. They are necessary to draw the user's attention to residual risks or sources of danger. All warnings are listed in Chapter 3 below each other.)

Table 9.1: Symbols and definitions

10 Declaration of Conformity

These instructions are prepared for the conformity-assessment submission. The device may be supplied for routine clinical use only after the applicable conformity assessment and declaration are complete.